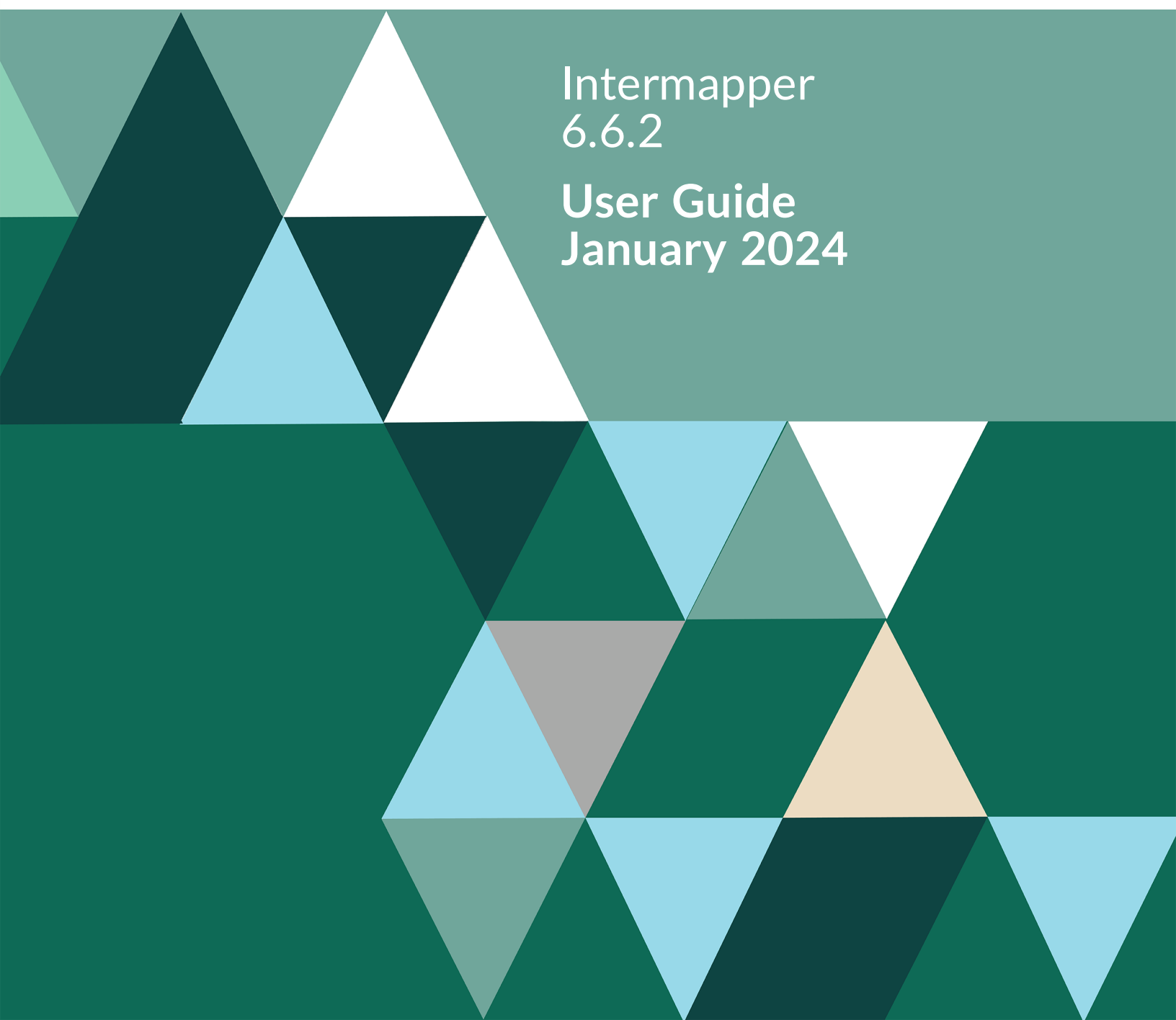


FORTRA



Intermapper
6.6.2
User Guide
January 2024

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202401241244

Table of Contents

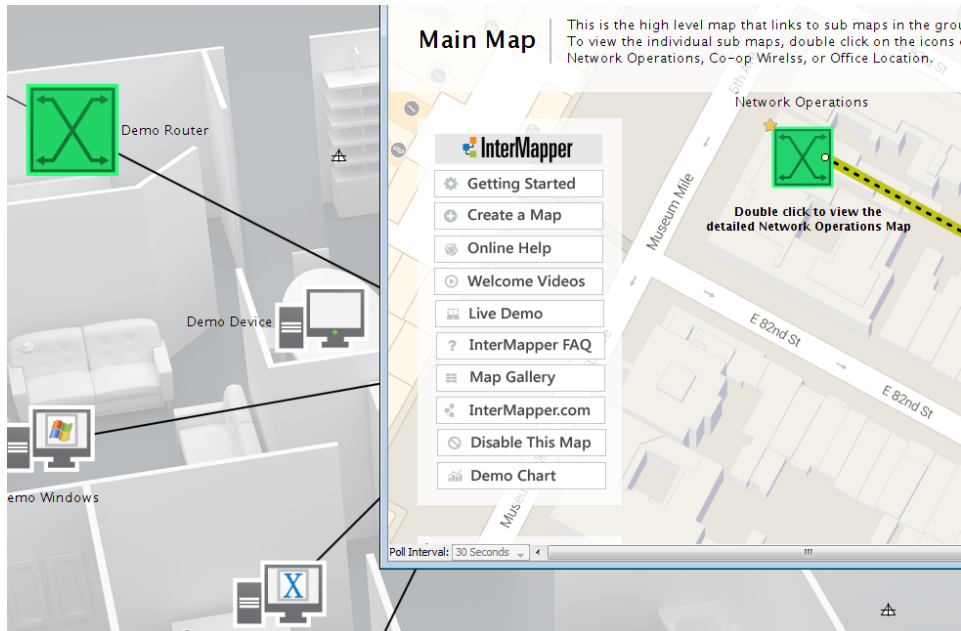
Welcome to Intermapper	6
Intermapper Server and Network Monitoring	6
Getting Started	8
Installing and Launching Intermapper	8
Using Demo Maps	8
Registering Your Software	8
Intermapper Control Center	9
Automatic Update Notifications	12
Installing Intermapper Flows	13
Intermapper Quick Tour	13
Using Intermapper	17
Using Intermapper	19
Creating Maps	41
Arranging Your Map	79
Notifiers and Alerts	106
Monitoring Your Network	154
Server Settings	224
Intermapper Flows™ Overview	291
Using the Layer 2 View	315
Intermapper Reports	329
Using Intermapper Remote Access	345

Intermapper Reference	347
Command and Menu Reference	347
Probe Reference	409
Configuring Intermapper DataCenter	605
Intermapper Files and Folders	618
Importing and Exporting	625
Using the Web Server	679
Telnet Server Command Reference	693
Configuring Intermapper Server Using a Command Line	702
Using Intermapper With Splunk	715
Intermapper FAQs	721
How can I stop the Intermapper server from polling for a while?	721
How can I stop the Intermapper server? How can I restart it?	721
How can I move Intermapper from one server to another?	721
How can I uninstall the Intermapper server?	722
Why do I have trouble with Telnet using my Windows terminal program?	722
On an Xserve, can I use the serial port for paging?	723
How can I know that the embedded Java is secure?	724
Intermapper FAQs	725
Intermapper Flows FAQs	729
About IP Addresses	730
Quick Intro to IPv6 Address Formatting	733
About DNS	733

SNMP Information	734
About WINS Names	739
Cross-Platform Questions	739
Troubleshooting Intermapper	741
Troubleshooting Intermapper Remote Access	746
Troubleshooting Intermapper DataCenter	747
Index	748
Contacting Fortra	799
Fortra Portal	799
Customer Portal	799

Welcome to InterMapper

InterMapper Server and Network Monitoring



InterMapper is a network monitoring and alerting program. It continually tests routers, servers, hubs, and other computer devices that are attached to your network. If InterMapper detects a failure, it sends notifications to one or more individuals using sounds, email, pagers, SMS text, or by running a program to correct the problem.

InterMapper includes the following components that work together to help you understand what is happening on your network:

Component	Description	For more information, see
InterMapper	The core functionality of the product that gathers data about your network and provides polling, alerting, and notifications about its operation.	<u>Using InterMapper on page 19</u>
InterMapper Flows	Uses NetFlow, sFlow, and J-Flow data to provide detailed information about the kinds of data flowing through the network.	<u>InterMapper Flows™ Overview on page 292</u>

Intermapper Data Center	Additional components that enhance Intermapper. Includes access to external authentication servers and a PostgreSQL database.	<u><i>Data Collecting and Reporting on page 617</i></u>
Intermapper Remote Access	A GUI application that allows you to view and configure your Intermapper system from any location.	<u><i>Using Intermapper Remote Access on page 345</i></u>

Getting Started

Installing and Launching Intermapper

Obtain the installation files for Intermapper from the [Support portal](#) and install it. See the *Intermapper Installation Guide* for information on installation, trial versions, and licensing..

The Intermapper installer also includes Intermapper DataCenter and Intermapper Flows. During the trial period, all three are available. After your trial license expires, you need a license to run Intermapper or Flows.

The first time you launch Intermapper, a Welcome page is displayed. Use the shortcuts on the Welcome page to guide you to the area of Intermapper that will best get you started.

Using Demo Maps

Regardless of your platform, a set of demo maps is available when you open Intermapper. You can watch the demo maps operate and experiment with them to see how Intermapper works. For more information, see [Trying Out Demo Maps](#).

Registering Your Software

After you install and run Intermapper, the License Key Required dialog is displayed. From this dialog, you can register your copy of Intermapper.

To register Intermapper:

1. From the **License Key Required** dialog, select one of the following:
 - **Enter a license key now** - if you already have a key, you can enter that key now.
 - **Request a trial license key** - if you do not have a key and want to request one. The Request Trial License window is displayed.
 - **Order now** - to purchase the product.

Requesting a Trial License

To request a trial license:

1. Click **Request a trial license key**.
The Request Trial License dialog is displayed.

2. Click **Send Request**.

Intermapper contacts to retrieve a trial key. The new key is displayed in the area shown above.

3. Click **Register**.

The Register InterMapper Server dialog is displayed.

The license shows the registered name, type of license, and the number of devices and other licenses associated with the key.

4. Click **Register**.

The license key is registered.

Entering Multiple Licenses

You can enter multiple serial numbers to unlock additional Intermapper functionality. The Registration pane in the Intermapper Server Settings window shows the licenses that are currently registered.

To enter multiple licenses:

Click the Registration tab and select one of the following options to add, delete, or view your license information:

- **+** - to add a new license or serial number.
- **-** - to remove the selected license or serial number.
- **i** - to view detailed information about the selected license or serial number.

Intermapper Control Center

Use the Intermapper Control Center to start and stop the Intermapper and Intermapper Flows servers and perform other basic configuration tasks.

On macOS systems, Intermapper installs a Menu Bar Application that provides a summary of Intermapper's status, allows you to start and stop the Intermapper daemon, opens the Intermapper Control Center, and starts Intermapper.

On Microsoft Windows systems, Intermapper installs an icon in the System Tray (lower right corner) that allows the same functions. Click the icon to open the Intermapper Control Center or right-click it to view a menu similar to the macOS menu bar application. You can also view Intermapper's status from either the menu or the Control Center window.

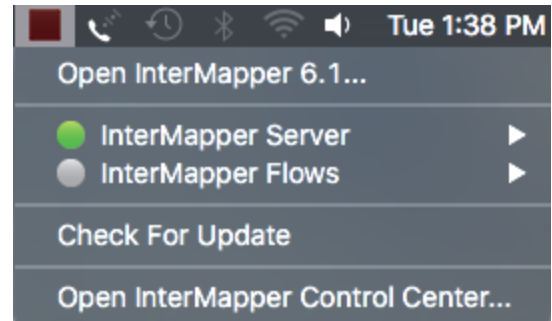
The System Tray Icon and Menu Bar Application are available only on the machine hosting the Intermapper server.

macOS

The menu bar application includes an icon that reflects the most serious state of InterMapper. When the server is not running, the InterMapper program icon is displayed. The icon can be green, yellow, orange, or red, depending on the server status.

The menu bar application can also do the following:

- Open InterMapper.
- Start or stop the InterMapper server daemon.
- Open the InterMapper Control Center.
- Check for software updates.



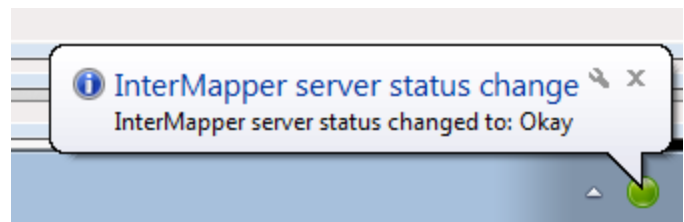
The InterMapper Server Status window displays the server name and version, as well as the current state of the InterMapper server. This window also allows you to start or stop the InterMapper server or open InterMapper.

Microsoft Windows

- Right-click the system tray icon to view the menu shown above.
- Click the system tray icon to view the InterMapper Control Center, shown below.

The InterMapper Control Center application is available on [supported Microsoft Windows systems](#).

It has the same function of the macOS application, but is called from the System Tray (lower right corner of the screen).



You can do the following from the InterMapper Control Center:

- Specify whether the Microsoft Windows balloons appear when map status changes.
- Start and stop the InterMapper or Flows services.
- Open InterMapper.

- Specify whether to automatically check for software updates.
- Manually check for software updates.

You can do most of these same functions from the context menu that appears when you right-click the Intermapper status icon.

NOTE: When you stop or start a service from the Intermapper Control Center, the states of those services are maintained when you restart the machine.

Opening the Intermapper Control Center

macOS Systems

- From the Intermapper menu, click **Open Intermapper Control Center**.
The Intermapper Control Center dialog is displayed.
Click **Now** to open the **Fortra portal** (<https://support.fortra.com/products-and-downloads/downloads/>).
- On the **Intermapper 6.6 is available for download** dialog, click **Yes**. The Fortra portal is displayed.

Microsoft Windows Systems

- Right-click the Intermapper Control Center icon in the System Tray and select **Show Intermapper Control Center**.
The Intermapper Control Center dialog is displayed.
- Click **Check Now** to open the **Fortra portal** (<https://community.fortra.com/products-and-downloads/downloads/>).
- On the **Intermapper 6.6 is available for download** dialog, click **Yes**. The Fortra portal is displayed.

Automatic Update Notifications

Intermapper can automatically check to see if a new version is available for download. This check is performed at startup and again every 24 hours.

After the first run of the check, Intermapper displays a dialog that allows you to disable the automatic checking. At any time, you can disable the feature, either by selecting **Edit > Preferences > Behavior > Version Updates** or by opening the **Intermapper Control Center**. When a new version is available, a message is displayed that includes a link to the new version.

When you first start up Microsoft Windows version of Intermapper, a message is displayed that asks if you want Intermapper to check for new versions. This is the only time it asks this question. If you answer Yes, the check is performed at startup and again every 24 hours.

To enable or disable automatic update checks:

1. Open **Intermapper Control Center**.
2. Select or clear the **Automatically check for updates to Intermapper** check box.

When a newer version of the software is available, a dialog is displayed that indicates that a newer version is available. From the dialog, you are prompted if you would like to download the new version.

3. Click **Yes** to launch a browser with the URL to the new version.

Installing Intermapper Flows

Consider the following before installing Intermapper Flows:

- Intermapper Flows is installed automatically with Intermapper. For more information, see [Installing and Launching Intermapper](#).
- If you are running a trial version, Intermapper Flows is fully operational. After your trial expires, an Intermapper Flows license is required.
- Remove any firewalls on the selected UDP ports for NetFlow. The default port is 2055.

NOTE: The Intermapper Flows service/daemon might not start if another program is using port 2055 (or whatever port you have designated for netflow packets). Stop or uninstall other netflow packages on the system.

- Configure one or more Flows exporters to send data to the Intermapper Flows server. Intermapper Flows automatically detects the exporters and begins data collection. Many switches and routers can be configured to export Flows data.

Intermapper Quick Tour

Try the following with Intermapper to familiarize yourself with the interface and its capabilities. Learn how to create maps, make maps attractive, send alerts, make charts, and so on. See [Intermapper User Guide](#) for more information.

1. Try out demo maps.

When you install Intermapper for the first time, a set of demo maps is installed. From the Welcome page, click **Try Out The Demo Maps** and take a couple of minutes to try the steps listed in the help text. When you are finished, click **Disable This Map**. You can disable the demo map from the Enabled Maps pane of the Server Settings window.

2. Build maps.

There are several ways to build maps. You can use the Autodiscovery functionality, manually enter addresses, and import a file. Try the following:

- **Autodiscovery** Intermapper can scan a network to find devices
 - Create a new map by clicking **File > New map**. Name the map (for example, Local Network) and click **Next**.
 - Check the **Autodiscovery** button in the window and click **Next**. The Autodiscover window is displayed.
 - Enter a starting point address (the default value is fine) and click **OK**. You can also specify a range of addresses to scan.
 - Autodiscovery begins. Let the query process or click **Cancel** in the top of the map to stop the scan.
 - **Manual Entry** allows you to add devices manually by typing or pasting a list of DNS names or IP addresses into the window.
 - Create a new map, name it **North America**, and click **Next**. Click **Manual Entry > Next**. The Add Device(s) window is displayed.
 - Type **www.fortra.com** and **www.example.com**. Click **Add**. Note that they appear as devices (rectangles) and turn green a few moments later. (Intermapper is already testing them.)
 - Add a background image to the map by dragging the **NorthAmerica.jpg** from the **Hands-on Extras** folder to the map window.
 - Click **Window > Zoom window** to resize the map to the image.
 - Drag the rectangles to the desired location on the background map.
 - **Create top-level map** allows you to create a top-level map that indicates the most serious condition of a sub-map. You can add icons to the Local Network and the Unalakleet sub-maps on the North America map.
 - Open the **North America** map and position it and the **Map List** so you can see both windows.
 - Drag the **Unalakleet** icon from the **Map List** to the **North America** map.
 - Drag the **Local Network** map icon to the **North America** map.
 - Double-click the **Local Network** icon on the top-level **North America** map to drill down. This opens the Local Network map.
3. **Make attractive maps.** The following techniques are available for making the maps look more attractive or to convey more information:
- **Drag items around** to match your network configuration. Lines between devices are displayed to show interconnections.
 - **Add a background image** to position devices as needed. Drag a PNG, JPEG, or GIF image into the map window to add it or click **Edit > Map Settings**.
 - **Select different icons and shapes for devices** to select new icons for the devices by clicking **Format > Icon**.

- **Change labels on devices** The label is the text that appears in or next to the icon on the map. To edit a device label, click **Format > Label** or type **Ctrl Cmd-L**.
 - **Arrange devices on the map** Click **Format > Arrange** to display available options.
 - **Align command** The **Format > Align** (Ctl/Cmd-Shift-K) command aligns items vertically and/or horizontally.
 - **Add a link between devices** Select two devices and click **Insert > Add link** or type **Ctrl Cmd-E**.
 - **Connect multiple devices to a point** Select the devices and click the **Attach to** context menu. Lines are drawn and are applied to the next object that you click.
4. **Probes for Various Servers** In addition to pinging them, Intermapper can monitor dozens of devices and display their special characteristics. Right-click or control-click, or click **Monitor > Set Probe**, to select the probe for one or multiple selected devices. You can also select one of the following:
- **Automatic** This probe uses either Pings or SNMP queries to monitor the device. If the device speaks SNMP, Intermapper uses the SNMP Traffic probe to query the device. If not, Intermapper pings the device and report if it ever goes down.
 - **SNMP Traffic** The SNMP Traffic probe monitors traffic on routers, switches, and so on. It works with nearly all networks from different vendors.
 - **Network Devices** There are many probes for monitoring various other equipment, such as Cisco, Apple, APC and other UPS vendors, and other equipment.
 - **Servers-Standard** Standards-based servers, such as mail, web, LDAP, Radius, DNS, and so on.
 - **Servers-Proprietary** Vendor-specific probes for Apple, Barracuda, Big Brother, FileMaker, Lotus, and so on.
 - **Miscellaneous** Nagios, legacy probes, and probe bundles for wireless and other gear.
5. **Alerts and Notifications** Intermapper can place a device into one of five states: OK, Critical, Warning, Alarm, or Down. Each time the device goes into a new state, Intermapper can trigger a notification or alert.
- **Create Notifiers** Notifiers are like a robot that watches a device and performs some action to send an alert when it changes its state. Click **Edit > Server Settings** and scroll to the **Notifier List** at the bottom. Add an email notifier for yourself.
 - **Examine various notification types** Mail, pager (analog modem and SNPP), command line, trap, group, or syslog.
 - **Look at schedule** Alerts are only triggered during the selected schedule, otherwise they are ignored.

- **Attach a notifier to a device** To attach a notifier, click **Monitor > Device Notifiers** and select the states that you want to trigger a notification for.
6. **Acknowledgment** After alerts and notifications are sent, you probably want to set those problems aside so you can detect new ones. Acknowledging a device changes its icon blue (to indicate that it has been acknowledged). The device is still down, but its blue color shows that someone is looking into it. Acknowledging also helps you know who is working on the problem. Each time you acknowledge a device, you can enter an acknowledgment message in the Event log. This contains the login name of the person who acknowledged it.
 - **Monitor > Acknowledge...** (Ctrl/Cmd-') This does the following:
 1. Stops subsequent repeated notifications.
 2. Logs the message to the Event Log file, along with the name and IP address of the person who acknowledged it.
 3. The icon stops blinking and turns blue to indicate that it has been acknowledged and that someone is working on it.
 - **Basic acknowledgment** Only for duration of that state
 - **Timed** For the next *n* minutes, hours, or days
 - **Indefinite** Until canceled
 7. **Dependencies** Intermapper suppresses notifications if a device is unreachable because of another failure. Intermapper supports automatic dependencies and it follows the links from the vantage point through the map to the failed device. If there is an outage on that path, Intermapper will not send notifications for the dependent device.
 - **Automatic** Intermapper follows the links from the Vantage Point.
 - **Set the Vantage Point** - only one per map
 8. **Charts** View the history of selected variables.
 - **Open a status window for a device.**
 - **Tear off window** by dragging outside.
 - **Click an underlined value** to create new chart.
 - **Drag another underlined link** to add it to an existing chart.
 9. **Edit > Server Settings** The server settings shows the preferences for a server.
 - **Per server** Use the **Edit > Server Settings**.
 10. **Intermapper Remote Access** Allows you to do all of the above, but from anywhere on the Internet
 - **Connects to multiple servers** at remote locations
 - **Works through firewall** at client/remote site. You select the port.
 - **SSL Encryption** is the default. You can install your own SSL certificate.

Using Intermapper

You experience Intermapper through the [Map List Window](#), where you view a list of available maps. When you open a map, it appears in a [Map Window](#).

If you are using [RemoteAccess](#), you might be viewing more than one map list in the Map List window, one for each server.

You can customize Intermapper by defining [Helper Applications](#) and by specifying what actions should be taken when you [double-click an object on a map](#). You can also set [user preferences](#) for Intermapper and Intermapper RemoteAccess.

Creating Maps

Use this section to find out how to [start your map](#), to [use Autodiscovery](#) to find and map each device on your network, and to manually [add devices](#) and [networks](#). After you are familiar with what maps are and how you can use them, you can add devices to your map by [importing them](#). You can also [export data from maps](#) for use in spreadsheets and databases.

You can [place a physical map image in the background](#) of your map and [use geographic coordinates](#) as you import to place devices automatically in specific locations in relation to the background image.

Use Intermapper's [different probe types](#) to query your devices in specialized ways to give you more accurate information about the device states.

As you become more familiar with what Intermapper can do, you can [add networks](#) and [scan them](#). You can [create sub-maps](#), allowing you to view large networks through an overview map and drill down to see more details

Arranging Your Map

After you create your map, you can [rearrange devices into logical groups](#), [change the appearance of devices](#), change the [device labels](#), [add text](#), or add a [background image](#). For maps with large switches, you can [hide some detail](#). For tips on arranging your map, see [Arranging Tips](#).

Notifiers and Alerts

You can [set up devices to alert you to problems](#) in a number of ways. When a device goes into the specified state, a notifier is triggered and alerts you to the problem.

You can [create your own notifiers](#) and [configure them](#) to send an [Email message](#), page (through a modem or [network](#)), [send a text message](#) to a cell phone, or [execute a script or system command](#). You can also [open a WinPopup window](#) on a Microsoft Windows system, [send an entry to a Syslog server](#), or [send an SNMP trap](#).

You can attach notifiers in the following ways:

- For each map, you can [define a default set](#) of notifiers to be attached to a device.
- You can [attach one or more notifiers](#) to one or more specific devices.
- You can create [groups of notifiers](#) and assign them to a device.
- You can [attach a notifier to one or more interfaces](#) on a device.

If a device goes down and other devices are attached to that device, you can [set a Vantage Point](#). Intermapper can then determine that the attached devices are dependent on the down device, and will not send notifications for those devices.

Network Monitoring

Intermapper begins polling devices as soon as you create your map. A lot of information is immediately available by viewing the [Status window](#) for a device, network, or link. You also view and edit a device or network information from the [Info window](#). For routers, switches, and other devices with interfaces, you can view status or other information about specific ports through the [Interfaces window](#).

You can set thresholds for a number of statistics:

- For devices, you can set thresholds for [packet loss](#) or [network traffic](#), and Intermapper alerts you when a behavior is out of range.
- For links, you can set thresholds Error, Link Utilization, and Interface Discards.
- You can set default thresholds the server, a map, or a device.

You can [create charts](#) that graph one or more data values associated with a device. You can also [view a detailed Event log](#) and [Outage log](#) to help you accurately troubleshoot problems. You can also [create new log files](#) for logging specific data.

If a device or link goes down, you can [acknowledge the problem](#), which prevents Intermapper from sending notifications. There are several options for acknowledging problems that allow you to control the resumption of notifications after acknowledgment.

You can [collect data from devices](#) and save it in the [Intermapper Database](#), through the Intermapper DataCenter. The data can be retrieved for reporting and analysis. You can [set policies](#) to specify how much data is retained and how long it is retained.

Server Settings

Use the [Server Settings panel](#) to view [information about Intermapper](#), to [set preferences](#), and to [configure](#) Intermapper's [Remote](#), [Web](#), [Telnet](#), and [Authentication](#) servers. You can also maintain Intermapper's [firewall](#) and [user](#) list, [enable and disable](#) or [control access to maps](#), and [create notifiers](#).

Intermapper Reference

Use Intermapper Reference to view comprehensive lists of [menu commands](#), details about the available [device probes](#), [file and folder locations](#), and learn [advanced data import and export techniques](#). You can also learn how to use and customize the [Intermapper web server](#) and how to use the [Intermapper Telnet server](#).

Troubleshooting Intermapper

Use the Troubleshooting section to help you learn about [IP addresses](#), [Domain Name Servers](#), [SNMP](#), [WINS Names](#), and view a number of frequently asked questions.

Using Intermapper

You experience Intermapper through the [Map List Window](#), where you view a list of available maps. When you open a map, it appears in a [Map Window](#).

If you are using [RemoteAccess](#), you might be viewing more than one map list in the Map List window, one for each server.

You can customize Intermapper by defining [Helper Applications](#) and by specifying what actions should be taken when you [double-click an object on a map](#). You can also set [user preferences](#) for Intermapper and Intermapper RemoteAccess.

Creating Maps

Use this section to find out how to [start your map](#), to [use Autodiscovery](#) to find and map each device on your network, and to manually [add devices](#) and [networks](#). After you are familiar with what maps are and how you can use them, you can add devices to your map by

[importing them](#). You can also [export data from maps](#) for use in spreadsheets and databases.

You can [place a physical map image in the background](#) of your map and [use geographic coordinates](#) as you import to place devices automatically in specific locations in relation to the background image.

Use Intermapper's [different probe types](#) to query your devices in specialized ways to give you more accurate information about the device states.

As you become more familiar with what Intermapper can do, you can [add networks](#) and [scan them](#). You can [create sub-maps](#), allowing you to view large networks through an overview map and drill down to see more details

Arranging Your Map

After you create your map, you can [rearrange devices into logical groups](#), [change the appearance of devices](#), change the [device labels](#), [add text](#), or add a [background image](#). For maps with large switches, you can [hide some detail](#). For tips on arranging your map, see [Arranging Tips](#).

Notifiers and Alerts

You can [set up devices to alert you to problems](#) in a number of ways. When a device goes into the specified state, a notifier is triggered and alerts you to the problem.

You can [create your own notifiers](#) and [configure them](#) to send an [Email message](#), page (through a modem or [network](#)), [send a text message](#) to a cell phone, or [execute a script or system command](#). You can also [open a WinPopup window](#) on a Microsoft Windows system, [send an entry to a Syslog server](#), or [send an SNMP trap](#).

You can attach notifiers in the following ways:

- For each map, you can [define a default set](#) of notifiers to be attached to a device.
- You can [attach one or more notifiers](#) to one or more specific devices.
- You can create [groups of notifiers](#) and assign them to a device.
- You can [attach a notifier to one or more interfaces](#) on a device.

If a device goes down and other devices are attached to that device, you can [set a Vantage Point](#). Intermapper can then determine that the attached devices are dependent on the down device, and will not send notifications for those devices.

Network Monitoring

Intermapper begins polling devices as soon as you create your map. A lot of information is immediately available by viewing the [Status window](#) for a device, network, or link. You also view and edit a device or network information from the [Info window](#). For routers, switches, and other devices with interfaces, you can view status or other information about specific ports through the [Interfaces window](#).

You can set thresholds for a number of statistics:

- For devices, you can set thresholds for [packet loss](#) or [network traffic](#), and Intermapper alerts you when a behavior is out of range.
- For links, you can set thresholds Error, Link Utilization, and Interface Discards.
- You can set default thresholds the server, a map, or a device.

You can [create charts](#) that graph one or more data values associated with a device. You can also [view a detailed Event log](#) and [Outage log](#) to help you accurately troubleshoot problems. You can also [create new log files](#) for logging specific data.

If a device or link goes down, you can [acknowledge the problem](#), which prevents Intermapper from sending notifications. There are several options for acknowledging problems that allow you to control the resumption of notifications after acknowledgment.

You can [collect data from devices](#) and save it in the [Intermapper Database](#), through the Intermapper DataCenter. The data can be retrieved for reporting and analysis. You can [set policies](#) to specify how much data is retained and how long it is retained.

Server Settings

Use the [Server Settings panel](#) to view [information about Intermapper](#), to [set preferences](#), and to [configure](#) Intermapper's [Remote](#), [Web](#), [Telnet](#), and [Authentication](#) servers. You can also maintain Intermapper's [firewall](#) and [user](#) list, [enable and disable](#) or [control access to maps](#), and [create notifiers](#).

Intermapper Reference

Use Intermapper Reference to view comprehensive lists of [menu commands](#), details about the available [device probes](#), [file and folder locations](#), and learn [advanced data import and export techniques](#). You can also learn how to use and customize the [Intermapper web server](#) and how to use the [Intermapper Telnet server](#).

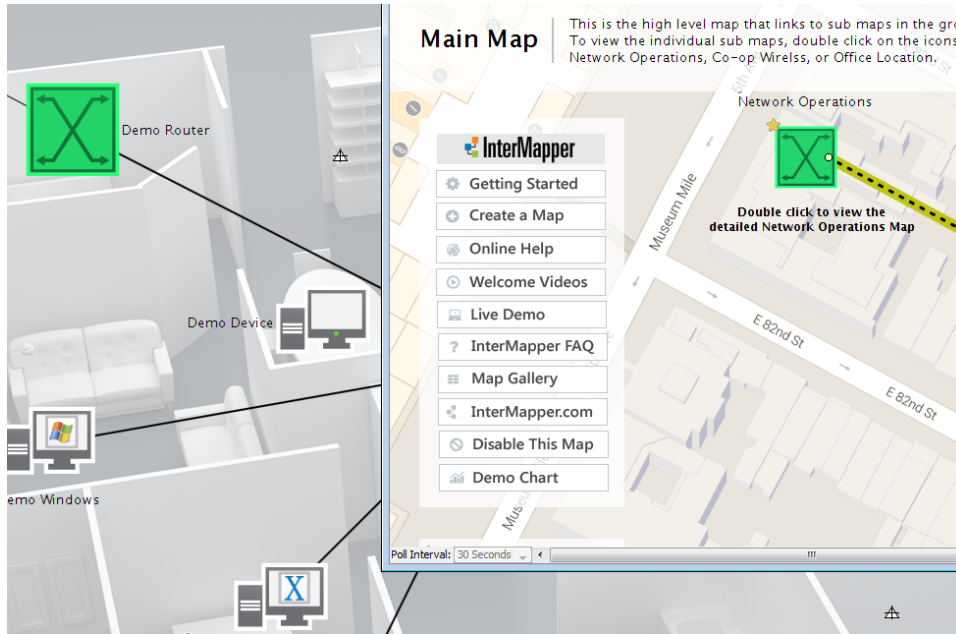
Troubleshooting Intermapper

Use the Troubleshooting section to help you learn about [IP addresses](#), [Domain Name Servers](#), [SNMP](#), [WINS Names](#), and view a number of frequently asked questions.

Trying Out Demo Maps

The first time Intermapper launches, the Demo Map file is opened to show simulated network activity such as outages, high traffic, and other problems that you might see in a real network.

The following image shows a portion of an example map with devices (rectangles) that are connected by links (lines).



The following describe the items on the map:

- Devices are displayed in **green** to indicate that the device is up and running.
- Devices that cannot communicate with Intermapper are displayed in **blink red**.
- Click and hold a device to see a status window of detailed information and outage history, or right-click or Ctrl-click it and select **Status Window** from the menu.
- You can **tear off** status windows to keep them open by dragging the mouse outside their boundary.
- Different **sounds** indicate that there are failures. (Intermapper can also send email or pages.) To silence these alarms, click **Preferences** from the **Edit** menu, click the **Sounds** subcategory of the **Behavior** category and clear the **Play sound notifications** check box.
- Lines (**links**) show **dotted lines (ants)** when traffic exceeds a threshold
- Links are displayed in a **yellow or orange background** when traffic exceeds 50% or 90%.

- **Circles at the ends of links** (they look like raindrops in puddles) indicate errors that have been detected by the interface.
- **Circles close to the device** indicate receive errors.
- **Circles close to the network** indicate transmit errors.
- **Click and hold on a link** to see a status window of port and interface information and traffic statistics or **Right/Ctrl-click** it and select **Status Window** from the menu.

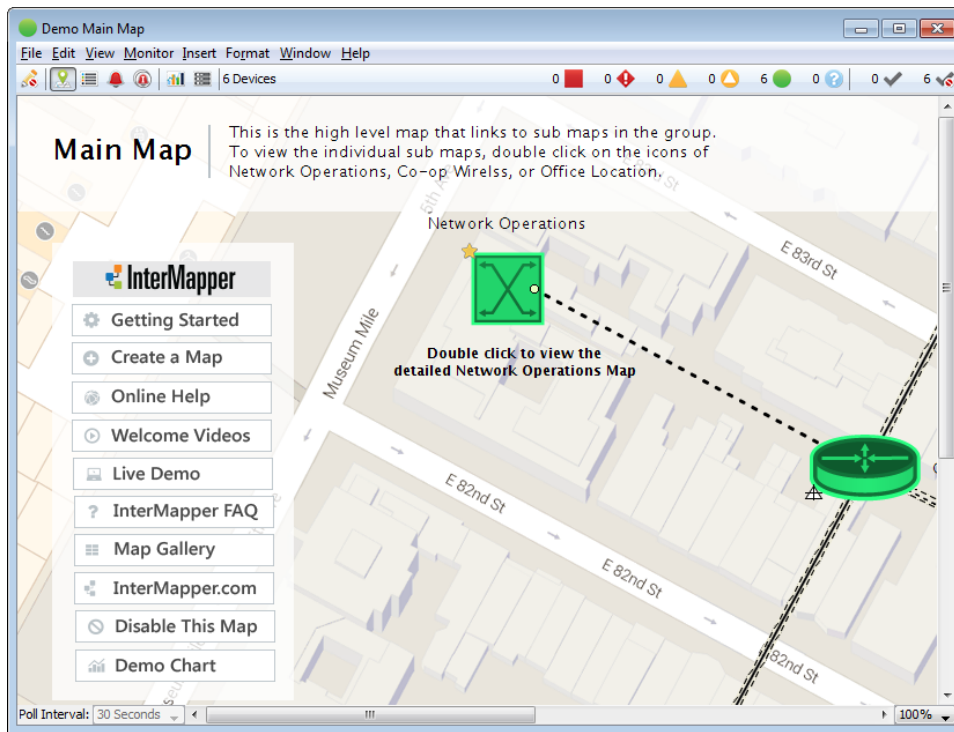
In addition, note the following on the map as it operates:

- Some devices become dim from time-to-time because they shadowed by another failure on the map. The shadowed devices depend on all devices in the path to it. Intermapper can automatically detect this state and avoids notifying the network manager about outages if the dependent devices are unreachable because of the other failure.
- On several of the demo maps, a star appears on a device to indicate the Vantage Point for shadowing. Intermapper suppresses notifications for a device if it cannot reach the device from the Vantage Point without going through a failed device. (It is in the shadow of a failed device.)

Map Window

You can view any map in a Map window. The following example shows maps installed with Intermapper.

For an in-depth explanation of the elements that appear in the map window, what they mean, and how to use them, see [Monitoring Your Network \(Pg. 154\)](#).



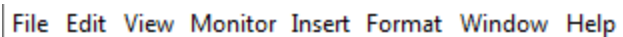
Title Bar

The Title bar shows the map's title, state, and standard controls for zooming, minimizing, and closing the window.



Menu Bar

The Menu bar contains the map menus.



For more information on each menu, see the [Command/Menu Reference \(Pg. 348\)](#).



Toolbar

The Toolbar contains buttons to toggle the edit mode and to switch from one view to another.



Switching Between Monitor Mode and Edit Mode


Click the Lock button at the left end of the tool bar to switch the map between Monitor mode and Edit mode:

	In Monitor mode - The map is not editable and status windows appear when you click and hold a device, link, or network.
	In Edit mode - The map is editable. Status windows can be opened with menu commands.

Tip: Press **Tab** to switch between Monitor and Edit modes.

Switching Views in the Map Window

Click one of the following buttons to switch to a different Map Window view:

	Map view - Shows the map graphically, showing devices, networks, and their interconnections.
---	---



List view - Shows the devices on the map as a list, with columns for the device status, name, address, probe type, and current and previous condition.

- Select columns and sort as described in [**Choosing and Sorting Columns in List Views**](#) on page 29 below.
- Drag items from one map to another. The source map must be in the List view. The target map must be editable, but can be in any view.
- Sort by Status to see the most serious conditions appear at the top of the list.
- Alt-click or Cmd-click (Mac) a value in the **Poll Interval** column and select a new value to set all devices to the same poll interval.

NOTE: You can also view a global list of devices.

To view a global device list:

- With a server selected in the map list, select **Device List** from the Map List Window menu. A list of all devices on the selected server is displayed.



Device Notifiers view - This view allows you to see which notifiers are attached to each device on a map. Another way to think of it is as a responsibilities view - what devices does a certain notifier apply to.

- Select a notifier from the menu. You can see the checkboxes for all recipients.
- To set a value for all devices, Alt-click or Cmd-click (Mac) to set a value. The value changes to the selected value for the entire column. This works for all check boxes, **Delay**, **Repeat**, and **Count** columns.
- To see and edit all notifiers, select **Edit Notifiers** from the Notifier menu.
- Select columns and sort as described in [**Choosing and Sorting Columns in List Views on page 29**](#) below.



Link Notifiers view - This view allows you to see which notifiers are attached to interfaces on a map.

- Attach notifiers to interfaces in exactly the same way as in the Device Notifiers view.
- Alt-click or Cmd-click (Mac) a check box to set the notifier status for all links to the same value.
- Select columns and sort as described in [**Choosing and Sorting Columns in List Views on page 29**](#) below.



Chart view - Shows the list of charts for the map.

- Expand the tree to view a chart's datasets.
- Double-click a chart name to open the chart.
- Right-click the Chart List button to open a chart without switching the view.
- Right-click a chart to do one of the following:
 - Show the chart
 - Rename the chart
 - Delete the chart
- Right-click a dataset to do one of the following:
 - Show the chart containing that instance of the dataset
 - Show the device generating the dataset
 - Raise the status window for the device generating the dataset
 - Rename the dataset
 - Remove the dataset
 - Export data from the dataset
 - Delete data from the dataset
- Select columns and sort as described in [**Choosing and Sorting Columns in List Views**](#) on page 29 below.



Dataset view - This view shows the datasets available for charting and data collection in this map. With the map in edit mode, you can choose a retention policy for any dataset.

This view shows the following:

- A list of devices on the current map.
- The dataset name, type, and current retention policy and variable for a selected device.
- Available interfaces and associated datasets.
- Select columns and sort as described in [**Choosing and Sorting Columns in List Views**](#) on page 29 below.

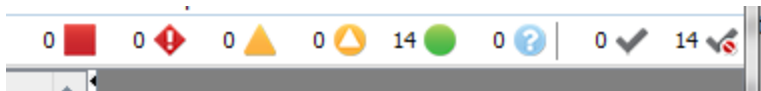
Choosing and Sorting Columns in List Views







Use the **Choose/Sort** menu (Click ⚙️, upper right corner of the list) or the **Columns** and **Sort** menus in the **View** menu to select which columns you want to view and the order in which you want to sort the list.




- Select or clear a check box from the **Choose/Sort** menu in the upper right of the window or pane to **include or exclude a column**.
- Use the **Sort** submenu to **select the column you want to sort by**.
- Click a column heading to **sort by that column**.
- Click again to **sort in reverse order**.
- Use the **Columns** submenu in the **View** menu to **select the columns you want to view**.
- Use the **Sort** submenu in the **View** menu to **select the column you want to sort by**.

Map Legend

The Map legend to the right of the toolbar shows the different states of the map and the number of devices in each state. It also acts as a filter in list view.



Badge	Color	Meaning
	Red (Flashing)	Down - No response has been received from the device within the specified timeout period.
	Red (Solid)	Critical - The specified threshold for the critical state has been met.
	Orange	Alarm - The specified threshold for the alarm state has been met.
	Yellow	Warning - The specified threshold for the warning state has been met.
	Green	Up - The device is working below the specified thresholds.
	Gray	Unknown - The device is not being polled, so its state is unknown.

	Purple	Searching - The device is searching for adjacent routers (during auto-discovery) or is tracking unnumbered interfaces.
		Acknowledge - Timed or Indefinite - The problem has been acknowledged and notifications are suppressed, either indefinitely or for a specified period of time.
		Acknowledge - Basic - The problem has been acknowledged, and notifications are suppressed until the device comes back up, at which time the checkmark is cleared. List Acknowledged Devices - (Filter button) Lists all devices that have been acknowledged.
		List Un-Acknowledged Devices - (Filter button) Lists all devices that have not been acknowledged.

- Click a legend icon to view a list of devices that are currently in that state.
- Click the icon again to return to the previous view.
- Shift-click icons to view devices in more than one state.

Example: Shift-click the Alarm and Warning icons to see devices in either of those states.

- Click one of the Acknowledge Filter buttons (to the right of the legend) to list acknowledged or un-acknowledged devices.

NOTE: The filter buttons work with the legend icons. Clicking a Filter button shows only the devices in the selected state that are acknowledged or un-acknowledged. It is possible to click a filter button and see no devices.

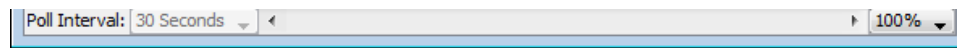
Map Area

The Map area is the canvas on which you create your map. To get started, look at [Creating Maps for information on starting your map \(Pg. 41\)](#). The Creating Maps section provides information on [creating \(Pg. 41\)](#), [arranging \(Pg. 79\)](#) and making your map look [just the way you want \(Pg. 79\)](#) it to look. You can also find a quick reference of [editing shortcuts \(Pg. 1\)](#).

For an in-depth explanation of the elements that appear in the map window, what they mean, and how to use them, see [Monitoring Your Network \(Pg. 154\)](#).

Status Bar

The Status bar contains controls for switching in and out of map edit mode, setting the polling interval, and zooming in and out of the map.



<p>The Poll Interval menu sets the polling interval for the map.</p>	<p>Poll Interval: 30 Seconds ▼ 30 Minutes ▲ 20 Minutes 10 Minutes 5 Minutes 2 Minutes 1 Minute 30 Seconds ▼</p>
<p>The Map Zoom menu sets the zoom factor for the map. If you select Auto, the map zooms automatically when you resize the window.</p>	<p>100% ▼ 100% ▲ 125% 150% 175% 200% 225% 250% 275% ▼</p>

Map List Window

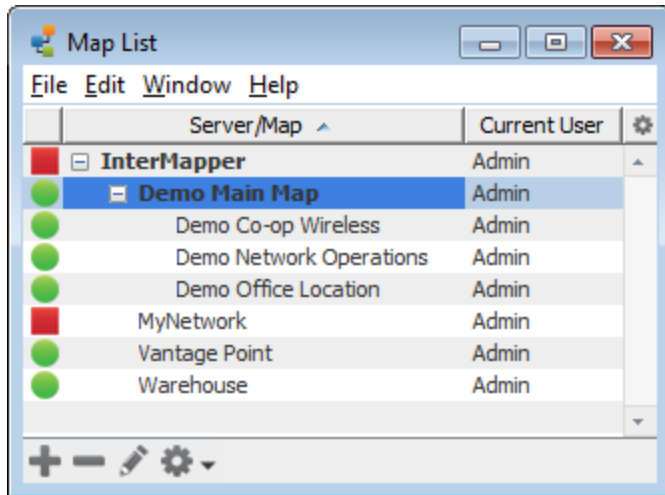
Use the Map List window as the primary interface to Intermapper.

- With Intermapper, you can control all aspects of the Intermapper server running on your local machine. You can also disable a map by right-clicking it and selecting **Disable Map**.
- With Intermapper Remote Access, you can access multiple Intermapper servers from the same machine. If you have administrator access, you can edit all server settings on a remote server. You can also disable a map by right-clicking it and selecting **Disable Map**.

The menu items available in the File menu differ slightly between Intermapper and Intermapper Remote Access. For more information, see [File Menu \(Pg. 349\)](#).

Map List Window

Use the Map List window to view a list of maps. If you have Intermapper Remote Access, you can also view a list of other available Intermapper servers, to log into one or more servers, and to view a list of maps currently running on each server.



Using the Map List Window

The following are tips for getting the most out of the Map List window:

- A green map name indicates that the map is open.
- Position the cursor over a map in the list to view its DNS Name and/or IP address, and the port on which it is listening for Intermapper Remote Access connections.
- Right-click or Ctrl-click (Mac) a map to select commands from the context menu.
- Use the Quick Menu, described below, to perform map-related commands and operations.
- Select columns and sort as described in [Choosing and Sorting Columns on page 33](#).
- Use the Columns menu to select which columns to view in the Map List window.

Quick Menu

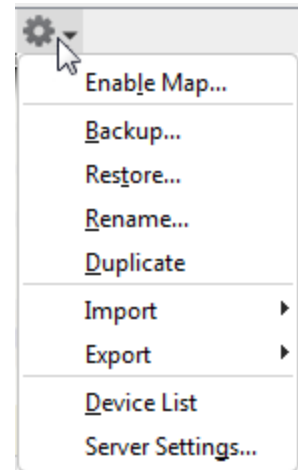
Use the following quick menus at the bottom of the map list window to access frequently used functions:



- Click the **Add** menu to add a map or server.
- Select a map and type Delete (-) to remove the map from the Map Window.

NOTE: This does not actually delete the map; it simply disables it.

- Select a server and click **Info** to view or change info about a server.
- Use the **Tools** menu to perform a number of map-related operations. You can enable and disable maps, back up, restore, or duplicate a map. You can also import or export maps and data files, as well as open the Server Settings window.



Choosing and Sorting Columns

Use the **Choose/Sort** menu (Click ⚙, upper right corner of the list) or the **Columns** and **Sort** menus in the **View** menu to select which columns you want to view and the order in which you want to sort the list.

- Select or clear a check box from the **Choose/Sort** menu in the upper right of the window or pane to **include or exclude a column**.
- Use the **Sort** submenu to **select the column you want to sort by**.
- Click a column heading to **sort by that column**.
- Click again to **sort in reverse order**.
- Use the **Columns** submenu in the **View** menu to **select the columns you want to view**.
- Use the **Sort** submenu in the **View** menu to **select the column you want to sort by**.

Arranging your Maps into Folders

You can arrange your maps into folders as shown above, using the Server Configuration > Enabled Maps pane of the Server Settings window. For more information, see [Enabled Maps \(Pg. 266\)](#).

Viewing the Global Device List

From the Map List window, you can view a list of all devices on a particular server.

To view a global device list:

With a server selected in the map list, select **Device List** from the Map List Window menu. A list of all devices on the selected server is displayed.

Device List Window

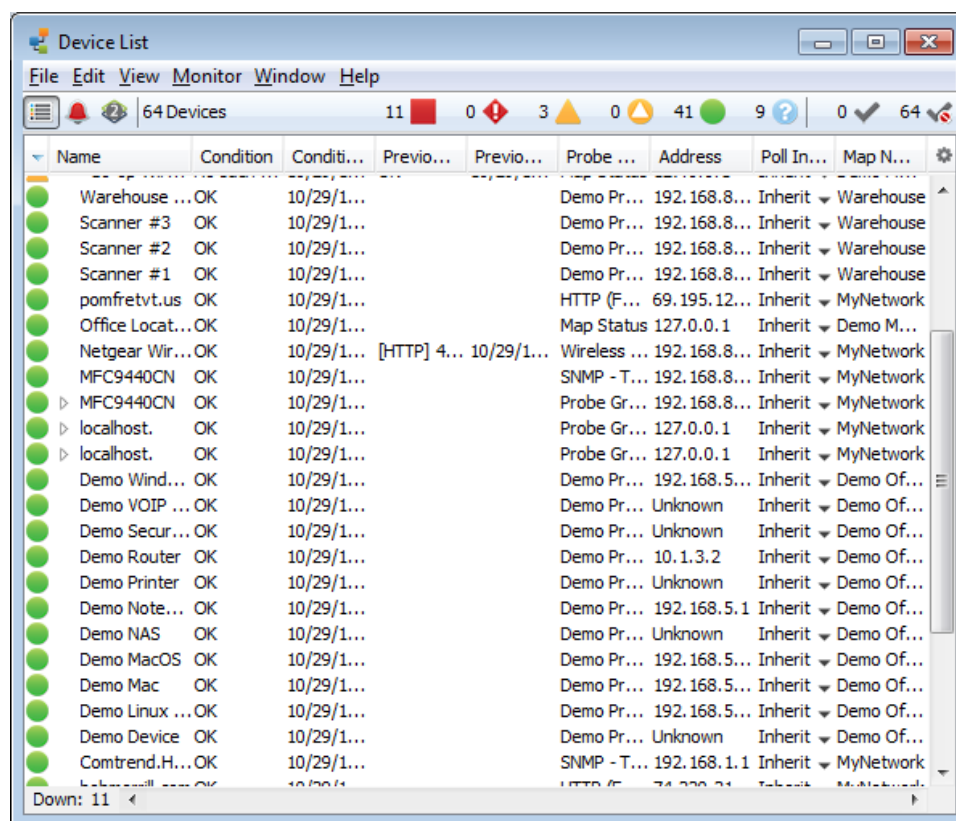
Use the device list window to view the following:

- Global list of devices
- List of notifiers
- List of Layer 2 devices

List View



Use the Device List view to see a global list of devices used in all of the maps on the Intermapper server.



Device List Columns

Status

The state of the device. The icon color matches its color in the map.

Name	The first line of the device name as shown on the map.
Condition	The most severe (worst) status of the device.
Date	When the device entered its current state.
Previous condition	The device status before it entered the current state.
Date & Time	When the device entered the previous condition.
Probe Type	The probe type of the device.
Address	The network address of the device.
Map Name	The name of the map in which the device appears.

Manipulating the Device List

You can interact with the Device List as follows:

- Double-click an entry in the Device List to switch to the proper map and highlight the device with zooming rectangles.
- Select columns and sort as described in [Choosing and Sorting Columns in the Device List Window on page 36](#).
- Resize columns by dragging the separator between the columns to the proper size.
- Reorder the columns by dragging a column to a new position in the **Device List** window.
- When the map is editable, use the menu in the **Poll Interval** column to set the poll interval for a device.
- To **set the poll interval for all devices at once**, **Alt-click** the menu in the **Poll Interval** column and select a value.

Notifier View



Use the Notifier List view to view a list of devices attached to the selected notifier and all settings for that notifier or device combination.

Using the Notifier List view, you can attach a notifier to a device or check to see which devices are attached to a given notifier. You can set delay and repeat parameters to control escalation of a problem.

- Choose a notifier from the menu.
- Select or clear the check boxes for the device states for which you want to trigger an

alert.

- Set delay, repeat, and repeat count settings for the device as needed.

Layer 2 View



Use the Layer 2 List view to view a list of switches, VLANs, and NIC manufacturers, with a list of devices connected to each.

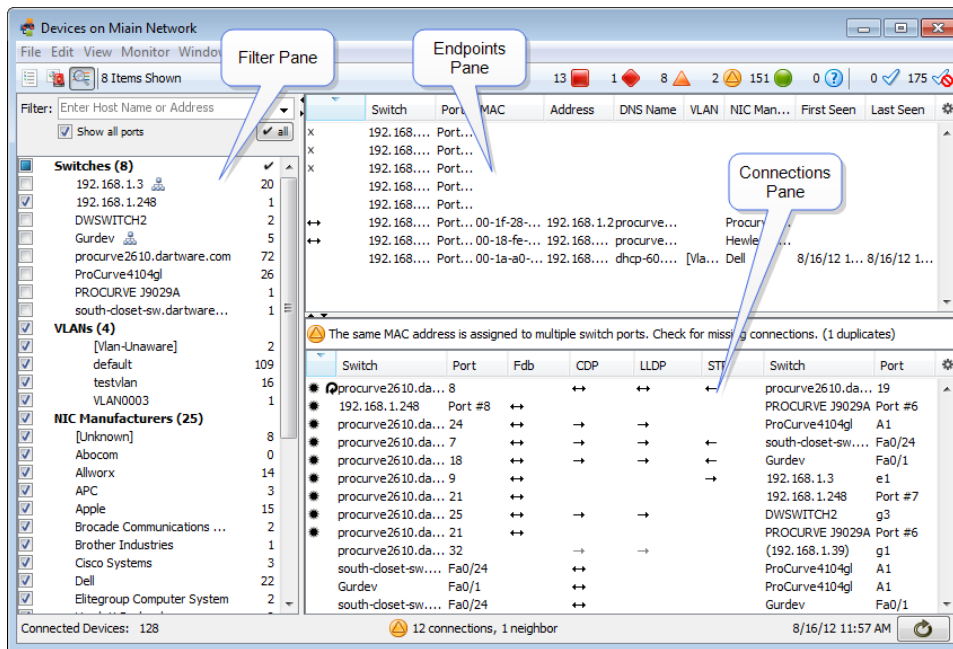
For more information on the Layer 2 view, see [The Layer 2 View](#).

Choosing and Sorting Columns in the Device List Window

Use the **Choose/Sort** menu (Click ⚙, upper right corner of the list) or the **Columns** and **Sort** menus in the **View** menu to select which columns you want to view and the order in which you want to sort the list.

- Select or clear a check box from the **Choose/Sort** menu in the upper right of the window or pane to **include or exclude a column**.
- Use the **Sort** submenu to **select the column you want to sort by**.
- Click a column heading to **sort by that column**.
- Click again to **sort in reverse order**.
- Use the **Columns** submenu in the **View** menu to **select the columns you want to view**.
- Use the **Sort** submenu in the **View** menu to **select the column you want to sort by**.

Layer 2 View



The Layer 2 View contains the following panes:

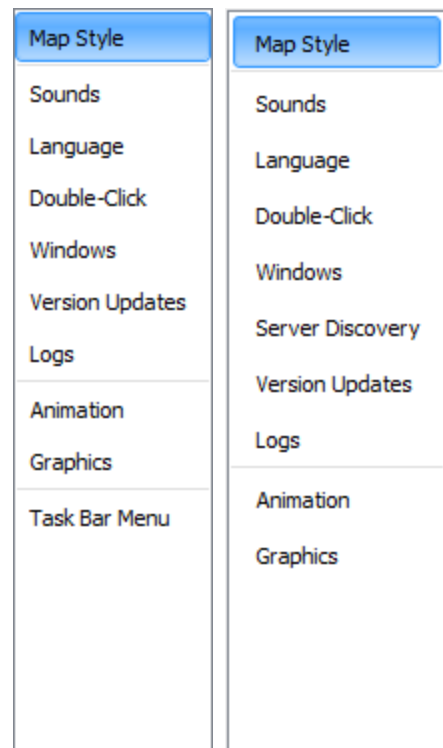
- **Endpoints pane** - the upper-right pane lists all switch ports and the devices connected to them. It contains only those ports and devices that match the filter criteria in the Filter pane.
- **Filter pane** - the left pane provides criteria for showing or hiding endpoints based on their presence on a particular switch, VLAN, or the endpoint's manufacturer. It also lists available switches, the VLANs in which they appear, and manufacturers of network interface cards of the devices connected to them. Use the check boxes to select or hide endpoints in the Endpoints pane and type additional criteria to help select the endpoints to view.
- **Connections pane** - the lower-right pane provides details about switch-to-switch connections.

Intermapper User Preferences

Use the **Preferences** command, available from the Edit menu, to set user preferences for the Intermapper user interface. These settings affect only the copy of the Intermapper or Intermapper Remote Access you are running; it does not affect other user settings.

To view and edit Intermapper's preferences:

1. From the **Edit** menu, click **Preferences**. The Preferences window is displayed.
2. In the left pane, click the name of settings you want to change. If necessary, expand a section to view the more settings. The selected settings panel is displayed in the right pane.



Map Style

Use the Map Style panel to set your preference for the style in which your maps are displayed.

- **Use three-dimensional map style** - (selected by default) Select this check box to use the current three-dimensional display style, with gradient colors, rounded rectangles, and status icons.
- **Display the following status badges on devices** - select or clear the check boxes for the badges you want to appear on devices. By default, the Ok badge is not selected, but all other badges are.

Intermapper

Remote Access

Sounds

Use this panel to enable or disable sound notifications. Select or clear the **Play sound notifications** check box to turn sounds on or off.

Language

Use this panel to specify the language you want Intermapper to use in the user interface.

To change the language from the system default, select your language from the Language Options menu. All available language options are listed.

NOTE: You must restart Intermapper or Intermapper Remote Access to apply your changes.

Double-Click

Use this panel to specify the default action to take for a device or network that does not have an action assigned. Use the **Action** dropdown menu to choose from these options:

- **Helper App** - Select a helper application to launch.
- **Open URL** - Type a URL in the **Action** text box.
- **Built In** - Select an Intermapper menu command from the menu tree. By default, the Info window is displayed.

Windows

Use this panel to specify whether charts and status windows are hidden when a map becomes inactive. You can also reset the state of Ignored windows.

- **Hide charts and status windows when Map is inactive** - Select this check box to hide charts and status windows for any map that is not the Active window. If the box is not selected, all open charts and status windows remain open.
- **Reset Ignored Windows** - A number of alert messages provide the option not to show the message again. Click this to reset the state of all ignored windows.
- **Customizing Status Windows** - Status windows can be modified with customized font names/sizes and background colors.

Status Windows

You can change the background color, font, and size of a status window. Color changes are immediately applied. Font changes are applied to the next status update or when you close and reopen the status window.

Font Name:

Font Size:

Background:

Preview: Device Status

Server Discovery (Intermapper Remote Access Only)

Use this panel to specify whether or not to search for Intermapper servers on the local LAN.

Discover Intermapper Servers on the LAN - Select this check box if you want Intermapper Remote Access to search for Intermapper servers on the local LAN.

Version Updates

Use this panel to enable or disable the Automatic Update function by selecting or clearing the **Automatically check for updates** box and select **Daily**, **Weekly**, or **Monthly** from the menu. This function is also available from the [Intermapper Control Center](#). To check for updates immediately, click **Check Now** on the Intermapper Control Center.

Logs

Use this panel to control the amount of information saved in the server log and whether to save it to disk.

- **Log Line Count** - Specify the number of lines of the server log that appear in the Debug, Event, or Outages Log window. This can reduce the amount of memory required to display a log window.
- **Client Debug Log** - Select the **Store Client Debug Log on disk** check box to save the debug log to your local disk.

Animation

Use this panel to specify the animation settings. Faster animation looks better, but might use more CPU power than you want if you are running a slower CPU or have very large maps.

- Select or clear the **Display Animations** check box to turn animations off or on. (They are off by default.) This turns off traffic indicators (ants) and transition effects (scale changes, scrolling to found devices, effects when windows opening or closing, and so on).
- **Animation rate** - Select an animation rate by moving the slider left for slower rates or right for higher ones. The selected rate appears in the upper right above the slider.

Graphics

Use this panel to control how graphics are rendered.

Use the **Anti-aliasing** controls to smooth the jagged look of diagonal and curved lines. Some users find that anti-aliased text or lines are blurry or fuzzy. Select or clear the check boxes to apply anti-aliasing to text or graphics.

NOTE: The Anti-aliasing settings are hints to help the graphics system render the graphics. The settings might be ignored by some systems.

Use the **Image Scaling** slider to choose level of quality to use when viewing maps at a zoom level other than 100%. The selected algorithm can affect application performance.

Use the **Label Coloring** section to control the appearance of built-in shapes (rectangle, oval, cloud, and wire). For these objects, the outline is colored, but label text is black or white for contrast. To set the label text to the same color as the outline color for built-in shapes, select the **Use Outline color for Label Text on Built-in Shapes** check box.

NOTE: Deselect the object to see the effect of the **Label Coloring** change.

Task Bar Menu (Intermapper only)

Use this panel to specify whether to show a task bar icon for the Intermapper Control Center.

Show status in task bar - Select this check box to show the status icon in the task bar (Microsoft Windows) or menu bar (macOS).

Creating Maps

Starting Your Map

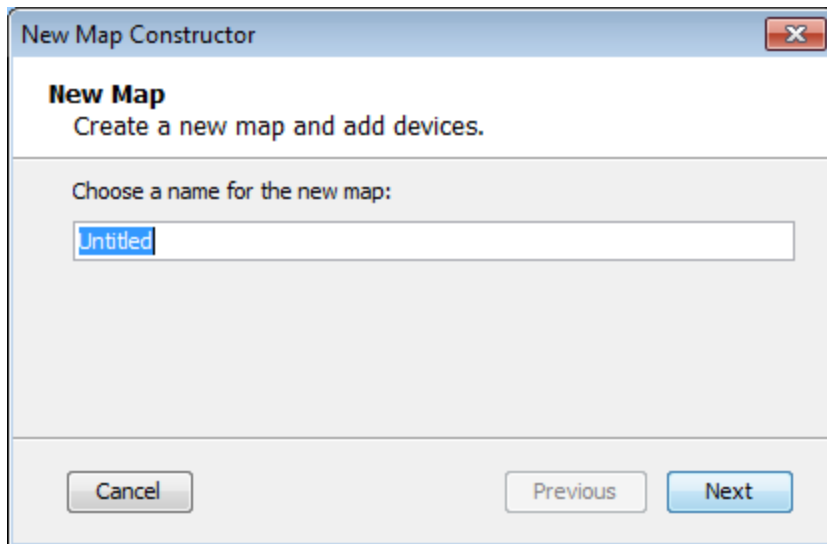
When you launch *Intermapper*, a Map List window is displayed. It contains several demo maps, which show examples of network maps and contains brief descriptions of the elements appearing on the maps. Double-click a map to open it.

After you explore the demo maps, you can use the Auto-discover function to create your first map.

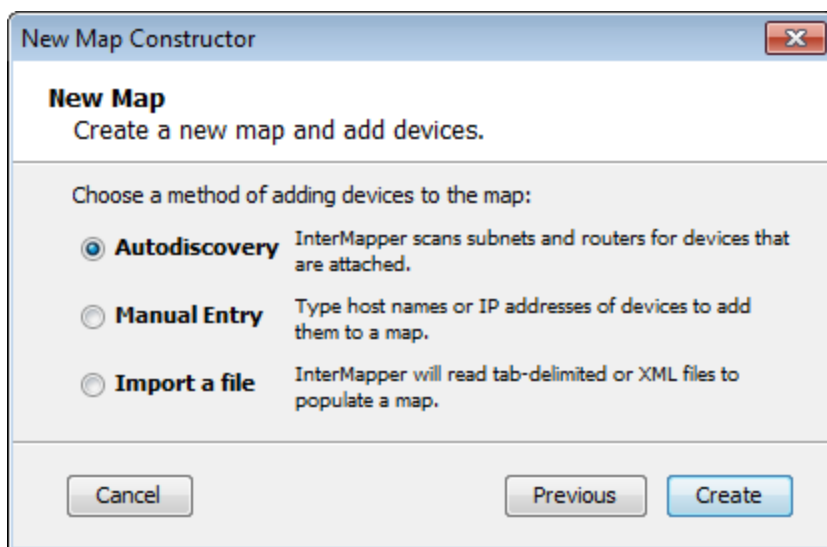
Creating a New Map

To create a new map:

To create a new map, choose **New Map** from the File Menu. The New Map Constructor window is displayed.



Type a map name and click **Next**. The second page of the New Map Constructor is displayed.



- **Autodiscovery** - Intermapper's Auto-discover function automatically scans your network, looking for network devices to add to your map. It uses several heuristic techniques (including SNMP probes, ICMP echo packets, and DNS and NBP queries) to discover all devices that are present. It then places those devices on a map.
- **Manual Entry** - Type or paste a list of host names or IP addresses for the devices you want to add to the map.
- **Import a file** - Specify a tab-delimited, CSV, or XML import file. For more information, see [Importing Data Into Maps \(Pg. 631\)](#).

For information on using the Auto-discover function, see [Using Auto-discover \(Pg. 43\)](#).

Importing Data into a Map

You can also create a map by importing data from a text file. For more information, see [Importing Data Into Maps \(Pg. 631\)](#).

Intermapper Labels

Intermapper adds a label to each discovered device. By default, it uses the device full DNS name. Networks are labeled with both an IP addresses and the number of bits in the subnet mask (indicating the network range). For example, the network labeled 192.168.1.0/24 indicates that the IP devices are in subnet 192.168.1.0, with a subnet mask of 24 bits (255.255.255.0).

NOTE: You can change a device label using the **Label** command, which is available in the [Format menu \(Pg. 385\)](#).

Using Auto-Discovery

You can use Auto-Discovery to create a new map. Auto-Discover scans your network and creates an IP-based, Layer 3 view of the map.

NOTE: If your network contains Layer 2-enabled switches, you can also use Layer 2 information to increase the accuracy of a map's representation of your network topology once the devices have been discovered.

For more information, see [Mapping With Layer 2](#).

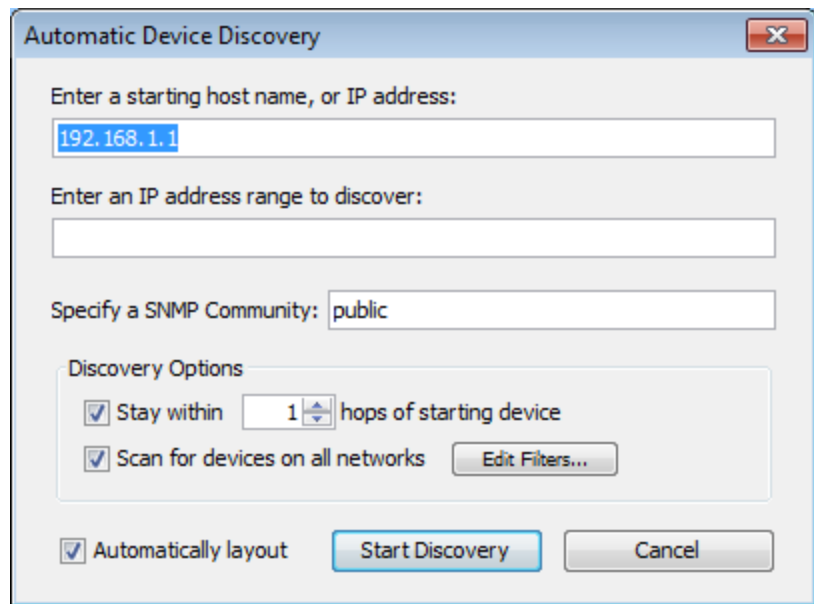
For existing maps, you can use the [manual technique](#) to convert the map. For new maps created with Auto-Discovery, use the [automatic technique](#).

To use Auto-Discover to create an initial network map:

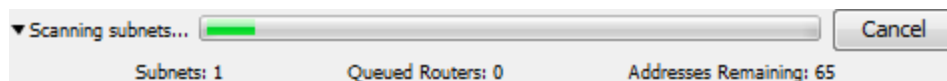
1. From the **File** menu, select **New**. The New Map Constructor window is displayed.
2. Type a map name and click **Next**.
3. Select **Auto-discovery** and click **Create**. The Automatic Device Discovery window is displayed.

4. In the **Enter a starting host name, or IP address** text box, type or paste the host name or IP address you want to use as the starting point for auto-discovery. A name is suggested for you. It is the DNS name or IP address of a router, or if there is no router, the computer Intermapper is running on. Accept the default or type any of the following:

- A DNS name
- An IP address (if you want to create a map of another part of a network.)
If you type a name or address of an SNMP-speaking router, Intermapper draws interconnections to other routers in the network more quickly.



5. To discover a range of addresses rather than all addresses, type them in the **Enter an IP address range to discover** text box. Use hyphens, wildcards, and CIDR slash notation to specify an IP address range. For more information, see [Entering an IP Address Range](#).
6. If you have SNMP-speaking devices in your network, type an [SNMP Community \(Pg. 734\)](#) string in the **Specify an SNMP Community** text box.
7. Select your **Discovery Options**, as explained in [The Auto-Discovery Window \(Pg. 45\)](#) below.
8. Click the **Filter** button to set a filter for the discovery.
9. Click **OK** to start the Auto-discovery process. A Discovery Status bar is displayed. The status bar shows progress statistics for subnets, queued routers, and addresses remaining to be scanned.



10. As the network is scanned, discovered devices appear in the current map (or in a list if you cleared the **Automatically Layout** check box). When Intermapper finds all devices within the specified subnet, the Discovery Status bar disappears.



Click the Map View button near the upper left corner of the Map window to view your network as a map, showing devices and networks as icons, with the interconnections between them.

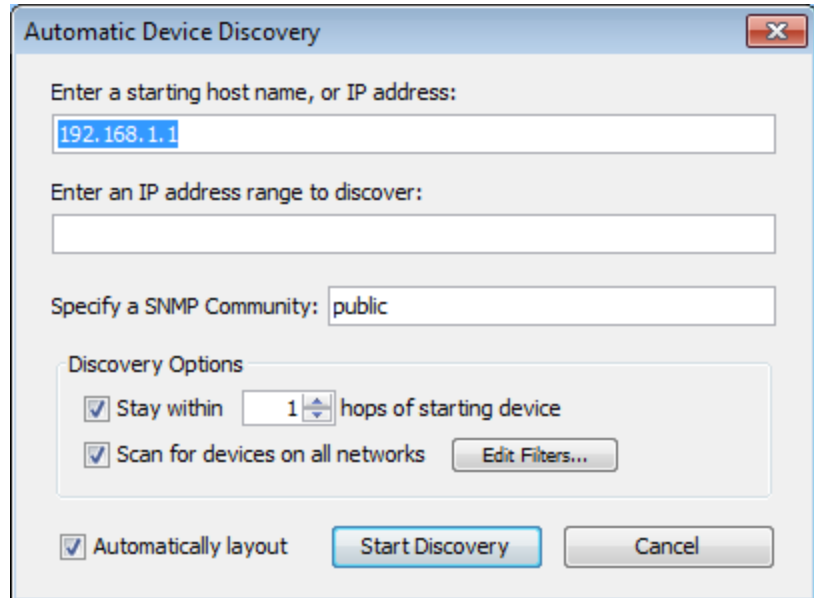
To stop the auto-discovery process:

Click **Cancel** to stop the discovery process and to avoid adding new devices or networks. All devices added before you stop the process remain in the list.

Automatic Device Discovery Window

You control the starting point, the [SNMP Community string \(Pg. 734\)](#), the breadth of the network search, and the kinds of devices that are automatically added to the map using the Automatic Device Discovery window.

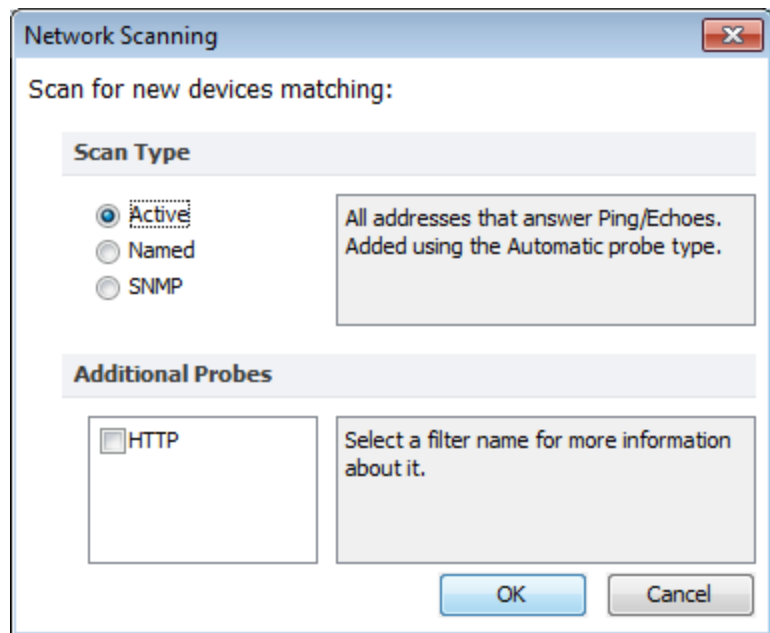
- **Starting host name** - The [DNS name \(Pg. 733\)](#), [IP address \(Pg. 730\)](#), or [WINS name \(Pg. 739\)](#) of a device to use as a starting point for the auto-discovery.
- **IP Address Range** - Use hyphens, wildcards, and CIDR slash notation to specify an IP address range.
- **Specify an SNMP community** - The SNMP read-only community string to be used to interrogate all devices. (Intermapper attempts to read SNMP information using the specified community string. It is set to public by default.
- **Stay within *NN* hops of starting device** - Stops autodiscovery after Intermapper searches the specified number of hops from the starting device.
- **Scan for devices on all networks** - Specify the device kinds to automatically add to the map. Select the check box or click **Edit Filters** to open the Network Scanning window.
- Click **Automatically layout** to allow Intermapper to automatically lay out the map.
- Click **Start Discovery** to initiate a scan of the specified host.



Network Filter Dialog

Select one of the following the filters you want to use to add devices to the map:

- **Active** - Intermapper performs a complete IP address scan for each network. A device is added for each IP address that responds.
- **Named** - Each IP address in the subnet is looked up in the DNS. If a corresponding name is present, the device is added to the map.
- **SNMP** - Intermapper sends an SNMP GetRequest to each address in the range. Any device that responds is added to the map and uses the SNMP Basic Traffic probe. If the device does not respond to SNMP, the probe is set to Ping/Echo.
- **HTTP** - If the device responds to an HTTP request, an HTTP probe is added to the device (along with SNMP Basic Traffic or Ping/Echo probe), and the device becomes a [probe group](#).



What Happens During Auto-Discovery?

During auto-discovery, Intermapper attempts to discover all devices on a network, based on the IP address and SNMP string provided. It does this by querying the router and ARP tables. Then, using any scan filters specified in the Network Scanning window, it scans all attached subnets, mapping all devices it finds, until it reaches the hop count specified in the **Discovery Options** section of the Automatic Device Discovery window. It then performs the following processes concurrently and iteratively until the specified limits are reached:

- If Intermapper discovers an SNMP speaking router, it attempts to discover the interfaces the router has and what other routers are connected to those interfaces. Intermapper then queries each of the discovered routers for their connected networks and begins auto-discovery on each network.
- For each network or subnet discovered, Intermapper pings every address on that subnet to find more active or named devices.
- When Intermapper finds a device, it uses several techniques to characterize it. For example, it sends SNMP queries (with the specified SNMP community strings) to determine what kind of device is present.

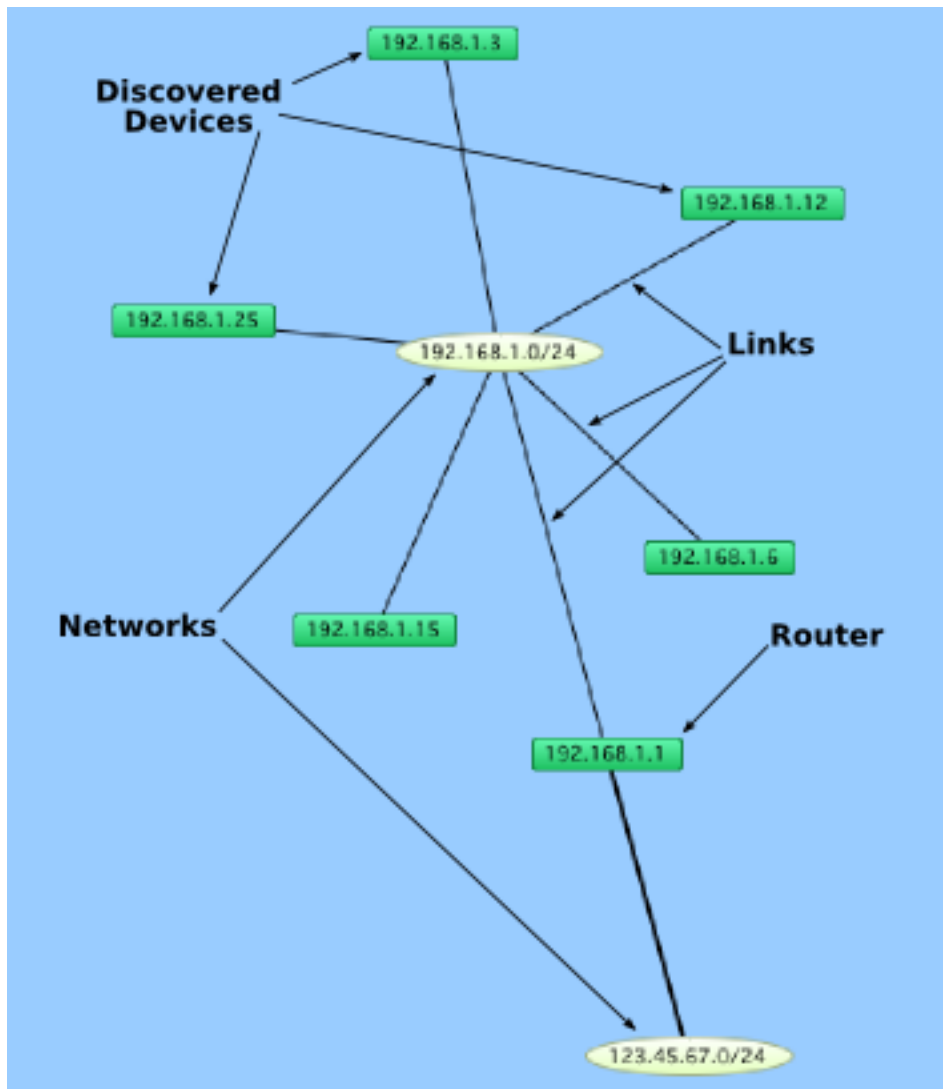
WARNING: In auto-discovery mode, Intermapper might ping or query every device address on a subnet. If your network has an intrusion detection system, autodiscovery might trigger intrusion alarms. Be sure to check with the network manager before using this feature.

NOTE: It might take a long time to perform auto-discovery on a large subnet (a Class A or B subnet). Intermapper limits its auto-discovery queries to two per second so that it does not overload any networks. Therefore, it takes about 32,000 seconds (just under 10 hours) to completely scan the class B subnet (with 65,535 addresses).

To create your maps more quickly, you can type or paste one or more host [DNS names \(Pg. 733\)](#), [IP addresses \(Pg. 730\)](#), IP address ranges, or [WINS names \(Pg. 739\)](#) in the Add Devices window (Insert menu). (WINS names must be preceded by "\\".) Intermapper immediately adds them to the map and connects them to the proper network.

You can also import a list of devices from a text file. For more information, see [Importing Data Into Maps \(Pg. 631\)](#).

The following is a typical map after auto-discovery is complete:



Entering an IP Address Range

You can enter IP address ranges in several ways, depending on what you need to do. These ranges are useful for configuring access in the Intermapper firewall, as well as for autodiscovery.

Valid Characters

- Use hyphens (-) to separate high and low values.
- Use wildcards (*) to indicate a full range of values.
- Use slashes (/) to enter a range in [CIDR](#) notation.

Examples

- **Address range using hyphens**
 - **192.168.1.1-31** - specifies any device in the range 192.168.1.1 to 192.168.1.31.
 - **192.168.1-10.1-10** - specifies in subnets 192.168.1.* to 192.168.10.* and finds addresses between 1 and 10 within each subnet.
- **Address range using "*" wildcards**
 - Each wildcard corresponds to a range of 0-255.
 - **192.168.1.*** -equivalent to 192.168.1.1-255.
 - **192.168.*.*** - class B range.
 - ***.*.*.*** - all addresses.
- **Address range using wildcards and hyphens**
 - **192.168.1-10.*** - finds 255 addresses in each of 10 subnets.
 - **192.168.*.1** - finds address #1 in each of 255 subnets.
- **Address range using [CIDR](#) ("slash") notation** defines length in bits. This is often referred to as prefix length or prefix bits.
 - **192.168.0.0/24** - equivalent to 192.168.0.* Class C.
 - **192.168.0.0/16** - equivalent to 192.168.*.* Class B.
 - **192.168.1.128/25** - equivalent to 192.168.1.128-255.
 - **example.com/24** - the last 255 addresses at example.com (Class C)
 - **example.com/25** - 126 addresses beginning with either 1 or 129, depending on the value of the last octet of the IP address for example.com.

Manually Adding Devices

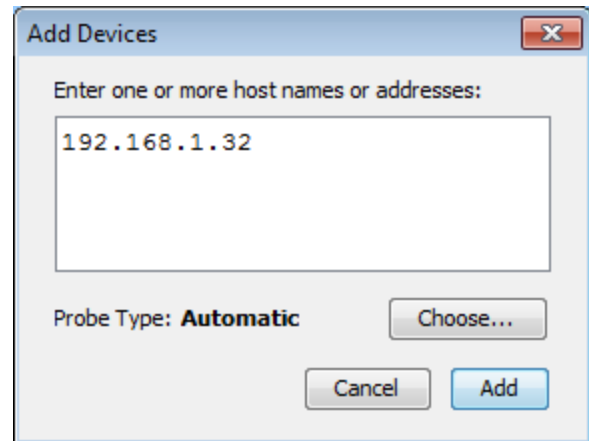
Add devices to your map manually using the **Device** command in the Insert menu or the **Add Device(s)** command in the context menu.

To manually add devices:

1. Make sure the map is in **Edit** mode.
2. From the **Insert** menu, select **Device** or right-click or Ctrl-click in the window and select **Add Device(s)** from the **Context** menu. The Add Devices window is displayed.
3. Enter the device names and/or addresses.
4. The device(s) are monitored with the specified probe. To select a different probe type, click **Choose** and select a probe as described in [Select Probe Window \(Pg. 50\)](#).
5. Click **Add**. All devices entered are added to the map.

NOTE: If you enter a DNS name, the device is added to your map only if a DNS entry can be found.

- **Enter one or more host names or addresses** - Enter individual host names or addresses or paste a list of DNS names, IP addresses, or WINS names into this window. Entries must be separated by commas (,) or by whitespace characters, such as spaces, tabs, or carriage returns. You can copy a list of host names and addresses from a text file or from a traceroute program. You can also use [WINS names \(Pg. 739\)](#) (preceded by backslashes \). For each entry that responds, a device is added to the map.
- **Probe Type** - Shows the type of probe currently assigned to the device. Click **Choose** to open the Select Probe window and choose a different probe.
- Click **Add** to add the devices to the map.



Add Device(s) window.

NOTE:

If any of the device names cannot be resolved (if a device name is not configured in your domain name system server) or if a device cannot be tested with the selected probe, you can still correct the entry.

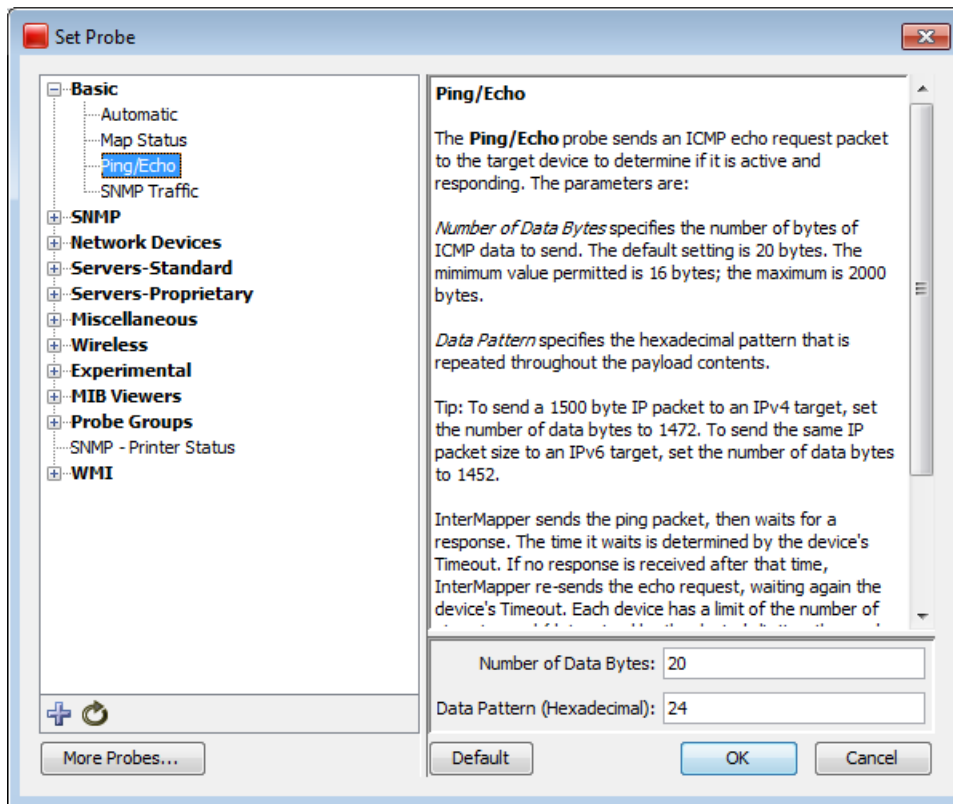
NOTE: IPv6 To ensure that when possible, host names are resolved to IPv6 addresses rather than IPv4 addresses, enclose the host name in [square brackets]. For example, [myserver.example.com].

Set Probe Window

Use the **Set Probe** command, available from the Monitor menu, the device's context menu, or by clicking **Choose** from the Add Device(s) window, to view the Select Probe window. From this window you can select and configure the probe for selected devices.

- The left pane contains a hierarchical list of probes, divided into sections and subsections.
- The right pane shows the description and configuration options for the selected probe.



For a comprehensive list of probes with descriptions, see the [Probe Reference \(Pg. 409\)](#).



To choose and configure a probe:

1. **Choose a section** - In the left pane, click the plus sign (+) to expand the section and subsections to view the probes. Click minus sign (-) to collapse an expanded section or subsection.
2. **Choose a probe** - In the left pane, click a probe within a section or subsection to select it. The description and options for the probe are displayed in the right pane.
3. **Set the probe's options** - In the right pane, enter or select the options you want to use with the selected probe. These options vary, depending on the probe. Click **Default** to reset the probe options to the default settings.
4. Click **OK** to select the probe.

Additional Set Probe Window Actions

	Import a probe - Click this button and select from a standard file dialog to import a probe file.
	Reload probe list - Click this button to reload the list of probes found in the Intermapper Settings/Probes folder.

More Probes...

Click this button to launch your browser and view a list of probes contributed by Intermapper users.

Adding Networks to the Map

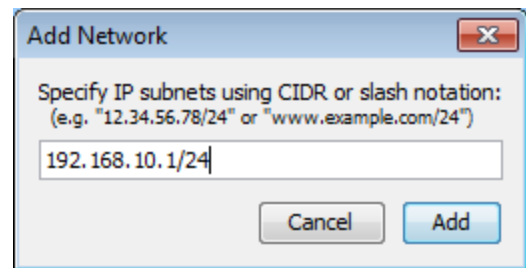
Intermapper uses network ovals to represent a subnet (a range of IP addresses). It uses these networks as graphical connecting points for all the devices on the subnet. When Intermapper places an SNMP-speaking device on a map, it automatically adds a network for each of its interfaces.

You can also manually add new networks.

To add a new network:

1. From the Insert menu, click **Network**. An Add Network window is displayed.
2. Enter the IP subnet information or range and click **OK**. For more information on IP addresses and subnets, see [About IP \(Pg. 730\)](#).

The network is added to the map as an oval, labeled with the specified network information. Devices that belong to that subnet are automatically connected to the new network.



Add Subnet window.

Enter an IP subnet (in the form of x.x.x.x/yy).

NOTE: Adding a subnet does not automatically initiate the discovery process. To scan the new network, right-click the new network oval and click Scan Network. For more information, see [Scanning a Network \(Pg. 53\)](#).

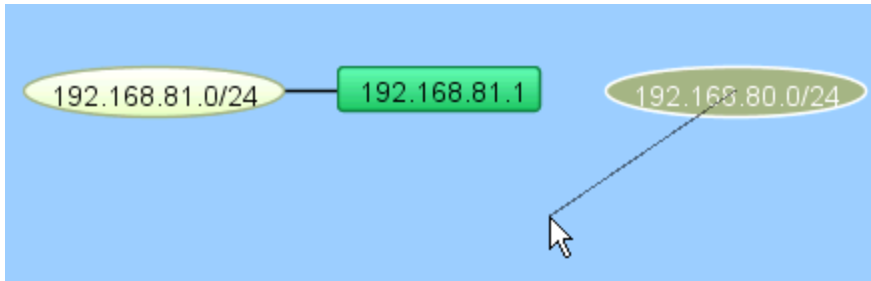
Adding and Removing Links

Intermapper might not connect devices to the proper network in every case. If this happens, you can make the connection manually.

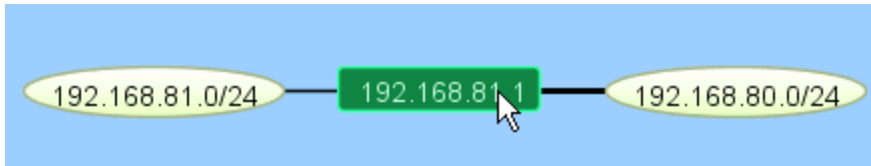
To manually add a link:

1. Make sure the map is in [Edit mode \(Pg. 154\)](#).
2. Right-click or Ctrl-click one of the objects that you want to link to another.

- From the menu, click **Attach To**. A line appears, connecting the selected object to your cursor. For example,



- Click the object you want to connect to. A link is created between the two objects. For example,



NOTE: After a manual connection has been established, Intermapper remembers it. You can drag manually-connected items around the map, and they work just like the links Intermapper that created automatically.

To remove a manually-connected link:

- Make sure the map is in [Edit mode \(Pg. 154\)](#).
- Right-click or Ctrl-click the link and select **Remove**. The link disappears.

Scanning A Network

Intermapper can scan an IP address range to discover all devices on that network. It then adds the discovered devices to the map and connects them to the proper network.

To scan a network:

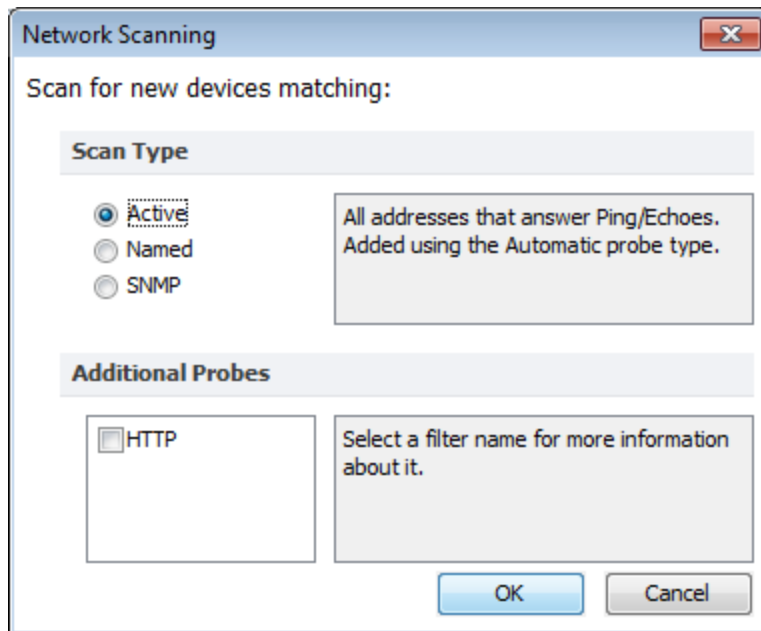
- Select a network oval and click the **Insert** menu.

or

Right-click the network oval.

- Click **Scan Network**. The Network Scanning window is displayed.
- Select a **Scan Type**.
- In the **Additional Probes** field, specify if you want to add an HTTP probe to the device (converting it to a probe group) when a response to an HTTP request is received.

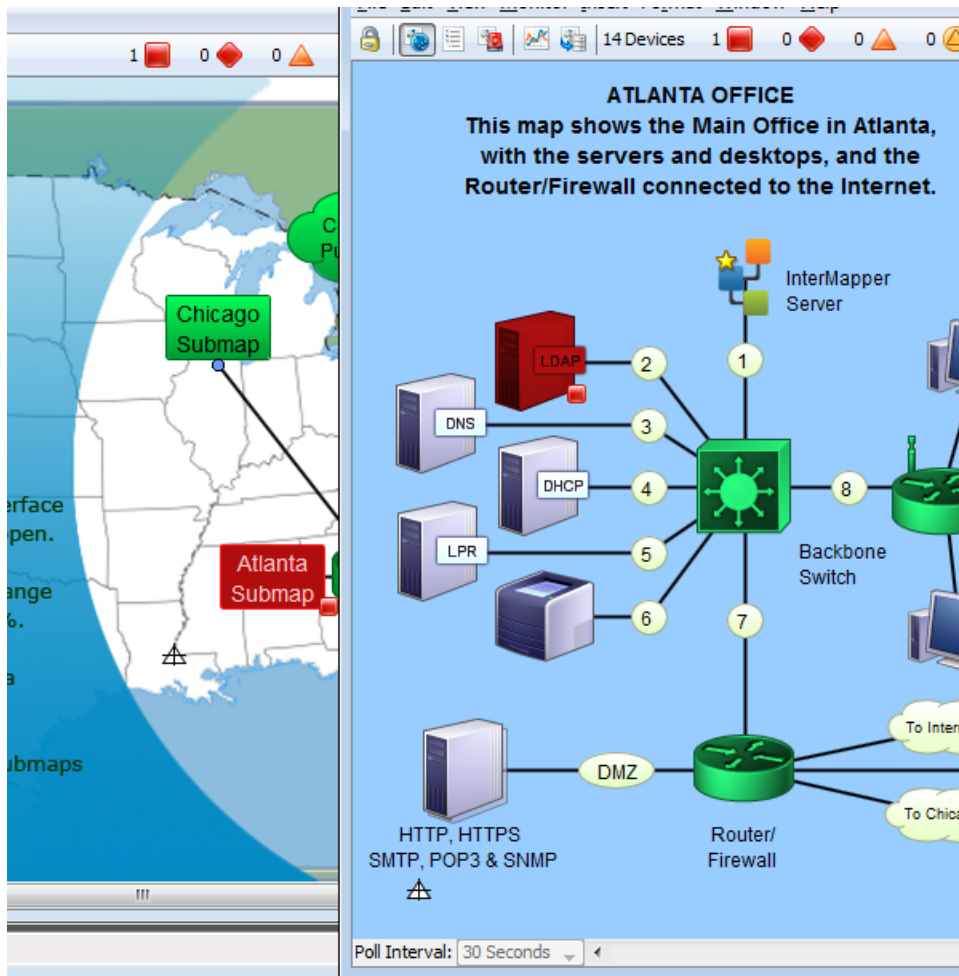
- Click **OK**. The network oval turns purple and remains that way until scanning is complete, at which time the color changes to the default network color.



Creating Sub-Maps

You can hide details by creating a top-level map that provides an overview of many individual maps. Each icon on the top-level map shows the status of another map (a sub-map). The color of the icon indicates the most serious condition on its sub-map. Sub-maps can be on a local computer or could even be on another Intermapper server.

The following example shows the Atlanta map that opens when you double-click the Atlanta icon on the National map. Notice that on the National map, the Atlanta icon is down (displayed in red). The Atlanta map shows that the LDAP server is the reason for the outage.



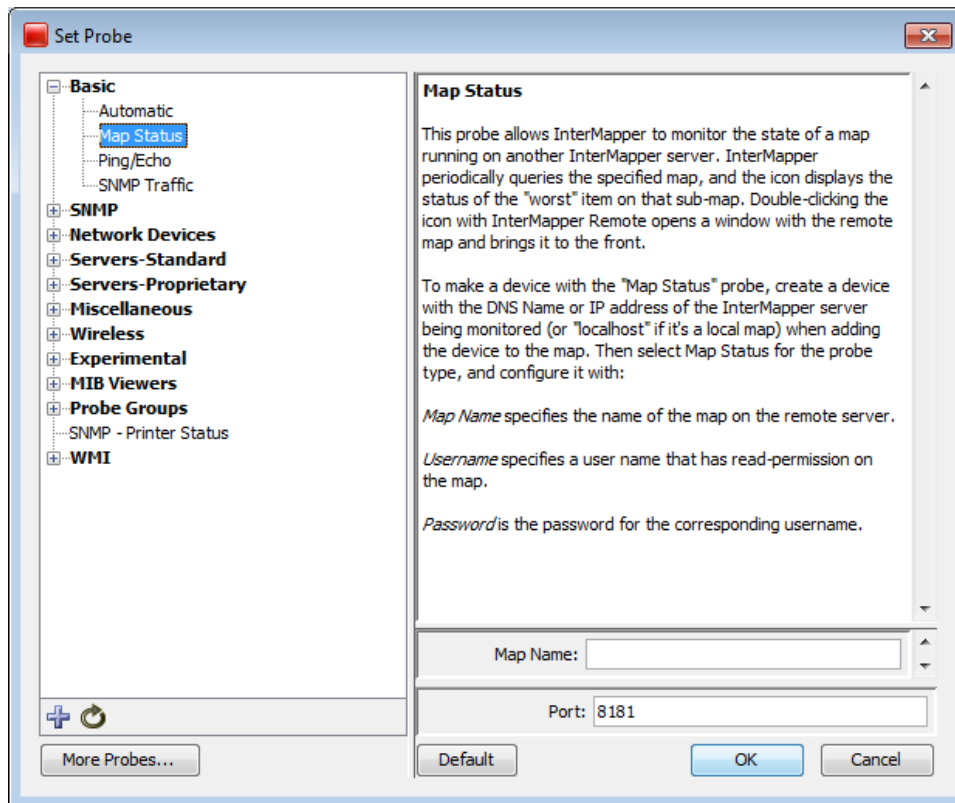
Creating a Sub-Map

Use the Map Status probe to create an icon that represents a sub-map. To do this, add a device with the address of the Intermapper server on which the map is running, (127.0.0.1 if it's on the local computer) with a Probe Type of **Map Status**.

The color of the icon for a map item using a Map Status probe indicates the most serious condition on sub-map.

To add a sub-map item to a map:

1. The easiest way to add a sub-map is to drag the desired map from the **Map List** window to the map. In certain cases, the Set Probe window is displayed with the Map Status Probe selected.
2. Click **OK** to accept the default settings. A new device is added, using the current map and user account information.



To manually add a sub-map:

1. From the **Insert** menu, select **Device**.
2. Type the [IP address \(Pg. 730\)](#), [DNS name \(Pg. 733\)](#), or [WINS name \(Pg. 739\)](#) (preceded by backslashes \\) of the Intermapper server that contains the sub-map. Sub-maps might be running on the local Intermapper server (use the address 127.0.0.1), or type the address of Intermapper running at a customer site, at a branch office, or at an international office.
3. Specify the **Port** to connect to (default is 8181).
4. From the Basic category, select **Map Status**.
5. Type the **Map Name**.

NOTE: If your map is nested in a sub-folder, you must enter the full path to the map. For example, "/MySubFolder/MyMap.map". If you add the sub-map by dragging it into the map from the Map List window, the path is entered automatically.

6. Type the **User Name** and **Password** of an account on that server. This account must have read-access to the map.

7. Click **OK**. The new icon is displayed on the map and its color reflects the state of everything on the sub-map.

To view the sub-map:

Double-click the sub-map icon. The map opens so you can see and modify (if you have been granted permission) the settings on the sub-map.

Sub-Map Best Practices

The following are best practices when setting up a map status probe:

- Use a username that has the minimum amount of privilege (read-only). Never set up a map status probe using a username that has administrative privileges.
- Use only one username per server for map status probes. Intermapper has a limit of 2 user logins per connection. If map status probes monitoring maps on a server are configured using more than one username, you might need to explicitly log out from the map status probe before you can access a map status probe that uses a different username.

For example, assume you have access to map status probes on server S, and MapB and MapC are on server S that you do not have access to. When you double-click a map status probe for MapB, the Intermapper client logs you in as user B (you are logged in twice on server S). You cannot open MapC before you log off of MapB. This restriction is only for one server, if you are using map status probes to monitor maps on multiple Intermapper servers, you can use a different username for each server.

Creating Probe Groups

Overview

Use a probe group to include multiple probes targeting the same IP address into a single icon on a map. A probe group shows the worst status among the probes in the group. A probe group counts as a single device against your license count.

NOTE: Only those devices that reference the same IP address can be added to a group.

About the Control Probe

Each probe group can contain a control probe. Setting a control probe affects the probe group as follows:

- When a control probe is defined, no notifications for the other probes in the group are sent if the control probe is down.
- The group's interfaces match those of the control probe.

When you create a group containing an SNMP probe, a control probe is automatically determined for the group. This is the first SNMP probe detected and can be changed. If there are no SNMP probes in the group, no control probe is defined. See [Setting a probe group's control probe \(Pg. 60\)](#).

How Grouped Devices are Probed

The following is how devices are probed after grouping:

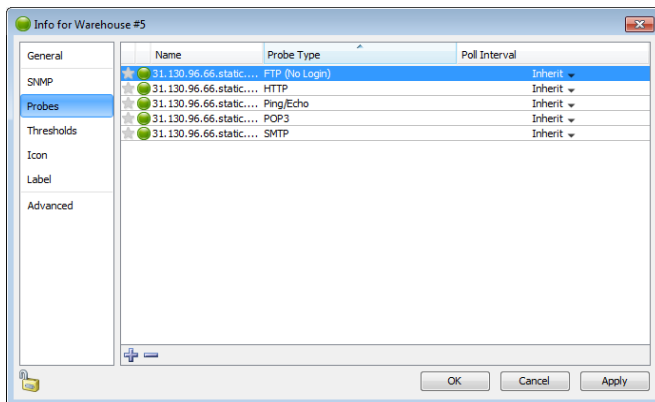
- **Each member probe is polled at its own rate, with its own settings.** The settings in place when the device is added to a probe group are used, including poll rate, attached notifiers, and probe parameters. You can edit the settings for any probe. For more information on editing these settings, see [Editing Settings for a Probe Within a Probe Group](#).
- **The device icon's state reflects the most serious condition of its member probes.** When the state of a member probes becomes the most serious state, the device icon's state changes to reflect it.
- **By attaching a notifier to the device,** you can get notifications whenever any probe in the group has a problem.
- **By attaching a notifier to a member of the group,** you can get notifications when that member probe has a problem.
- **If the control probe is down,** no notifications are sent for any other member of the group.
- **Interface information is shown** based on the selected control probe.

Use the **Group** command to create a probe group from a set of selected devices.

To create a probe group:

1. With the map editable, select the devices you want to group. All devices must use the same IP address.
2. From the **Insert** menu, select **Group**. The selected devices are replaced by a single device icon.

When you double-click the resulting device icon, the grouped probes appear in a list in the group's Info window.



Warehouse #5
66.96.130.31
Ping/Echo

Warehouse #5
66.96.130.31
POP3

Warehouse #5
66.96.130.31
SMTP

Warehouse #5
66.96.130.31
FTP (No Login)

Before grouping

Warehouse #5

After grouping

NOTE: When you group probes, the resulting group uses the first line of the first device as its label. You can change the label before or after grouping.

Creating One or More Empty Probe Groups

You can create an empty probe group and add probes to the group as needed.

To create an empty probe group:

1. From the **Insert** menu, select **Empty Probe Group**. The Add Probe Group(s) dialog is displayed.
2. For each probe group you want to add, type or paste a host name or IP address.
3. Click **Add**. A probe group icon is displayed for each entered host name or address.

Adding Devices to Probe Groups

You can add probes to a group by doing the following:

- Add an existing device to a group.
- Add a new device to a group.
- From the list view, drag and drop a device into a group.

To add an existing device to a probe group:

1. Select the group and the devices you want to add to it.
2. From the **Insert** menu, select **Group**. If all selected devices use the same IP address or host name, the selected devices are added to the existing probe group.

To add a new device to a probe group:

1. From the probe group's Info window, click the **plus sign (+)**. The Set Probe window is displayed.
2. Select the probe you want to use, set its parameters, and click **OK**. The probe is added to the group.

To remove probes from a group:

1. Double-click a probe group. The probe group's Info window is displayed.
2. From the **Info** window, select the probes you want to remove from the group. Shift-click to add contiguous probes to your selection or Ctrl-click to add or remove discontinuous probes from your selection.
3. Click the **minus sign (-)**. The selected probes are removed from the probe group and appear as separate devices in the map.

NOTE:

From the List view, you can also drag a probe out of a probe group.

Editing Settings for a Probe Within a Probe Group

Each probe in a probe group can be polled at its own rate, have its own settings, and can be edited while part of the group.

To edit a probe's setting within a group:

1. Double-click the probe group's device icon. The Info window is displayed, showing the list of probes in the group.
2. Double-click to open the Info window for the selected probe, or Right-click or Ctrl-click the probe, and select an option from the **Context** menu.

Setting a Probe Group's Control Probe

You can set the control probe for a probe group. If the control probe is down, no notifications are sent for any other member of the group and the group's interfaces match those of the control probe.

To set the control probe for a group:

1. With the map editable, double-click the probe group icon. The Info window is displayed.
2. Click **Probes** in the left panel. The probes in the group is displayed.
3. In the left column of the probe list, click the star icon for the probe you want to use as the control probe. The color of the star changes to indicate that the probe is the control probe.

	Name	Probe Type
★	31.130.96.66.static.eigbox.net.	FTP (No Login)
★	31.130.96.66.static.eigbox.net.	HTTP
★	31.130.96.66.static.eigbox.net.	Ping/Echo
★	31.130.96.66.static.eigbox.net.	POP3
★	31.130.96.66.static.eigbox.net.	SMTP

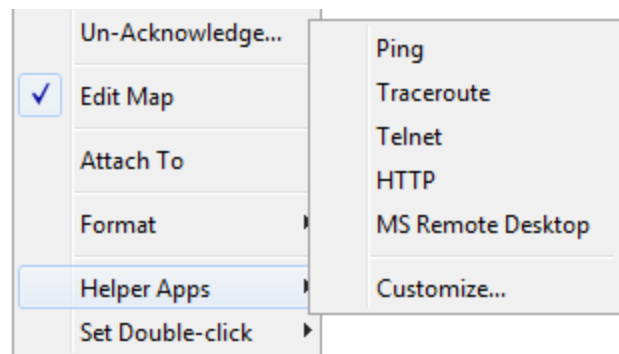
Using Helper Applications

You can use helper applications to get information for creating maps or to troubleshoot problems. These programs are available in a [Context menu](#).

To invoke a helper program:

1. Ctrl-click or right-click a device.
2. Select one of the helper applications to launch it using the device as its target.

For example, the Ping helper application invokes the system's ping utility: generally `/sbin/ping` on Linux, or macOS, or `ping` on Microsoft Windows. Including a URL as the helper application invokes the system's tool configured to handle the URL.



NOTE:

- You can specify the same helper application for several devices at the same time if more than one device is selected. The helper app is invoked for each selected device.
- The helper application that is invoked is platform-dependent: generally, Intermapper will open a terminal program and issue a command to run the helper.
- You can choose to invoke a Helper Application by double-clicking a device. See [Using Double-Click Actions](#) for more information.

Editing Helper Applications

Use the Helper Applications Customize window to modify the built-in helper applications, and add new ones.

To view the Helper Applications Customize window:

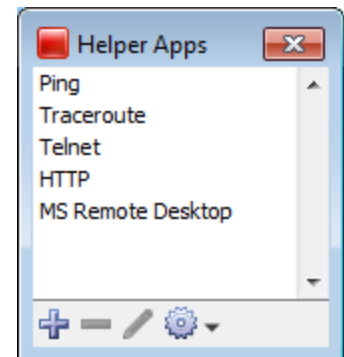
1. Right/control-click a device. A drop-down menu appears.
2. From the Helper Applications submenu, select **Customize**.

or

From the Monitor menu's Helper Apps submenu, select **Customize**.

The Helper Apps window is displayed.

This window shows the list of built-in helper apps and any user-added helper applications. To add, edit, or remove a helper application, see Adding or Editing Helper Apps. It also describes the *Launcher*, a platform-specific tool used to launch a helper app.



Adding or Editing Helper Apps

To add a new helper application:

In the **Helper Apps** window, click the plus sign (+). The Create Helper App window is displayed, showing default values for the new helper.

To edit an existing helper:

1. Do one of the following:
 - In the **Helper Apps** window, click the helper you want to edit.
 - Click the pencil tool. The Edit window is displayed, showing the current values for the selected helper.
2. Enter the following:
 - a. In the **Title** text box, type the human-readable name that appears on the Helper Applications sub-menu.
 - b. In the **Command Line** text box, type the actual string that will be invoked.

You can configure this string using the `${TITLE}`, `${PATH}`, `${ARGS}`, and `${LAUNCHER}` macros that are to be substituted when the command is invoked. In addition, you can use the `${ADDRESS}`, `${PORT}`, `${LABEL}`, or `${DEVICENAME}` macros.

- c. In the **Path** text box, type the full file path name for the helper application.
- d. In the **Arguments** text box, type the arguments to be passed along to the helper application.

Removing a Helper Application

You can remove any helper application definition you have created. Built-in helper apps cannot be removed.

To remove a helper app definition:

1. In the **Helper Apps** window, click the helper you want to remove.
2. Click **Remove**.

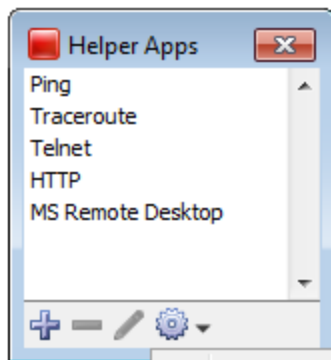
Launcher

The Launcher is a platform-specific program that allows you to invoke another program from Intermapper.

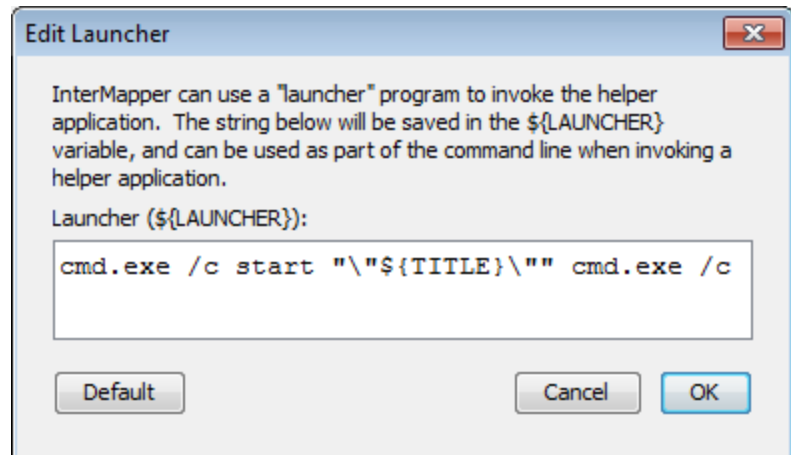
To open the Launcher window:

1. From the

Helper



Import...
Export...
Launcher...



Ap

ps window, click **Tools**. The Tools menu is displayed.

2. From the **Tools** menu, select **Launcher**. The Launcher window is displayed.

Exporting and Importing Helper Application Definitions

You can export your current Helper Application settings and import them to another instance of Intermapper.

To export the current Helper Applications definitions:

1. From the **Tools** menu in the **Helper Apps** window, click **Export**. A standard file dialog is displayed.
2. Specify a file name and location and click **Save**.

To import Helper Application definitions from a file:

1. From the **Tools** menu in the **Helper Apps** window, select **Import**. A standard file dialog is displayed.

2. Navigate to the **Helper Apps** definitions file you want to use, and double-click it or click it and click **Open**. The Helper Apps definitions are replaced with the definitions in the selected file.

How Does the Launcher Invoke an Application?

The method of launching an application is platform-dependent.

- On Microsoft Windows, Intermapper uses a command shell.
- On macOS, Intermapper opens a Terminal window.
- On Linux, Intermapper invokes the shell.

Using Default Values

For each platform, there is a default value for each built-in helper app. You can reset a helper app to its default values.

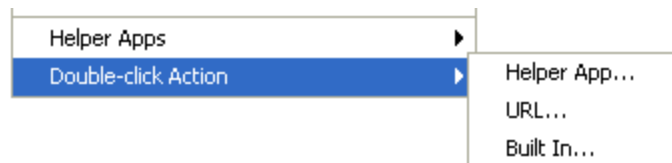
To reset a helper app to its default values:

Click **Default**. The launcher string is reset to the default value for that platform.

NOTE: You do not have to use the launcher for any helper, but it is often the easiest way to invoke another program on your computer.

Using Double-Click Actions

Intermapper defines Double-click Actions that it performs when a device is double-clicked. Many probes have a pre-defined double-click action, but this can be overridden.



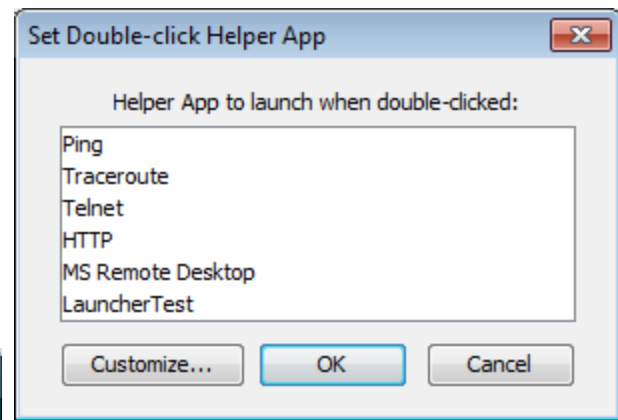
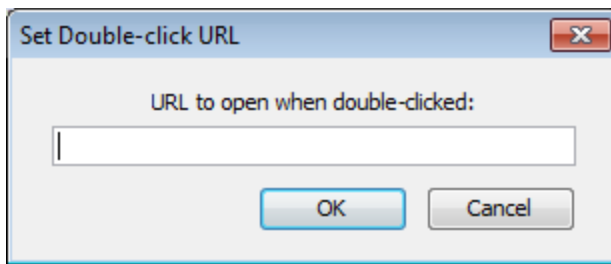
To change a double-click action, right-click the device, and select the proper choice from the sub-menu.

Helper App

Double-clicking this invokes a specified [helper application](#). This helper application runs on the same machine as the Intermapper client. Select the helper application from the current list of helpers.

URL

You can



supply

ly a URL (http, ftp, telnet, and so on) and Intermapper invokes it when the device is double-clicked. Enter a URL to be invoked when the device is double-clicked. You can use the `${address}`, `${port}` macros.

Enter a URL you want to use when the icon double-clicked. The default browser is launched with the specified URL.

Opening an Intermapper map

To open another Intermapper map, use the following URL format:

```
Intermapper://Host:Port/MapName
```

where:

- **Host** is the address or DNS name of the Intermapper server hosting the map. Use `$SAMEHOST$` to get to a map on the same Intermapper server.
- **Port** is the port for the specified Intermapper server.
- **MapName** is the name of the map, URL-escaped (`%20` for a space, `%3D` for a slash, and so on).

Example

The Example.com demonstration sub-maps link back to the Example.com parent map that look similar to the following:

Intermapper://\$SAMEHOST\$:8181/Example.com%20National%20Map

Built In

Intermapper can invoke nearly any of the menu commands as a result of a double-click. Select the desired item from the hierarchy of menu items.

Saving Your Map

Each time you make the map editable, a backup of the map is created automatically. You can revert to the backup version by selecting **Revert** from the Edit menu.

When you make a change to a map, the change is automatically saved immediately, every minute or so.

Backing Up Your Map

If for some reason you want to make changes to your map, but you want to be able to get back to your original version, you can make a backup of your map.

When you make a backup file, it stores references to your original chart data. If you restore a previous version, your chart data remains available.

To make a backup:

1. From the **File** menu, select **Backup**. The Backup Map window is displayed, showing a list of previous backups of the current map.
2. In the **Backup Name** text box, type the name you want to use for the backup file.
3. Click **OK**. A backup of the current map is created.

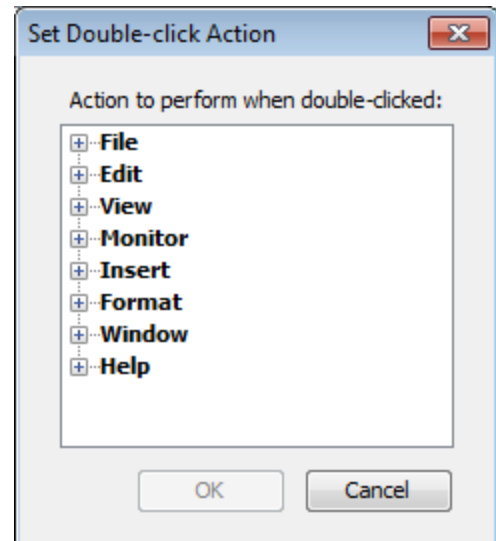
NOTE: Backups are stored in the Intermapper Settings/Maps (Backups) folder.

Restoring Previous Versions of Your Map

Use the Restore command in the File menu to restore a previous version of a map.

To restore a previous version:

1. From the **File Menu**, select **Restore**. The Restore from Backup window is displayed, showing a list of previous backups of the map.



2. Click the backup you want to use to restore the map.
3. Click **Restore**. The map is restored to the backup version.

Backup Types

Intermapper creates the following backup types:

- **Manual** - the backup was created using the Backup command.
- **Automatic** - the backup was created automatically by a change in a Layer 2-enabled map.
- **Scheduled** - the backup was created automatically, based on a schedule defined in the Map Backup panel of the Server Settings window.

Map Settings Window

Use the Map Settings window to specify colors for the map, to specify a background image, and to specify default thresholds and notifiers. Any changes you make are saved with the map, and do not affect any other maps.

To view the Map Settings Window:

1. Make sure the map is in [Edit mode](#).
2. From the **Edit** menu, select **Map Settings**. The Map Settings Window is displayed. The left pane contains a menu. The right pane contains the settings for the selected section of the menu.

Colors
Background
Device Thresholds
Interface Thresholds
Traffic Indicators
Default Notifiers
Retention Policy
Layer 2 Features

Left pane of the Map Settings Window

Setting a Map's Colors

☐ Use server defaults

Background:

Links:

Ants:

Labels:

Networks:

Discovery:

Up:

Warning:

Alarm:

Critical:

Down:

Unknown:

Acknowledged:

To view and edit the colors for the current map:

From the **Appearance** section of the **Map Settings** window, select **Colors**. The current colors for the map are displayed.

Intermapper uses a default color scheme that is controlled by the [default map colors](#) window. This color scheme applies to all new maps and to those maps for which the Use server defaults box is selected.

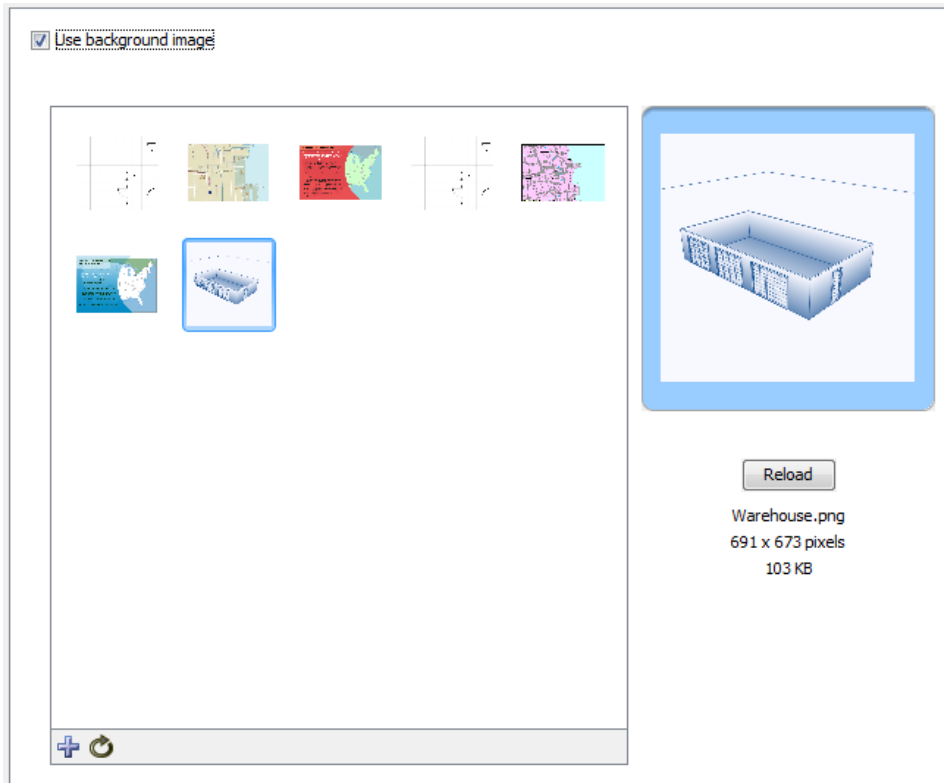
For more information on changeable colors, see [Colors you can change](#).

To use a set of colors different from the global color scheme:

1. Clear the **Use server defaults** check box.
2. Click the color box for the first color you want to change. The Color Picker window is displayed.
3. Select a color and click **OK**. The new color is displayed in the selected color box.
4. Repeat steps 2 and 3 for each color you want to change.
5. Click **OK**.

To restore the current map to the default color settings:

1. Select the **Use server defaults** check box.
2. Click **OK**. The map uses the default colors. The colors you defined are still saved with the map.

Adding a Background Image

You can define a background image for any map. The background image is displayed behind the map contents (devices, icons, and links on the map).

You can use a background image containing a floor plan of an office and move the items on the map to show the locations of each device in the office. You can also use an image containing street map of a city or topographic map of a county or state.

For more information, see [Background Images](#).

Setting a Map's Default Device Thresholds

Set thresholds to alert you to network problems.

☒ Use Server defaults

Down Thresholds

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Interface errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/>	per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

Intermapper can provide warnings or alerts when interface errors, packet loss, or round-trip times get too high. You can set default thresholds for all of these metrics from the Map Settings window.

- **Use Server Defaults** - select this check box to override the map settings and use the server default settings.
- **Down Thresholds** - Enter the number of lost packets required to generate a Down state.
- **Other Thresholds** - For each metric, in each column enter a value required to generate the a Warning, Alarm, or Critical state.

Setting a Map's Default Interface Thresholds

Use the Interface Thresholds pane of the Map Settings window to set Error, Link Utilization, and Discard thresholds for a specific map. These settings are applied to interfaces on each new device added to the map.

To create map-specific interface thresholds:

1. Clear the **Use server defaults** check box for the threshold type you want to make specific to this map.
2. Set the thresholds for the selected threshold type.
3. Click **OK**.

NOTE: You can also set thresholds for an individual link. For more information, see [Setting Thresholds for Individual links](#).

Set interface thresholds to alert you to network problems.

Error Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Errors (Received):	10	20	30	per minute
Tx Errors (Transmitted):	10	20	30	per minute
Total Errors (Rx + Tx):	10	20	30	per minute

Utilization Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

Discard Thresholds

☒ Use server defaults

	Warning	Alarm	Critical	
Rx Discards (Received):	15	25	35	per minute
Tx Discards (Transmitted):	15	25	35	per minute
Total Discards (Rx + Tx):	15	25	35	per minute

Controlling a Map's Traffic Indicators

Use traffic indicators to view network activity on a map. You can set the traffic levels at which moving ants show you the level and direction of activity on a particular link.

Set traffic thresholds to highlight network activity. Moving ants indicate the direction and magnitude of network traffic.

When the rate goes above these values, alter the display:

Frames Per Second: . . . - Some traffic
 Frames Per Second: High traffic
 Average bytes per frame: ---- Large frames
 Critical Errors: ##### ☉ Trouble

You can set the following values to control the appearance of traffic indicators:

- **Traffic units** - select bytes or frames per second from a menu. This unit is used for traffic thresholds.

- **Some traffic** - type the number of bytes or frames per second that represents some traffic.
- **High traffic** - type the number of bytes or frames per second that represents high traffic.
- **Large Frames** - type the number of bytes per frame that represents a large frame.
- **Critical Errors** - this threshold is set in the Interface Thresholds panel.

To set the default values for traffic indicators:

1. In an editable map, select **Map Settings** from the **Edit** menu. The Map Settings window is displayed.
2. In the left pane, click **Traffic Indicators**. The current traffic indicator settings for the map appear in the right pane.
3. Enter the settings you want to change and click **OK**. The map uses the new settings.

NOTE: Traffic indicators are part of Intermapper's Animation feature set. By default, animations are not enabled because they might require additional CPU resources. You can turn them on from the Animation Settings pane of the [Preferences window](#).

Specifying a Map's Default Notifiers

Notifier Name	Down	Up	Critical	Alarm	Warn	OK	Trap	Delay	
Day Sounds	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Alternate Sounds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Command Line No...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Email Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Jack - Page	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Jack - SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
My AutoMate Task	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
PowerShell-Local-dir	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
SplunkLog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Uli - Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Uli - SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	
Write To Screen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None	

Use the Map Settings window to specify the notifiers you want to attach to new devices in this map by default.

To specify the default notifiers for the current map:

- For each map state, select the check box for each notifier you want to attach to that state. For more information, see [Configuring a Notifier](#).
- To **choose all notifiers at once**, Alt-click or Cmd-click (Mac) a check box in any column. All boxes are selected or cleared in that column. You can also use **Alt-click** to set **Delay** and **Repeat** to the same value for all notifiers.

To edit a notifier:

1. Click the row of the notifier you want to edit. The notifier row is highlighted and the **Edit Notifiers** button is enabled.
2. Click **Edit Notifiers**. The Configure Notifier window for the selected notifier is displayed. For more information, see [Working With Notifiers](#).

Resetting the Default Notifier

If you changed the default notifier or edited its settings, you can reset all of the devices on the map to have the current default notifier or updated settings.

To reset the default notifier or its settings for all devices on the map:

Click **Reset All**. All devices on the map now use the current version of the default notifier.

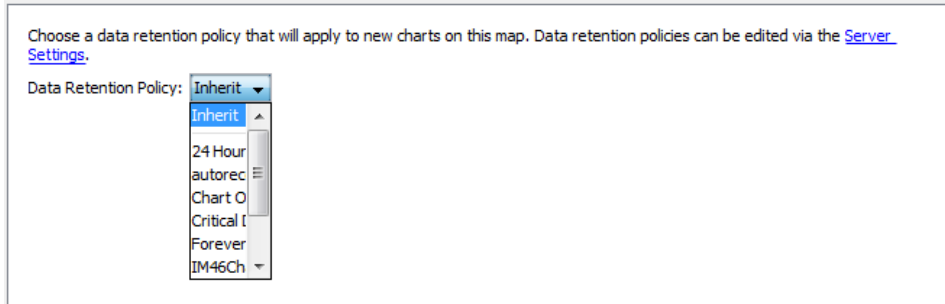
Specifying a Map's Default Data Retention Policy

If you are using Intermapper Database to collect device and network data, you can specify a default retention policy for a map. This setting overrides the default policy set in the Server Settings window.

Use the Map Settings window to specify the Retention Policy you want to use with new devices in this map. Data Retention Policies are defined from the [Retention Policy pane](#) of the Server Settings window.

Setting Your Map's Retention Policies

Use the Retention Policy panel to select a retention policy for new devices added to the map.



Data Retention Policy - select a retention policy from the menu.

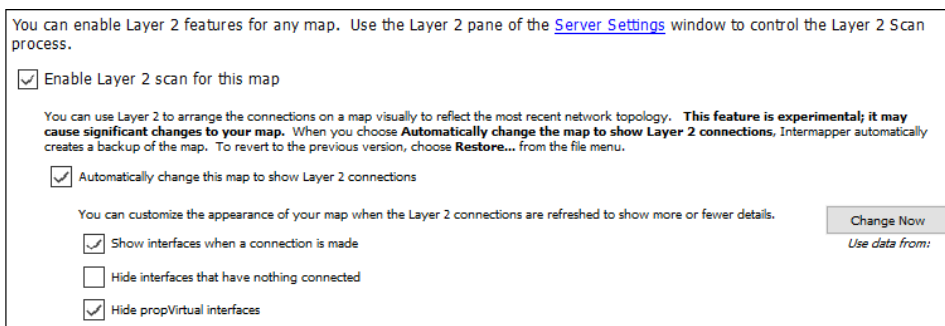
Setting Your Map's Layer 2 Options

Use the Layer 2 Settings panel to turn on Layer 2 scanning for a map and to choose how Layer 2 connections should appear. To use this panel, you must enable Layer 2 collection in the [Layer 2](#) pane of the Server Settings window.

NOTE: Layer 2 features are experimental.

Automatic Changes

When using Layer 2, you can allow the map to be edited automatically. Intermapper uses Layer 2 information to rearrange the map to match the current topology of your network. This is not a precise task; it depends on the accuracy and completeness the information collected during the Layer 2 scan.



- **Enable Layer 2 scan for this map** - select this check box to allow this map to be edited using Layer 2 scan results.
- **Automatically change this map to show Layer 2 connections** - select this check box to allow Intermapper to edit the map automatically to show Layer 2 connections.

- **Change Now** - click this button to initiate the visual arrangement of connections on the map to reflect the most recent topology using Layer 2 data.
- **Show interfaces when a connection is made** - select this check box to show Layer 2 interfaces when a connection is made.
- **Hide interfaces that have nothing connected** - select this check box to limit the number of interfaces shown to those that have something connected to them.
- **Hide propVirtual interfaces** - select this check box to hide interfaces whose ifType is propVirtual.

Editing Your Map

This is a quick overview of editing the map. Also see [Arranging the Map \(Pg. 79\)](#).

NOTE:

- Right-click (Microsoft Windows) = Command-click (macOS)
- Alt-click (Microsoft Windows) = Option-click (macOS)

To edit the map:

Do one of the following:

- Press **Tab** on your keyboard.
- Right-click in the map and select **Edit Map**.
- Click the lock in the upper left-hand corner to unlock the map for editing.
- With a map editable, drag items from another map's List View window to copy them to the new map.

To move an object on a map:

Select the object and drag it to the preferred location.

To change the shape or label characteristics of an object:

From the **Format** menu, select the node and the appropriate command.

To resize a wire-shaped network:

Click and drag the end points.

To select a node and its adjacent nodes:

Alt-click an object. Continuing to Alt-click continues to select adjacent items.

To select the devices at each end of a link:

Alt-click the link.

To re-center the map:

Ctrl-click the background of the map. The point you click is centered in the map window.
To scroll the contents of the map:

Do one of the following:

- Ctrl-drag the background of the map. The window scrolls the map contents within the map window.
- Press Alt+[arrow key] (or Option+[arrow key], macOS) scrolls the map in the direction of the arrow.

To zoom in or out:

Do one of the following:

- Ctr+Alt+drag (Ctrl+Option+drag on macOS) to select an area of the map to zoom into.
- Ctrl+scrollwheel (Cmd+scrollwheel on macOS) to zoom in or out.

Summary of Selection Tricks:

- **To select multiple items** - Shift-click.
- **To select adjacent items** - Alt-click. Alt-click again to select the items adjacent to those items.
- **To select all routers, networks or various other groups of items** - From the **Edit** menu, select the appropriate command from the **Select Other** sub-menu.

Configuring PowerShell for Intermapper

Before you can use PowerShell probes or notifiers, you need to configure the Intermapper machine and any target machines to allow connections. There are many options, and an exhaustive tutorial is beyond the scope of this topic.

For more information, see [overview to using PowerShell](#) on remote computers.

NOTE: This topic assumes you know how to launch PowerShell and that the Intermapper machine and the machines you want to connect to are running Microsoft Windows.

Enabling PowerShell Remoting

To enable PowerShell remoting, open a PowerShell window and run the following command (also known as a *cmdlet*) on all the machines you want to connect to:

```
Enable-PSRemoting -Force
```

The command starts the WinRM service, configures it to start automatically, and creates a firewall rule that permits incoming connections. The `-Force` attribute accepts the default settings.

NOTE:

- You must be logged in as an administrator to execute these commands.
- If both the local and remote computers are in a domain, enable PowerShell Remoting only on remote machines.
- If the local and remote computers are not in a domain, enabling remoting on the local machine is recommended. Among other things, it allows you to access and modify TrustedHosts, which is required in order to connect to a remote computer.

Configuring TrustedHosts

NOTE: The TrustedHosts configuration can result in security vulnerabilities. If you are not well-versed in security issues, you should consult an expert.

TrustedHosts is a list of trusted resources for your computer. The TrustedHosts list consists of a comma-separated list of computer names, IP addresses, and fully-qualified domain names. For a given computer, only administrators can change the TrustedHosts list.

Before you can connect to a remote computer, your TrustedHosts list must contain the IP address of that computer.

If your computers are not on a domain, you need to configure the TrustedHosts setting on the Intermapper server for all the computers you want to connect to. Execute these commands, providing an IP address, or use wildcards to specify an IP range (see below). Separate entries with commas (,).

Setting the Value of TrustedHosts

The following is a sample command that sets values in TrustedHosts:

```
Set-Item wsman:\localhost\client\trustedhosts [IP address],  
[IP address], ...  
Restart-Service WinRM
```

Using Wildcards When Configuring TrustedHosts

When configuring TrustedHosts, PowerShell accepts only a single asterisk (*) as a wild card.

The following are not allowed:

```
...\trustedhosts *.*.*.*, 192.168.*.*
```

The following are allowed:

```
...\trustedhosts *, 192.*, 192.168.*
```

Testing the Connection

To test the configuration, execute the following command:

```
Test-WsMan [COMPUTER]
```

A successful test shows a several lines of information. The last line is most interesting, as it shows the version of Microsoft Windows Management (WsMan) running on the target machine.

Executing a Command

You can now try a command. To determine the versions of PowerShell and several other related systems, run the following command:

```
Invoke-Command -ComputerName [Target Computer] -ScriptBlock {  
$PSVersionTable } -credential [UserName]
```

This returns a list of versions of PowerShell, WsMan, and other systems.

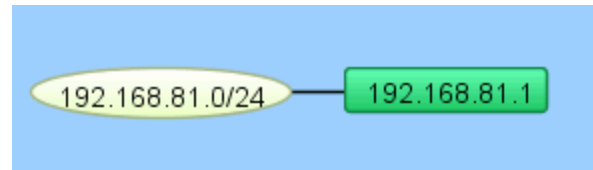
If the command runs successfully, you can try running PowerShell probes and notifiers.

Arranging Your Map

After you add all the devices to the map, you can arrange them to suit your ideas about the network.

Default Appearance of Devices and Networks

By default, *Intermapper* displays devices as rectangles in its map. These devices are connected by links (straight lines of differing thickness to indicate the kind of link) to networks, which are represented as ovals.



Possible Arrangement Approaches

You can use *Intermapper's* layout tools to arrange your maps in ways that are most useful to you.

1. Find one or more clusters of related items and move them close together.
2. After you create clusters, you can move them to different parts of the map.
For example, an Ethernet or FDDI backbone with its attached routers might make a good cluster. Similarly, a central router or switch with its attached networks might serve as a cluster.
3. If networks or ports are not important for a map, you can hide them from the [Interfaces Window](#).

See [Using the Arrange Commands \(Pg. 94\)](#) for more information about using the commands from the Format menu.

For other information related to arranging your maps, see [Arranging Tips \(Pg. 98\)](#).

Enhancing Your Map's Appearance

Intermapper has many tools for enhancing your map's appearance. These include the following:

- **Setting Custom Icons:** Intermapper comes with a set of icons derived from Cisco's Icon Library. Use these industry standard icons, or import your own PNG, GIF, or JPEG images. For more information, see [Custom Icons \(Pg. 81\)](#).
- **Setting a Map Background:** You can use a graphic as a "background" to the map. The devices being monitored will appear above this background image. For more information on using background images, see [Background Images \(Pg. 84\)](#).
- **Adding text objects:** You can add text objects your map to label groups of objects or provide information to the viewer. For more information, see [Text \(Pg. 383\)](#) in the Insert menu reference topic.

- **Importing Device Descriptions:** Intermapper allows you to import descriptions of the devices on a map directly from a tab-delimited file. This simplifies the creation of a new map, and makes it easy to add new devices as your network grows. For more information, see [Importing Data Into Maps \(Pg. 631\)](#).
- **Setting the Geographic Coordinates of the Map:** Intermapper allows you to indicate the latitude and longitude for benchmarks (known positions on the map). If, for example, you are using an actual geographic map as a background image, you can use geographic coordinates to place a device in the correct location on the map. For more information, see [Using Geographic Coordinates \(Pg. 634\)](#).

Setting a Map Background

Create a new map and save it. You can scan your own map or obtain an image that covers the right area from one of the sites listed in [Using Geographic Coordinates \(Pg. 634\)](#). Intermapper can use PNG, GIF, or JPEG image files as map backgrounds. You can obtain suitable images by scanning or creating your own maps, or use one of the many map sites listed in [Sources of Maps \(Pg. 637\)](#).

To add a background image to a map, drag the image file into the map window. It is added to the map and becomes visible.

Setting the Geographic Coordinates of a Map

If you use a geographic map for a background, you can associate specific points on the map with geographic coordinates (latitude and longitude) by adding benchmarks. For more information, see [Using Geographic Coordinates \(Pg. 634\)](#). After you specify the coordinates, you can specify geographic coordinates for devices as you import them to the map and they are automatically placed in the correct location.

Icons and Images on Maps

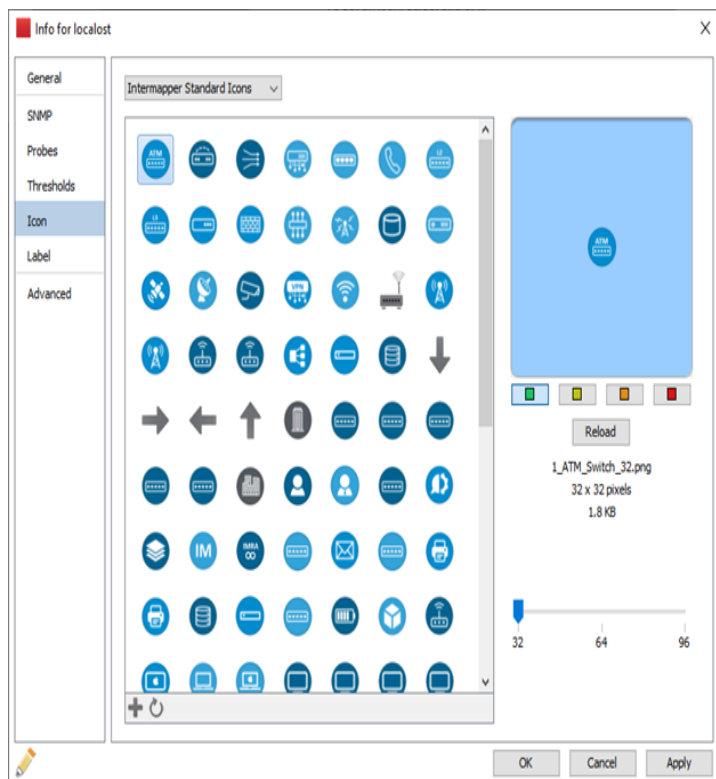
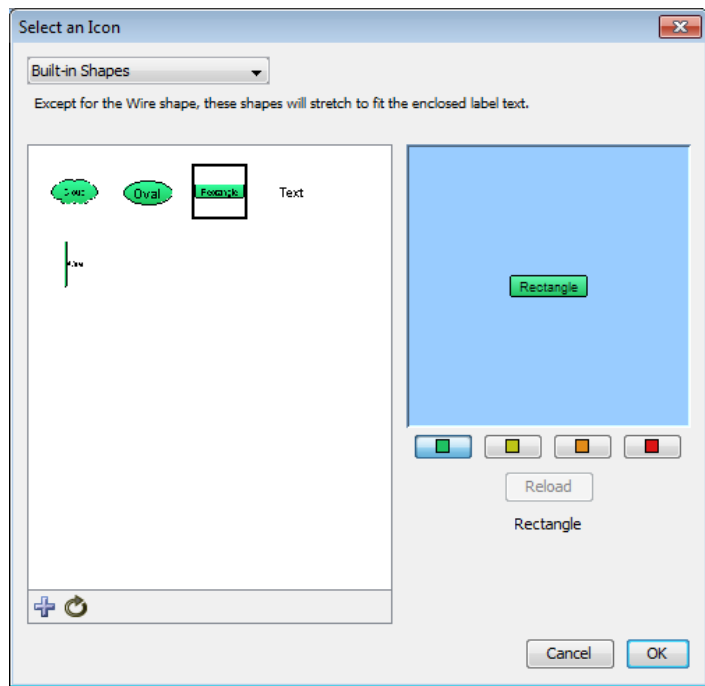
Intermapper can display devices on a map in one of several shapes. The default shape is a rectangle, with the device's Label inside. Intermapper can also display an oval, a wire (a straight line), a cloud, a text object which can be used as a legend on a map, or an icon.

A large number of built-in icons are provided with Intermapper. It is also very straightforward to import your own icons.

Setting an Object's Icon

To set an icon, select one or more items on the map then click **Format > Icon**. This opens the Select an Icon window. This window includes the following components:

- A menu lists collections of icons called Icon Sets. There are several built-in icon sets, including Traditional and Default icons sets and various Cisco-themed icon sets..
- A scrolling list on the left shows icons from the selected icon set. These icons appear at a uniform size in the list. Click one of these icons to use it for the selected devices on the map. Grayscale custom icons appear shaded with the color of a device when it is in the UP state (the default is green).
- A preview pane of the icon, showing the selected icon in the size it will appear on the map.
- Color preview buttons. The green, yellow, orange, and red buttons correspond to the different device states. Click a colored button to view the icon's appearance when it is in the indicated state.
- Below **Reload** is Information about the icon (filename, dimensions, and file size).
- Click **Refresh** (as shown) to force Intermapper to reload the image, perhaps after modification in an image editing program.
- Click **Import** (as shown) to import an icon or a folder of icons into Intermapper. These icons are sent to the InterMapper Settings > Custom Icons folder on the Intermapper server.
- Click **Refresh** to refresh the list of icons.
- Drag an image file to the window to import it into the current icon-set.



- Drag a folder of image files to the window to create a new icon-set, importing the image files in the folder to the new icon-set.
- If the Icon Size slider appears, use it to select the icon's size.

Icon Coloring According to the Device Status

Intermapper colors the icon depending on its status. When in the Up status, the icon retains its normal color. (Grayscale icons are tinted green.) If the icon goes to a warning, alarm, or down status (yellow, orange, or red, respectively) Intermapper shows a grayscale version, tinted to match the device's state.



Clicking the color preview buttons changes the color to show how the icon appears on the map in a given status.

Creating Custom Icon Files

Icons files can be saved in one of several common graphic formats:

- **Portable Network Graphics (PNG)** - (recommended) works with all operating systems and platforms.
- **Joint Photographic Experts Group (JPEG)** - works with all operating systems and platforms.
- **Graphic Interchange Format (GIF)** - works with all operating systems and platforms.

Other graphics file formats can work for you, but are not guaranteed to appear properly on all platforms.

The recommended file format is a PNG file, saved at 72 pixels per inch with 256 colors. You should use transparency for the area surrounding the icon, so the background color shows through properly.

If the icon's filename has a suffix of _## where ## is the size in pixels, the icons are grouped automatically, and the icon size slider is displayed.

Placing Arbitrary Icons and Images in Maps

Any icon or image can be placed in a map. Before you can place an image in a map, you must import it as an icon.

To place an image or icon in a map:

1. If the image has not yet been imported as an icon, import it now.
2. From the **Insert** menu, select **Icon**. The Select an Icon window is displayed.

3. Select an icon or image you want to insert and click **OK**. The icon or image is displayed in the map.
4. Move the icon or image to a desired location on the map.

NOTE: When you place an icon on a map, a network oval is added to the map, and the icon assigned to it. You can edit the network as you would any other network, changing the icon or label or adding a comment or subnet list.

Adding Background Images to Your Map

You can place a background image on a map so that it appears behind the devices, icons, and links on the map. All image [file formats supported for custom icons \(Pg. 83\)](#) can be used.

- You might use a background image containing a floor plan of an office, and move the items on the map to show the locations of each device in the office.
- You might use an image containing a street map of a city or topographic map of a county or state.

The figure below shows a map after placing an image in the background.

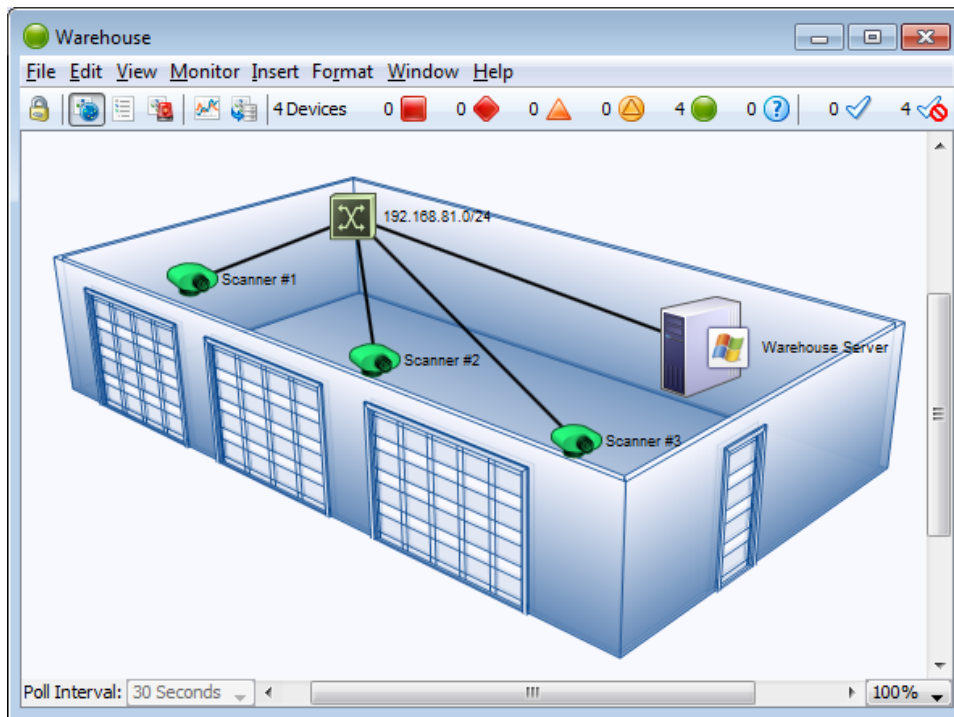
To place a background image in your map:

Drag an image file from a desktop folder to the map window.

or

From the **Appearance** section of the [Map Settings \(Pg. 68\)](#) window, available from the Edit menu, select **Background**. The Background pane appears, showing the current background image, if there is one.

Select **Use background image**.



Tips for Using Background Images

Image Size

Background images retain their height and width. Images are not scaled (stretched or shrunk) when you resize the window. If the background image is smaller than the current window size, the image is centered on the map and the map background color shows around the edges. If a large image is used, its dimensions determine the full size of the window.

Image Contrast and Brightness

Contrast images can make it difficult to see the devices and links against the background. To make the image more suitable as a background image, you can use a graphics program to increase the brightness and/or decrease its contrast before placing it in a map. We regularly use GraphicConverter, an inexpensive shareware graphics program from <http://www.lemkesoft.com>, to do this task. It has a Brightness/Contrast adjustment facility to simplify this task.

Image File Size

Large images consume large amounts of memory and slow Intermapper's redrawing of the window, especially when viewed over a remote connection. You should balance the image

quality against the size of the map. Larger maps might look better, but they might also consume large amounts of memory.

NOTE: Use of a compressed image file format such as JPG does not necessarily translate into less memory use.

Using Contrast and Compression to Reduce Image File Size

Decreasing contrast can decrease the size of an image, so that decreasing the contrast as described above decreases the size of the background image as well. Use compressed formats, such as JPG and GIF, to further decrease the overall size of the image file.

Editing Labels

Use the **Label** command, available from the Format menu (Cmd/Ctrl-L) to edit the labels for selected map objects. You can edit the label for a single device or network from the Device or Network Info window.

Every item on a map has its own descriptive label. Intermapper creates a default label showing the device's full DNS name or IP address(es).

To edit a map object's label:

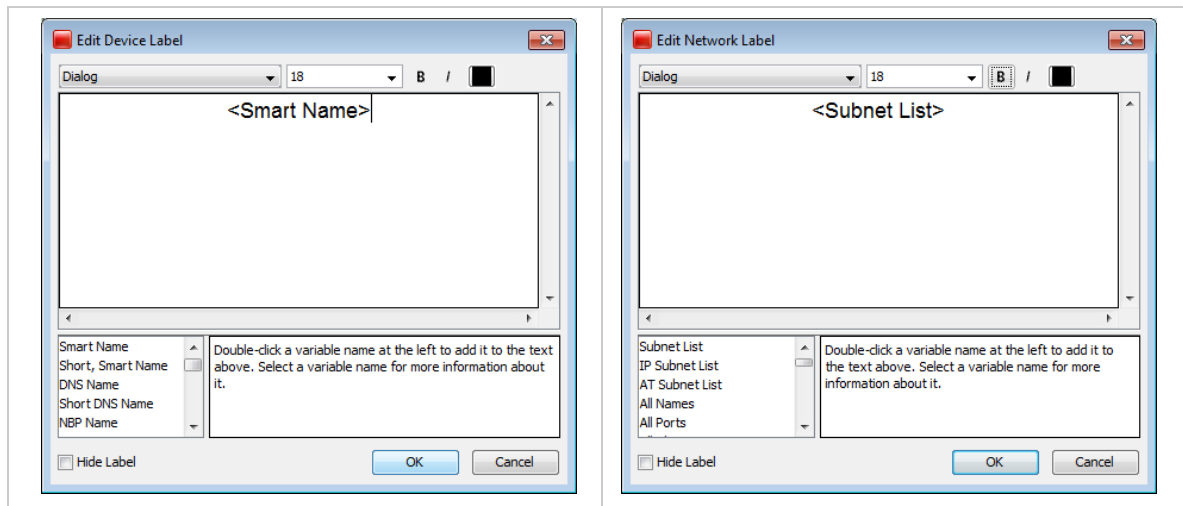
1. Make sure the map is in [Edit mode \(Pg. 154\)](#).
2. Select one or more map objects.
3. From the **Format** menu, select **Label** (Cmd/Ctrl-L).

Depending on the selected object, the Edit Device Label dialog or the Edit Network Label dialog is displayed.

4. Enter label data as follows:
 - Type text in the Label dialog's text box.
 - Double-click any variable name in the list at the lower-left to insert that value into the item's label.
 - Select **Hide Label**.

For example, the device in the Edit Device Label window uses the short, smart name (the leftmost part of the full domain name). The network shown in the Edit Network Label window has a static (unchanging) label of Our ISP with a list of all the subnets in the network shown on the next line.

NOTE: You can also use Intermapper variables and Javascript to insert information dynamically into a device label. For more information, see [Dynamic Label & Alert Text](#).



Hiding a Device or Network Label

In some cases, you might not want to display a device or network label.

You can hide the label for any device or network unless the icon is set to one of the following:

- Rectangle
- Oval
- Cloud
- Text

To hide the label for a device or network:

1. From the **Format** menu, select **Icon**. The Select an Icon window is displayed.
2. Select an icon other than one mentioned above and click **OK**. The icon is displayed for the selected device or network.
3. From the **Monitor** menu, select **Label**. The Edit Device Label or Edit Network Label window is displayed.
4. Select the **Hide Label** check box and click **OK**. The label for the selected device or network is removed.

Dynamic Label and Alert Text

When you edit a device label, notifier title, or notifier message, you can use a number of techniques to dynamically control the resulting text.

Showing Parameter or Variable Values in a Device Label

When editing a device label, you can show probe parameters, probe variables, and device export attributes in the label.

- **Probe parameters** - any field in the selected probe's Set Probe pane, specified in the [<parameters> section](#) of the probe.
- **Probe variables** - variables defined in the probe. In SNMP probes, specified in the [<snmp-device-variables> section](#) of the probe.
- **Device attributes** - any [attribute of a device](#) exported using [the Data File command](#) (available from the File menu's Export submenu).

Use the following syntax:

```
${param:<name of parameter, variable, or attribute>}
```

For example, to show the connect time in a device label corresponding to a TCP probe, your label might look similar to the following:

```
<Smart Name>
Time to establish connection: ${param:_connect} msec.
```

Notice, there is no space after the param: and the name of the variable. (The underscore is part of the variable name. Most names do not have the underscore.) Any variable that can be shown in the [<snmp-device-display>](#), [<script-output>](#), or [<command-display>](#) section of the probe can be used in a label using this syntax. You can show a parameter of the Basic OID probe just as well. For example,

```
Getting data from: ${param:Object ID}
```

You can show device export fields as follows:

```
Belongs to map: ${param:MapName}
```

Using JavaScript in a Device Label or Notifier

You can also use JavaScript in a device label or notifier to collect information, process it programmatically, and include the results in the label or notifier. Use the following label syntax in a label:

```
<? write( "Hello World" + "\n"); ?>
```

The `<?` and `?>` markers indicate the beginning and end of the JavaScript.

Variables and Scope in JavaScript

Important: JavaScript in labels and notifiers runs in the global scope within Intermapper. If you declare a variable within the global scope, rather than within a function, the variable is accessible for reading and writing by JavaScript running in any other device label within Intermapper. This can produce unexpected results if you attempt to run the same script in multiple devices.

JavaScript functions are supported and you can store values within devices and notifiers, which are remembered between polls. Fortra recommends using these techniques when you need to protect a variable from being overwritten. For more information on setting variables in devices, see [Remembering Values from One Poll to the Next](#).

Example: Simple Scripted Label

The following is a more complex example:

```
<Smart Name>
<?
  for (var i=1; i<=3; i++) {
    writeln( "Hello World #" + i);
  }
?>
```

The displayed label above appears as follows:



```
MyComputer.dartware.com
Hello World #1
Hello World #2
Hello World #3
```

write and writeln Functions

The following functions are used to write output to the label:

- The `write` function sends its output to the label without a line break.
- The `writeln` function sends its output to the label and appends line break at the end, so you do not need to explicitly append the `"\n"` in your JavaScript code.

Accessing Probe Parameters

Use JavaScript to access probe parameters using the following syntax:


```
<? writeln( "Getting data from: " + self.get( "Object ID")); ?>
```

The `self` object refers to the device whose label you are setting. The `self` object is always available when using JavaScript to generate a label. Use the same syntax to get access to a probe variable as well. For example,

```
<?
  var connTime = self.get( "_connect");
  writeln( "Time to establish connection: " + connTime);
?>
```

JavaScript Error Handling

If you misspell the name of your variable, (by using `_conect` in the previous example) the label is displayed as follows:



Time to establish connection: BAD ARG, see debug log

If you look in the debug log, you see the following message:

```
12:15:46 JS> [Device: map 'Exporting Fields', device
'nitro.dartware.com.', probe
'SNMP Traffic']:BAD ARG: There is no variable called '_conect'. It
should be the
  name of a probe variable without '$' or curly braces.
```

The error message tells you the map, device, and probe in which the error occurred as well as details about what caused the problem.

A JavaScript syntax error results in the following label:

JS EXCEPTION, see debug log

The debug log contains the exception message, but give details about the syntax problem.

Execution Time Limit

The execution time of a script is limited to 50 and 100 msec. This prevents the script from monopolizing the CPU. This is more than adequate time to produce a complex label or notifier output.

For example, the following:

```
<?
for (var i = 0; i < 1000000; i++) {
  if(i%10000 == 0) {
    writeln( "testing the timeout " + i);
  }
}
?>
```

Generates the following label:

```
testing the timeout 0
testing the timeout 10000
testing the timeout 20000
testing the timeout 30000
JS ABORTED, after 3 ticks
```

NOTE:

Three ticks is approximately 50 msec.

Remembering Values From One Poll to the Next

You can retain the value of a variable from execution of the JavaScript to the next using one of the following techniques:

- **JavaScript Global Variables** - any JavaScript variable declared at global scope is retained from one execution of JavaScript to the next. The variable is visible regardless of which device is running the script. The variable is also visible regardless whether the JavaScript is running to generate label text or a notifier's

text. Keep this in mind when using the same script for more than one device; you might unexpectedly overwrite a global variable.

- **Device JavaScript Variables** - a piece of data can be stored in a device. An advantage of these variables over global variables is that each device can have the same named variable but the value will be different for each device. You can use `self.get(...)` and `self.set(...)` to read and write this data. The name of the variable must be different than any probe parameter or probe variable.

Example: Storing a Value With a Device

To read the value stored in the device's variable "MyInformation" into myinfo:

```
var myinfo = self.get( "MyInformation" );
```

To write the value of myinfo out to the device's variable "MyInformation":

```
storedinfo = self.set( "MyInformation", myinfo );
```

The function `self.set(...)` returns the stored value. If the value cannot be saved, for instance, if you try to save to an existing probe parameter or probe variable, the returned value is the actual value of the parameter or variable, not the one you tried to save.

Example: Incrementing Counter

The following examples shows how to implement a counter that increments each time the label is drawn. Note that the first time the script runs, the counter variable does not exist.

This script below gets the value of "Count", displays it, increments it, and saves it. The first time the script runs, `self.get()` returns the "BAD ARG, see debug log" string . Since JavaScript cannot turn this value into a number, you can use the JavaScript `isNaN()` function to determine that n is NaN (Not a Number), and thus has not been initialized.

```
<?
var n = Number( self.get( "Count" ) );
if ( isNaN(n) ) n = 0;
writeln( "Count is " + n );
n++;
self.set( "Count", n );
?>
```

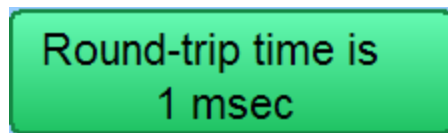
A similar technique would also work for JavaScript global variables as well.

Accessing Device Attributes

You can also use JavaScript to access device attributes. The syntax is different than for accessing probe parameters and variables. It still uses the `self` object, but the attribute names are simply properties of the `self` object. The syntax looks like this:

```
<?
var rtt = self.RoundTripTime;
writeln( "Round-trip time is \n" + rtt + " msec");
?>
```

The above JavaScript reads the last round-trip time into `rtt`, and displays it as follows:



Round-trip time is
1 msec

If you misspell a device attribute, the error shows up as a JavaScript syntax error because the misspelling is not JavaScript data, but actual language syntax. “JS EXCEPTION, see debug log” is shown in the label and a detailed explanation in the debug log.

Any device attribute can be used in a label. For a list of device attributes, see [Device Attributes](#).

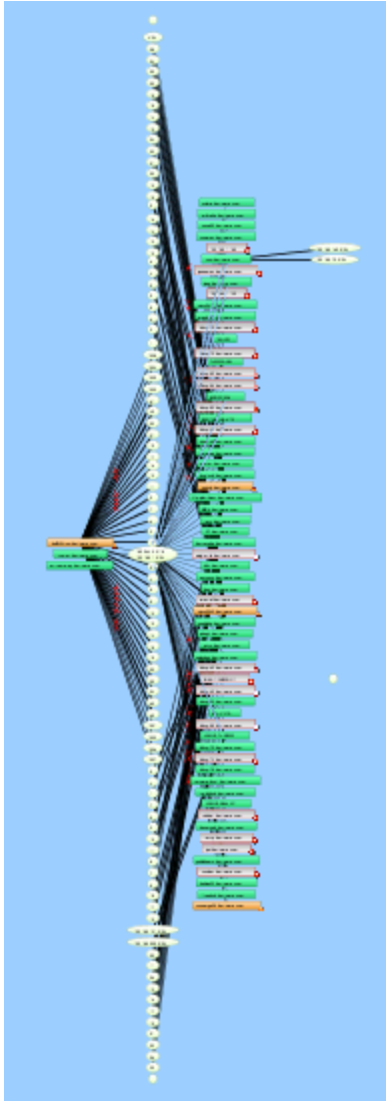
Accessing Interface Attributes

Devices connect to networks through interfaces. Each device has a property called `interfaces`. In JavaScript, this property is displayed as an array of Interface objects. The following example below lists all down interfaces:

```
<?
var downInterfaces = 0;
for (var i =0; i < self.interfaces.length; i++) {
  var ifc = self.interfaces[i];
  if ((ifc.Enabled == "TRUE") && (ifc.Status == "down")) {
    downInterfaces++;
    write( ifc.Index + ". ");
    write(ifc.Alias.length > 0 ? ifc.Alias : ifc.Name );
    writeln( " : " + ifc.Status);
  }
}
writeln();
writeln(downInterfaces + "/" + self.interfaces.length + " interfaces
down");
?>
```

Any interface attribute can be used in a label. For a list of interface attributes, see [Interface Attributes](#).

Using Arrange Commands



Use the Organic, Tree, Cycle, Bus, Star, and Grid commands from the Format menu's Arrange submenu to automatically rearrange and organize the selected elements.

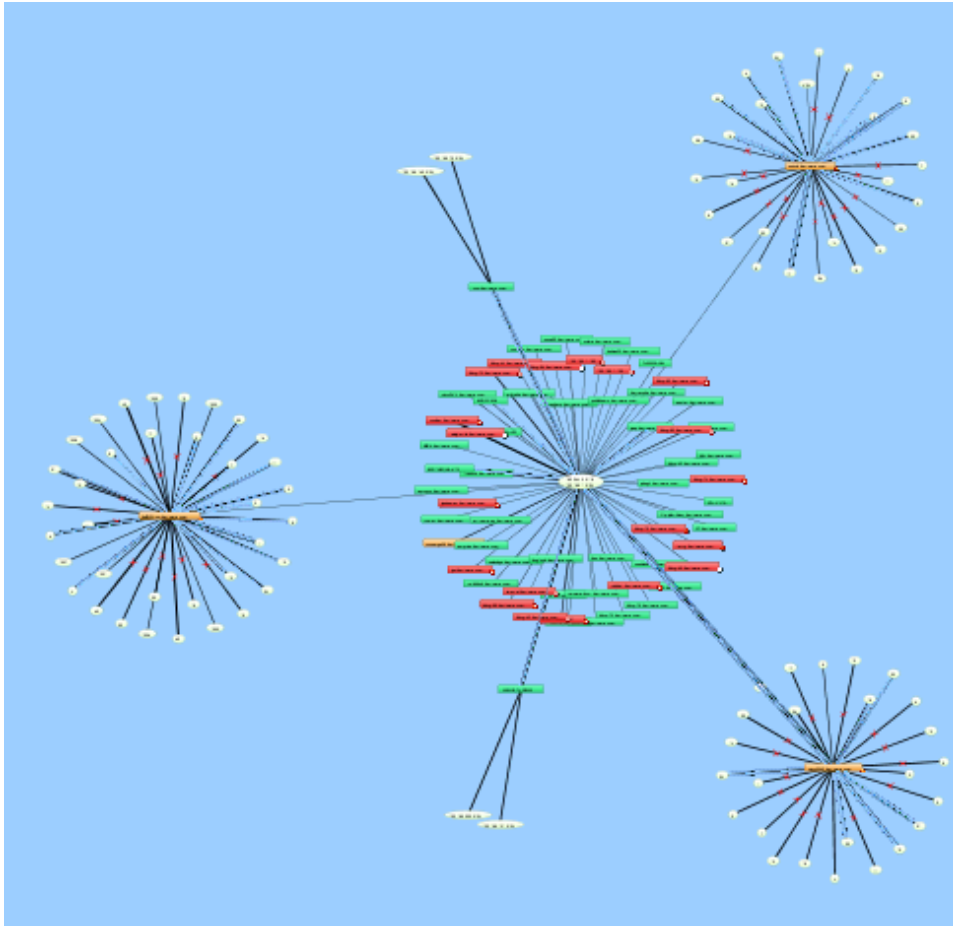
NOTE: If no objects are selected, Organic, Tree, and Grid operate on all map objects, or on any selected objects. For Star and Bus, you must have at least one object selected. For Cycle and Grid, you must have at least two objects selected.

Using Organic Commands

Use the Organic command, available from the Format menu's Arrange submenu, to arrange the objects on a map so that crossed lines are minimized and objects are not overlaid on each other. This is the method used to arrange devices during auto-discovery.

To the right is a complex map. Notice that there are many overlapping links.

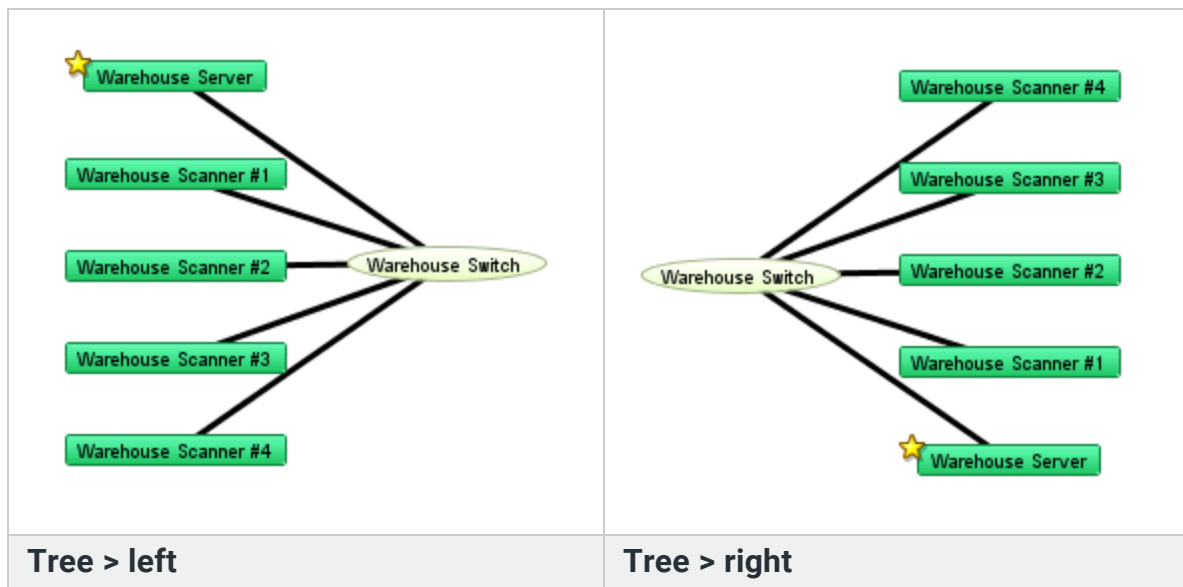
The following is the same map after applying the Organic command:



Using Tree Commands

Use the Tree command to arrange the current selection in a tree. A sub-menu controls whether the tree structure should be drawn to the right, down, left, or up.

Arrange items in a tree structure. Specify the direction of the branches. The following shows the difference between Tree > left and Tree > right:

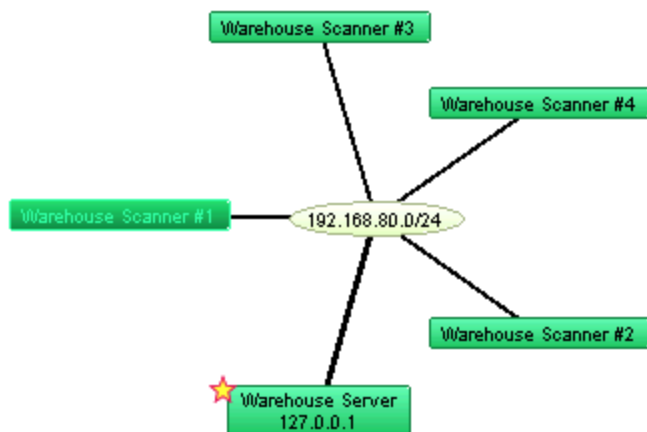
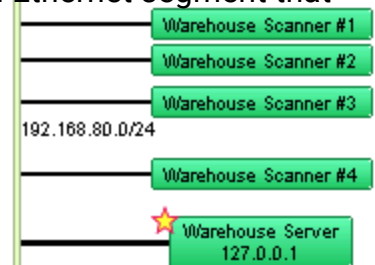


Using Bus Commands

The network oval in the center of the cluster above represents an Ethernet segment that interconnects several devices in an office. To make it a cluster, use the Bus command from the Arrange submenu.

Using Star Commands

The Star command arranges connected items in a circle around the selected item, similar to the Organic command.



Using Grid Commands

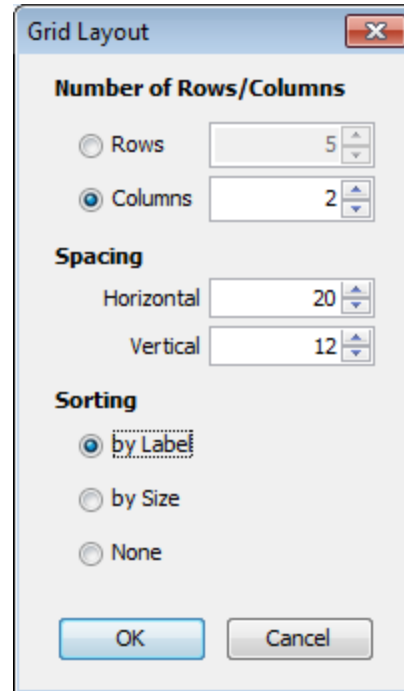
Use the Grid command to arrange connected items in a grid.

To use the grid command:

1. Select the devices you want to arrange in a grid.
2. From the **Format** menu's Arrange submenu, select **Grid**. The Grid Layout dialog is displayed.
3. Specify your parameters.
4. Click **OK**. The devices are arranged as specified.

NOTE: Sorting by None moves the selected devices to form a grid relative to the upper-left icon in the selection.

The following example shows the result of the Grid layout command after selecting only the devices in Star example above:



Using Cycle Commands

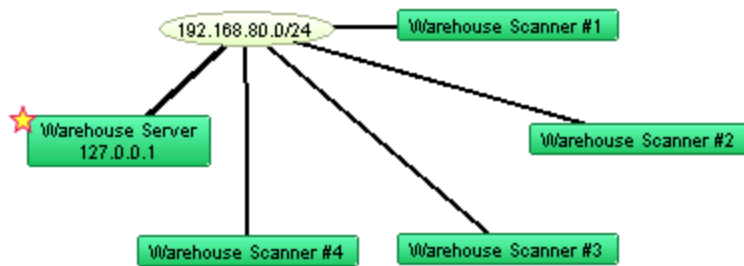
NOTE: The Cycle command is deprecated. Fortra recommends using the Organic command for initial map layouts.

Use the Cycle command to spread out items in the map and to make the relationships more clear. The Cycle command moves all devices and networks near the edge of the window.

To use the Cycle command on all map objects:

1. From the Edit's **Select** menu, select **Select All** (Cmd-A). All objects in the map are selected.
2. From the **Format** menu's **Arrange** submenu, select **Cycle**. The objects are evenly distributed around the map as shown below.

The Cycle command moves all devices and networks near the edge of the window. For example,



Tips for Arranging Your Maps

After you form a bus or star cluster, drag it to the edge of the window to see the interconnections of the remaining devices. Create other clusters as needed.

After you identify and arrange the clusters, use the following tips to fine-tune your map:

- **Move one or more items around the window** - drag them to a new position. Use shift-click to add or remove items from the current selection before dragging.
- **Automatically select connected items - Alt/Option-click** an object to select all connected leaves. (A leaf is an object that has no other connections.) A second **Alt/Option-click** selects all objects (leaves and non-leaves) connected to the current selection.

Subsequent Alt/option-clicks continue to expand the selection, choosing first the leaves, then the non-leaves that are attached to the current set of selected objects.

- **Use the Format menu commands** to affect placement of items in the map. In addition to the **Cycle**, **Bus**, and **Star** commands described above, use these menu commands to change the orientations or sizes of the items in the map.

Align	modifies the alignment of items
Rotate	rotates the selected items around their center
Scale	increases or decreases the separation of the selected items

- Use the following **Format** menu commands to affect the appearance of individual items:

Icon	changes the item's shape to a rectangle, oval, wire, cloud, text, or other icon
Label	modifies a text label for an item in the map

	Label position	changes the location of a text label relative to its item
--	-----------------------	---

- Right-click (or Ctrl-click) to set the Font, text Size and text Style from the context menu for all selected items.
- If networks or ports are not important for a map, hide them from the [Interfaces Window](#).
- See [Editing Labels for Devices and Networks](#) and [Connecting Devices to Switch Ports](#) for more tips on arranging the map.
- Intermapper periodically scans routers and switches and displays newly discovered interfaces. If you delete the interface/oval from the map, Intermapper rediscovers it and displays it again. You can hide them from the [Interfaces Window](#). For more information, see [Hiding and Un-hiding Detail](#).
- If you use a switch's VLAN capabilities to segment your network, you might want to show which equipment is connected to each VLAN segment. Do this by manually dragging device links to the proper port to indicate the correct connection point. See Connecting Devices to Switch Ports in the [Switches](#).
- If the layout of the network as discovered does not match your conceptual network layout, you can copy a network oval and move device links to the new network oval. For more information, see [Copying Network Ovals](#).

Connecting Devices to Switch Ports

The following are some tips for handling switches in your map.

Hiding Inactive Ports

Auto-discovered switches display all ports in a map. This can add clutter and can make it difficult to see the real structure of the map. In addition, an inactive (unused) switch port causes the switch itself to be placed in alarm.

NOTE: You can also convert your map to Layer 2. Using Layer 2 information, your map is automatically updated to match the topology represented by the switch's Layer 2 information. For more information, see [Mapping with Layer 2](#).

Use the Interfaces window to select and remove these switch ports.

To hide switch ports:

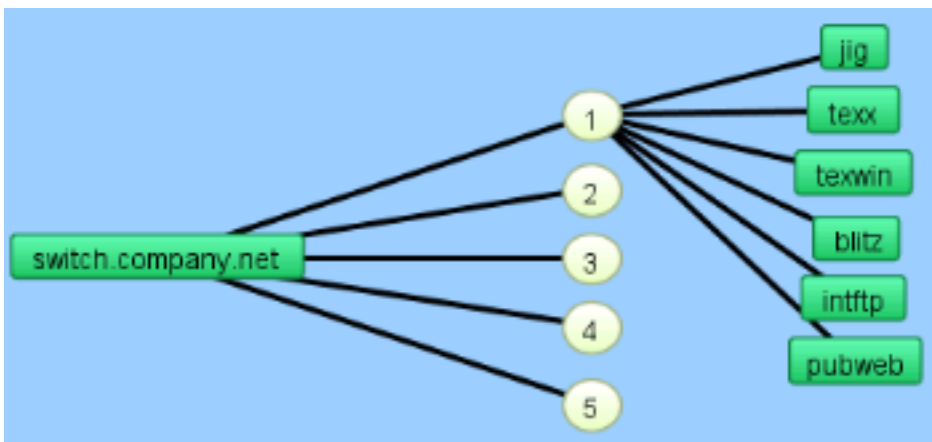
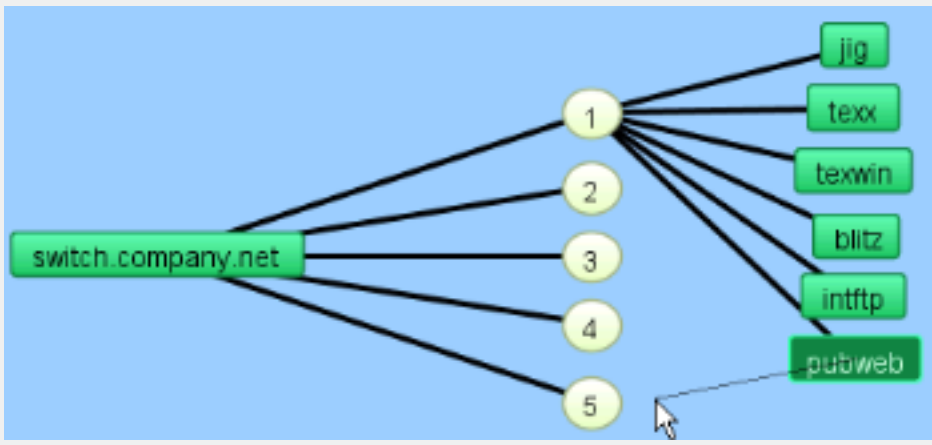
1. With the map editable, right-click or CTRL-click the switch and select **Interfaces Window**. The Interfaces window is displayed, showing the interfaces available to the switch.

2. Select or clear the check boxes to enable or disable switch ports. The disabled interfaces are removed from the map.

Connecting Devices to Switch Ports

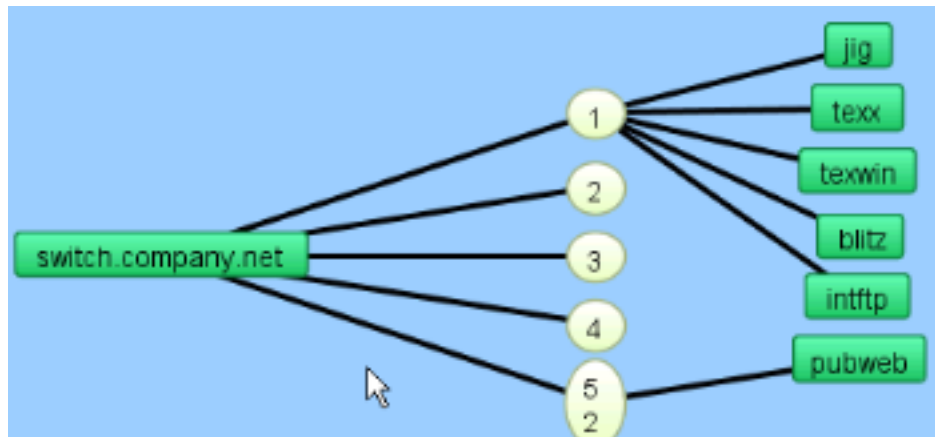
Intermapper does not connect devices to the proper port of a switch. Instead, it connects all devices of a subnet to the discovered first switch port (usually the port with ifIndex=1).

You can manually move a device's link to the proper port by dragging the link from the central oval (labeled switch.company.net in the figures below) to the proper port. For example,

<p>1. The map before making changes. The switch's ports are shown by the numbered ovals. (Make sure the map is in Edit mode (Pg. 154).)</p>	
<p>2. Click a link and drag it. A line is displayed and follows the cursor.</p> <p>NOTE: You can drag links only from a network.</p>	

3. Drag the link to the desired port. The link disconnects from the original network oval and remains connected to the new. Note that the port's oval now contains two port numbers: that of the switch (7) and the port number of the device (2).

Tip: When moving links to the proper ports on a switch, it is sometimes easier to change the port labels to display the port's number.



Copying Subnet Ovals

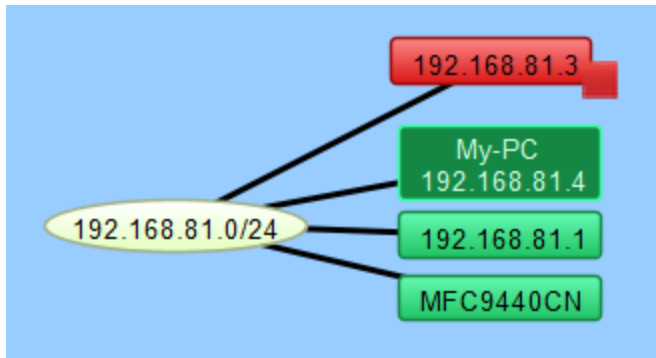
After discovering all devices, you might find that the map layout does not match your concept for a logical layout of your network.

You can make a copy of a subnet oval and reconnect your devices to it. This allows you to create visual arrangements that more closely match your concept of a logical map layout.

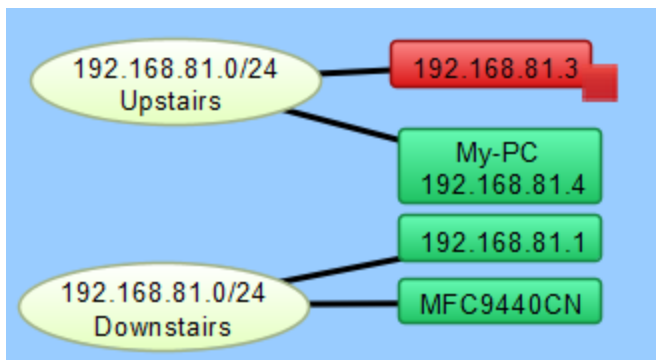
To copy a subnet oval and connect to it:

1. With the map editable, select the subnet oval you want to copy.
2. From the **Edit** menu, select **Copy**.
3. From the **Edit** menu, select **Paste**. The copy of the subnet oval is displayed on the map.
4. Move the subnet oval to the preferred location.
5. From the **Format** menu, select **Label** or press **Ctrl/Cmd+click** on your keyboard. The Edit Network Label window is displayed.
6. Add a meaningful label to distinguish it from original label. For more information, see [Editing Labels](#).
7. For each device you want to connect to the new oval, drag the link from the old oval to the new oval. The device is connected to the new oval.

Before:



After:



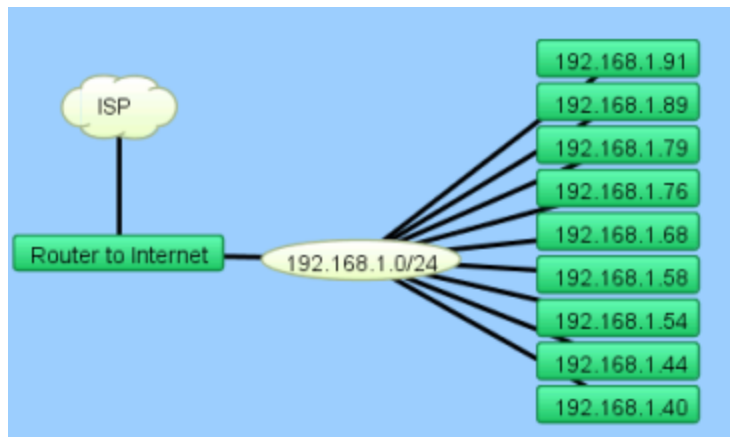
Adding Unmanaged Hubs and Switches to a Map

Intermapper cannot automatically discover or monitor unmanaged switches and hubs (called dumb devices) since they have no IP address. However, there is a workaround that allows you to represent them on an Intermapper map.

To perform the workaround, you can create a placeholder icon and then manually drag the links from the appropriate devices to this new icon. Although Intermapper cannot test or monitor this fake equipment, it appears on the map and displays the interconnections of your network as a tool to diagnose problems.

The following is a step-by-step description of the process. Note that this description works equally well for either switches or hubs.

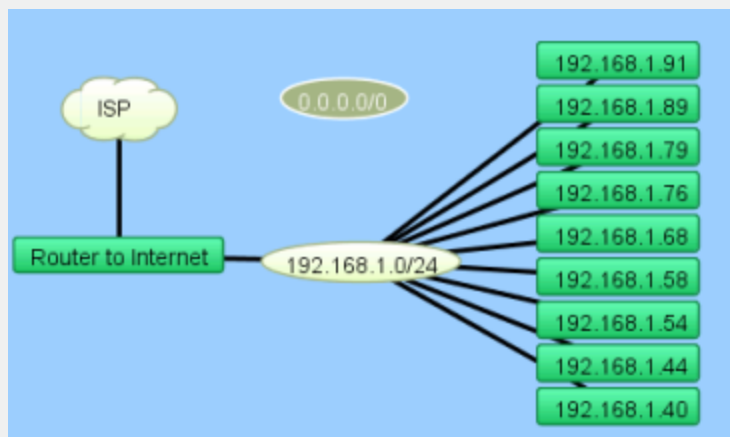
In the starting map, notice that Intermapper automatically connected a number of devices to the network oval labeled 192.168.1.0/24. The top three devices (IP addresses 192.168.1.91, .89, and .79) are connected to a dumb (unmanaged) hub on the floor. This page shows how to create a placeholder icon to represent the hub and connect those three devices to it.



Problem

The top three devices (IP addresses 192.168.1.91, .89, and .79) are connected to a dumb (unmanaged) hub.

We want to create a placeholder icon that represents the hub and then move the connections for those devices to the placeholder.

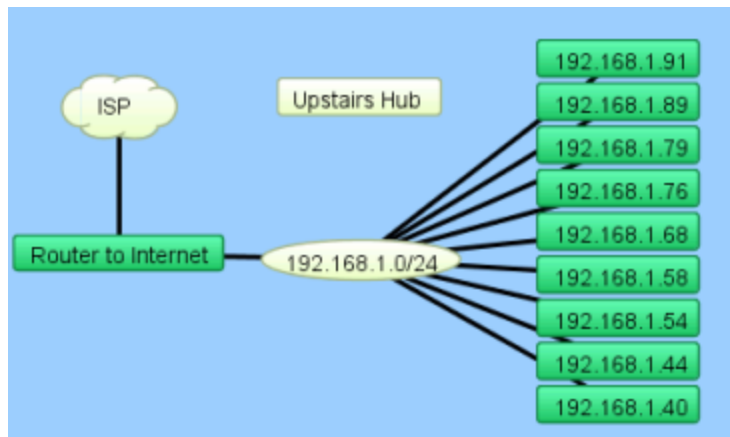


Step 1: Creating a Placeholder to Represent Your Hub

To create the new empty network:

1. From the **Insert** menu, select **Network**.
2. Enter a subnet number that is the same as the device's current subnet (oval) as shown in [Adding Networks to a Map \(Pg. 52\)](#).

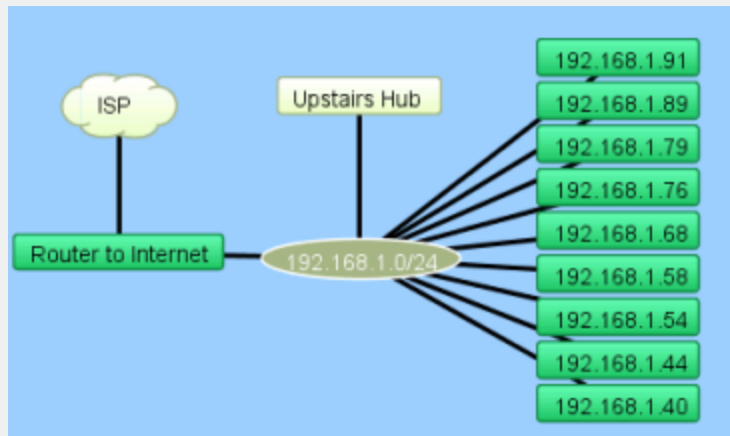
The new network is displayed as an oval, with the specified subnet number (not 0.0.0.0/0, as shown in this example).



Step 2: Tidying Item Appearances

To tidy up the appearance of the item:

1. Move the new network up.
2. Change its shape to a rectangle using the **Icon** command from the **Format** menu.
3. Change its name to **Upstairs Hub** using the **Label (Cmd-L)**.

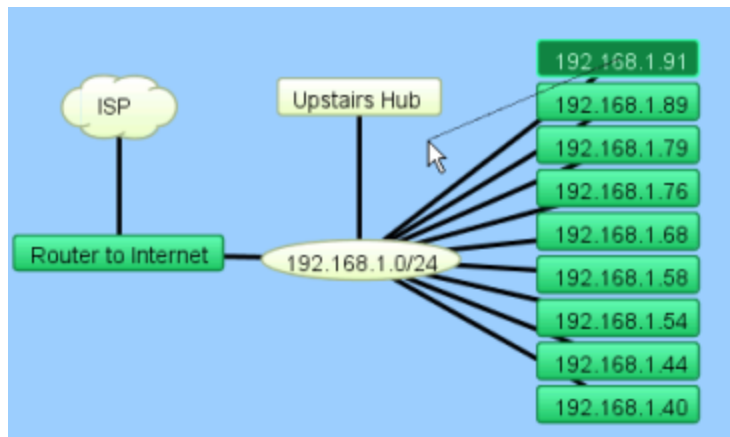


Step 3: Connecting the Hub to the Network

To connect the hub to the network:

1. Select the new rectangle.
2. From the **Insert** menu, select **Link**. A line is displayed, connected on one end to the rectangle and to your mouse cursor on the other. You can also right-click a selected device and select **Attach To** from the device's context menu.
3. Click the network oval below the rectangle. The hub is connected to the network.

A line is displayed, connecting the two items together. This line persists as you move the items around your map.

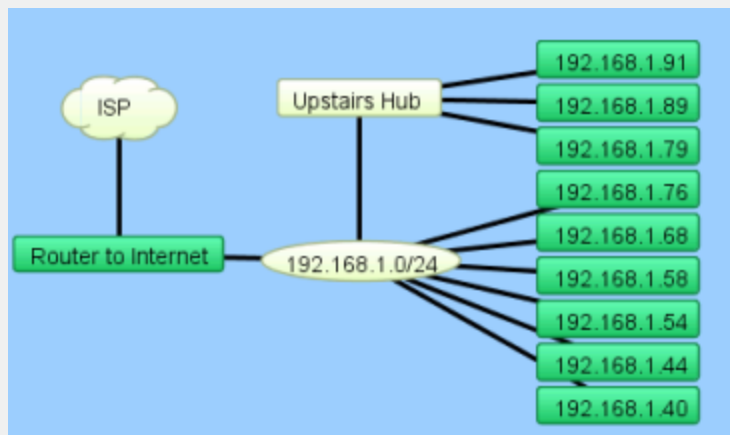


Step 4: Connecting Devices to the Hub

To connect the devices to the hub:

1. Click the link (line) for the first device and drag it toward the **Upstairs Hub** rectangle.
2. Release the mouse button when it is over the rectangle.

The line stays with the new rectangle. Do this for all three links.



Result

Your map should look similar to this after dragging the three links from the oval to the fake hub.

Hiding and Unhiding Details

You can create maps with more detail than you want to see, especially if your network contains one or more switches. This is because Intermapper periodically scans routers and switches and displays newly discovered interfaces. If you delete a network oval from the map, Intermapper no longer polls the associated interfaces.

- Use the **Delete** command to delete one or more networks. Select the networks you do not want to see and select **Delete** from the **Edit** menu or press the **Delete** key on your keyboard. Intermapper does not poll interfaces for deleted networks.

- Use the [Create sub-maps](#) to hide details, but continue to monitor its state and view it occasionally. You can create separate maps containing the details you want to hide and make a new map with devices which use the [Map Status probe](#). Each device represents a submap.
- Use the [Interfaces window](#) to hide or show interfaces. When you hide an interface, it is no longer polled and alerts are not sent.

Notifiers and Alerts

Intermapper can send different kinds of notifications to alert the network manager of network problems. You can configure an entire map to use a default notifier (or set of notifiers) and to apply a custom notifier to individual devices.

What is a Notifier?

Notifiers watch the state of one or more devices and perform a specified action when the device changes to a certain state. The action is called a notification.

You can attach notifiers to a device and specify which states (down, up, warning, alarm, critical) should trigger the notifier. When a device changes to the specified state, the notifier is triggered and Intermapper sends the notification.

For example, you can create a notifier that sends an email message. You can attach that notifier to a device. You might also specify that it should be triggered when the device goes down or comes back up. When the device goes into either of those states, an email message is sent.

Notifier Types

- [E-mail](#) - sends an email.
- [Alphanumeric Pager](#) - sends a page through a dial-up modem using the TAP protocol.
- [Network Paging](#) - sends a page across the Internet using the Simple Network Paging Protocol (SNPP).
- [SMS Alert](#) - sends a text message to a cell phone via SMS.
- [Sound](#) - plays a sound associated with the state of the device.
- [SNMP Trap](#) - sends an SNMP trap to the specified trap receiver.
- [Syslog](#) - sends a message to a syslog server.
- [WinPopup](#) (Microsoft Windows only) - sends a message to the specified user. The message is displayed in a separate window.
- [Command Line](#) - executes a command on the Intermapper host machine.

- **Group** - sends notifications to a group of existing notifiers.
- **PowerShell** - executes a PowerShell command or script on the Intermapper host machine or a remote Microsoft Windows machine.
- **AutoMate** - executes a task created with Fortra' Automate software.

What You Can Do With Notifiers

- The **Notifier List** (Available from the Server Configuration section of the Server Settings window) is a library of notifiers created by you.
- You can **create a notifier** from the **Notifier List** pane, available in the **Server Settings** window.
- You can **configure the notifier** and **test it** to make sure it is working properly.
- You can **attach a notifier** to a device using the Attach Notifier dialog.
- You can **remove a notifier** using the Notifier List.
- You can **define a set of default notifiers** using the Default Notifiers dialog. When you add a new device to a map, the default notifier set is automatically attached to the new device . (You can also create and attach notifiers to individual items.)
- You can attach notifiers only to devices, not to networks.

Parts of a Notifier

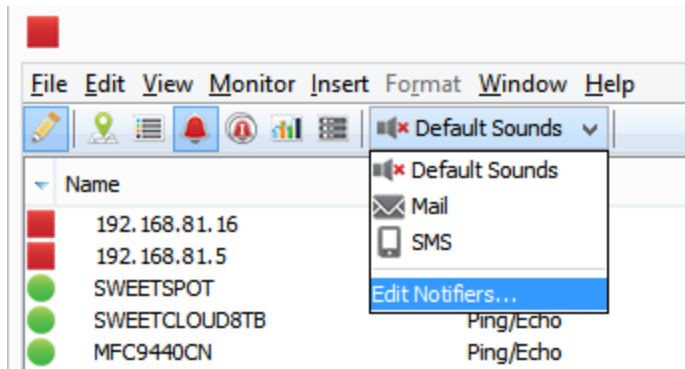
Notifier Name	A human-readable description of the notifier. It is useful to include the type and recipient in the name (for example, Network Techs via email or Syslog to Main Logger).
Notifier Type	The notifier type (email, sounds, traps, and so on). Each notifier you creates a notification or alert, depending on its parameters.
Notifier Parameters	The parameters of a notifier that indicate the recipient or the action to be performed. Parameters can specify an email address, a sound, the address of a syslog or trap server, a pager account, or a script or program to run. Each notifier type determines its parameters.
Notifier Schedule	The schedule associated with the parameter that specifies the days of the week and the hours of each day during which a notifier should send notifications. If an event happens outside the schedule, no notification is sent.

About the Notifier List

The Notifier list is a library of notifiers that you can attach to different devices on your map. It is available from the Server Settings window. You create, configure, edit, remove, and

disable notifiers from the Notifier list. Once you have created and configured the notifiers you want to use, you can attach them to devices.

Occasionally, you might be about to attach a Notifier but discover that you need to create a new one before you can attach it. Open the Notifier list from the Device Notifiers or Link Notifiers view of the map window. Select **Edit Notifiers** from the Notifier menu.



How Notifications Are Sent

When an event occurs, for example, when a device changes to a new state (Up to Down, Warning to Alarm, Alarm to OK) Intermapper triggers the attached notifiers that apply to that new state. The notifier sends a notification, as defined in its parameters, to the specified target users as defined by the notifier schedule.

Working With Notifiers

You can create and configure notifiers in the Notifier List pane, available from the Server Settings window. You can attach notifiers to devices in the Device Notifiers window.

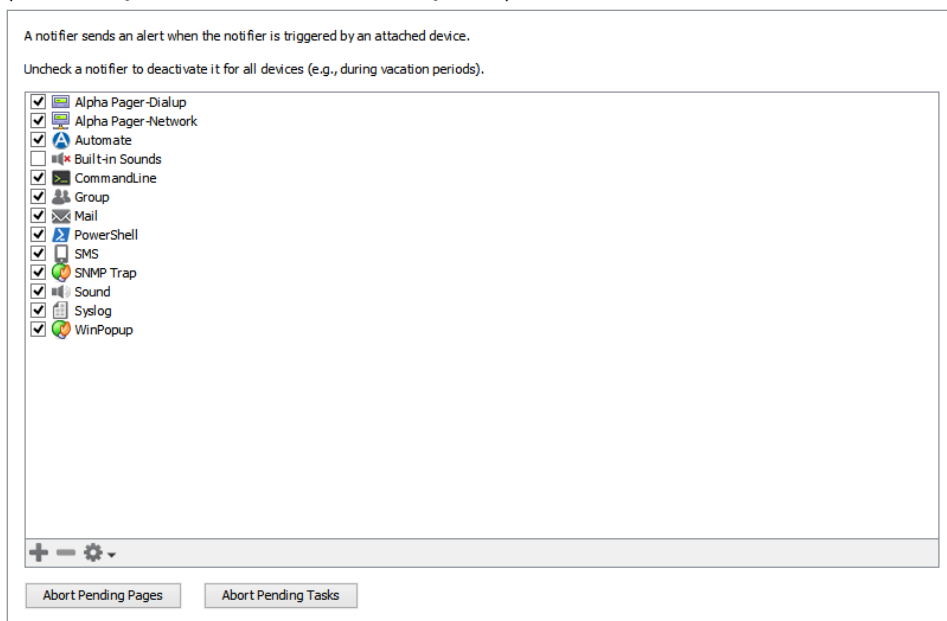
Using the Notifier List

Use the Notifier List to view a list of all notifiers defined for all open maps. You can also use the Notifier List window to do the following:

- Add new notifiers
- Edit existing notifiers
- Copy existing notifiers
- Remove a notifier
- Activate or deactivate a notifier

To view the Notifier List:

- From the **Server Settings** window, select **Notifier List**. The Notifier List is displayed (click/tap the thumbnail to expand).



To add a notifier:

- Click the plus sign **+**. The Configure Notifier window is displayed.
- Configure the notifier and click **OK**.

To edit an existing notifier:

- Select a notifier.
- Click **Edit**. The Configure Notifier window is displayed, showing the current configuration of the selected notifier.
- Edit the configuration and click **OK**.

To copy an existing notifier:

- Select a notifier.
- Click **Duplicate**. The Configure Notifier window is displayed, showing the current configuration of the selected notifier.
- Edit the configuration and click **OK**.

To remove a notifier:

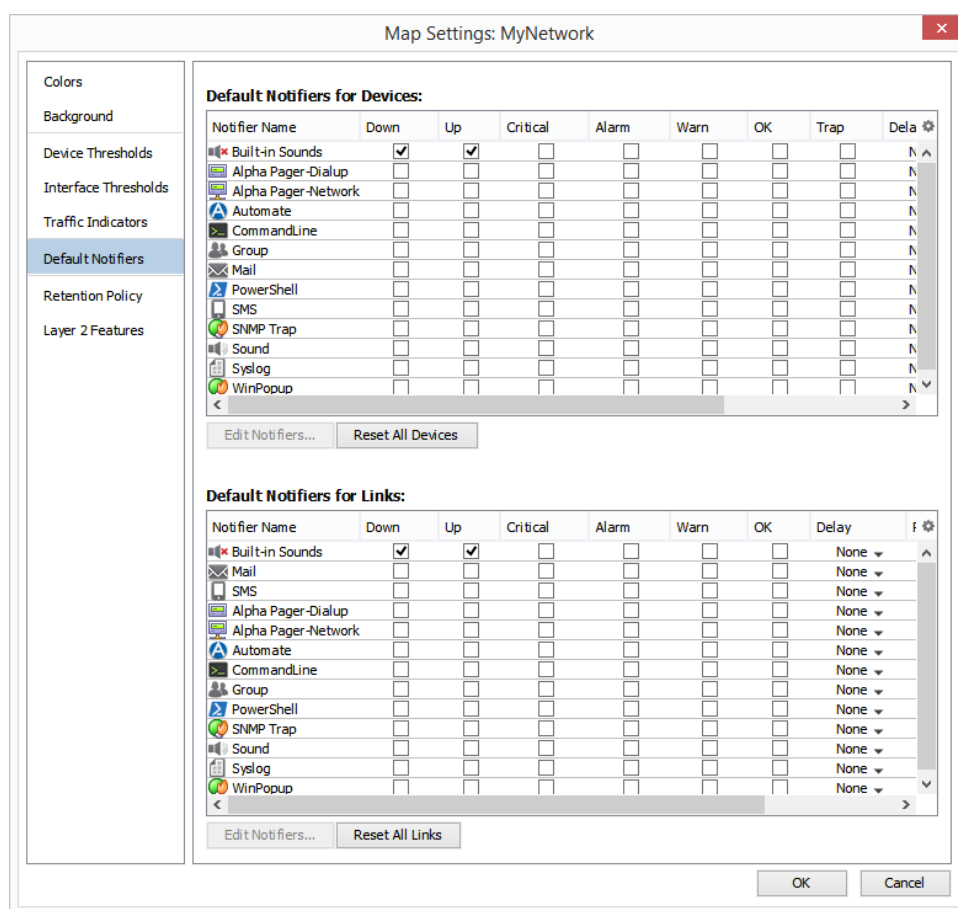
- Select a notifier.
- Click **Remove**. A confirmation dialog is displayed.
- Click **Remove**. The selected notifier is removed from the Notifier List.

To activate or deactivate a notifier:

Select or clear the check box to the left of the notifier name in the notifier list. When deactivated, the notifier never triggers notifications. This is useful for vacation periods or other times when you do not want the notifier to be used.

Defining Default Notifiers

You can define a set of default notifiers for a map that is attached automatically to any new device or link that is added to the map. For existing devices or links, these settings also affect all but those devices and links that have been set manually to use another set of notifiers.



Use the Default Notifiers pane, available from Map Settings window, to define a set of default notifiers to apply to devices or links in a particular map.

You can create one or more notifiers to attach to every device. When the status of the device or link changes to a specified state, the notifier automatically sends a notification.

Intermapper ships with one default notifier, called Built-in Sounds. It plays a default sound when a device goes down and another sound when the device comes back up.

To create a set of default device or link notifiers:

1. From the **Edit** menu, select **Map Settings**. The Map Settings window is displayed.
2. In the left pane, click **Default Notifiers**. The Default Notifiers pane appears, showing two check boxes, one for devices and one for links, each containing a list of defined notifiers. Each check box contains a set of columns with a check box for every possible device or link state.
3. For each notifier you want to attach to new devices or links, select the check box for each state you want to trigger that notifier.
4. Click **OK**. The specified notifiers are automatically attached to each device or link on your map and to all new devices or links added to the map.

Resetting All Devices or Links to the Default Set

NOTE: In versions of Intermapper prior to 6.4, changing default notifiers affected only new devices or links; it did not change notifiers already attached to existing devices.

With versions later than 6.4, changing the default notifier set changes all devices or links in the map except those that have been manually set to use another set of notifiers.

- To attach the default notifier set to all the devices on the map, including those that have been set manually, click **Reset All Devices**.
- To attach the default notifier set to all the links on the map, including those that have been set manually, click **Reset All Links**.

Attached notifiers are replaced with the default notifier set.

Attaching Notifiers to Multiple Devices

To change all device or link notifiers on a map:

Select all items on the map and open the **Device Notifiers** window from the **Monitor** menu, or Alt-click or Cmd-click (Mac) the context menu. Your changes are applied to the selected map items.

To change all link notifiers on a map:

Select all items on the map and open the **Link Notifiers** window from the **Monitor** menu, or Alt-click or Cmd-click (Mac) the context menu. Your changes are applied to the selected

map items.

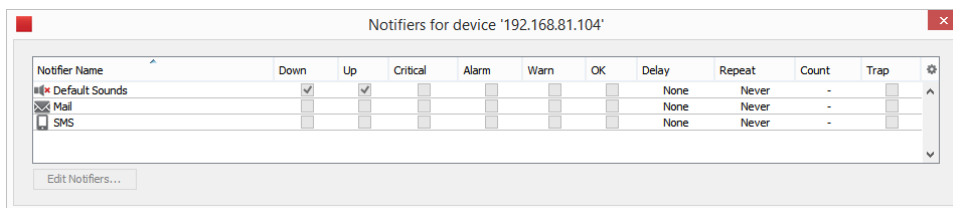
Attaching a Notifier to a Device or Interface

Attaching a Notifier to a Device

You can attach one or more notifiers to any device. For each notifier, you can specify which states trigger a notification. For example, a device might have a notifier send an email when a device goes down, but can have a second notifier that plays sounds when the same device goes down, comes up, or enters an alarm state. You can also send an email to an on-site system administrator during the day and to a different administrator outside business hours.

To attach a notifier to a device:

1. Select one or more devices.
2. From the **Monitor** menu, select **Device Notifiers** or right-click a device in the **Map List** or **Device List** view of the **Map** window. The Notifiers for device(s) window is displayed, showing which notifiers are currently attached to the selected items as shown below.
3. In each notifier row, select or clear the check boxes for the device states you want to trigger. A notification is sent when the device's state changes to any of the selected states for that notifier.



NOTE:

- **Configure a notifier** - Click a row to select a notifier and click **Edit Notifiers**. The Configure Notifier window is displayed.
- Attach all notifiers to selected devices, Alt-click or Cmd-click (Mac) . All check boxes in the column are toggled to the same state. Alt-click or Cmd-click (Mac) a **Delay** or **Repeat** menu and specify a value to set all rows to that value.

Attaching a Notifier to an Interface

You can also attach notifiers to a device's interfaces, so that alerts are sent for a link when that link goes down.

To attach a notifier to one or more interfaces:

1. Select the device containing the interfaces you want to attach notifiers to.
2. View the **Interfaces** window, either from the **Monitor** menu's **Interfaces** submenu, or from the device's context menu's **Interfaces** submenu. The Interfaces window is displayed, showing the device's interfaces .
3. Select the interfaces you want to attach notifiers to, using **Click**, **Shift-click** and **Ctrl-click**. Type **Ctrl-A** to select all of the device's interfaces.
4. Right-click or Ctrl-click (Mac) one of the selected interfaces and select **Notifiers Window** from the context menu's **Interfaces** submenu. The Notifiers for link window is displayed, showing the notifiers and the status they use to attach to the selected interfaces.
5. Select or clear the check boxes for the device states. Set **Delay**, **Repeat**, and **Count** values as needed. A notification is sent when any of the interfaces' states change to one of the selected states.

NOTE:

You can also attach notifiers to interfaces from the Link Notifiers list view of the Map window.

Resetting Devices or Links to the Default Notifier Set

If you change the default device or link notifier set after attaching it to all devices or links, you can reset all devices or links in a map to use the default notifier set.

To reset all devices or links in a map to use the default notifier set:

1. With the map window open, select **Map Settings** from the **Edit** menu. The Map Settings window is displayed.
2. From the left pane, click **Default Notifiers**. A list of notifiers is displayed, showing the default attachment settings used when a new device is added.
3. Do one of the following:
 - Click **Reset All Devices** to attach the default notifier set to all devices in your system.
 - Click **Reset All Links** to attach the default notifier set to all the links in your system.
 A Confirm Notifier Reset dialog is displayed.
4. Click **OK**. All devices or links on the map are set to the default notifier set.

Using Delay, Repeat, and Count Parameters

For each notifier, you can specify Delay, Repeat, and Count parameters. These parameters can be used to control how quickly and how frequently notifications are sent. For example, to avoid unnecessary pages, you can configure a notifier to wait until a device has been down for two minutes before sending the first page. You can also re-send a notifier every 10 minutes indefinitely. Notifications are sent until the count is reached, or until the device is acknowledged.

How Delayed Notifiers work

Intermapper maintains a queue of notifications to be sent. When a DOWN, WARN, ALARM, or CRITICAL event happens, Intermapper places a notification in the queue and sets its time to be sent according to the delay. (UP, OK, and Trap notifications are never delayed.)

When an UP or OK event occurs, Intermapper first searches the notification queue for the corresponding down, warn, or alarm notification. If it is there, Intermapper removes both the DOWN (or Warn or Alarm) notification and UP (OK) event and will not send either one. If not, Intermapper sends the UP/OK notification immediately.

Notification Escalation

You can use notifiers to implement a problem escalation system by creating two or more notifiers for a device. The first notifier can alert someone immediately. A second notifier can be delayed for a period of time, perhaps 30 minutes or an hour, before notifying a second person. If the problem remains when the second notifier's delay time is reached, the second notification is sent. As soon as a problem is acknowledged, no further notifications are sent, even if the outage lasts a long time.

Using Vantage Points

Intermapper can block or suppress notifications for devices that are behind or shadowed by another failed device. This helps to avoid receiving dozens (or hundreds) of notifications for devices that do not respond because there is a router or link down between Intermapper and that device.

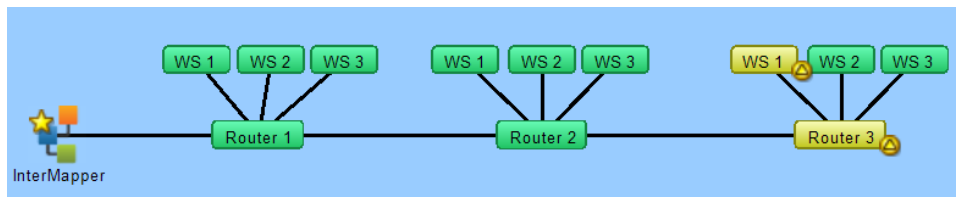
When one device depends on another, you can use this dependency to suppress the notifications for devices that depend on the failed device.

You do not need to set the dependencies manually between devices on a map. Instead, Intermapper follows the links that are already part of the map.

To enable dependencies, [set a Vantage Point \(Pg. 115\)](#). Vantage Point indicates the position from which Intermapper views the network. You usually set the Vantage Point on the actual device where Intermapper is running. After you set the Vantage Point, Intermapper can determine which devices depend on other devices.

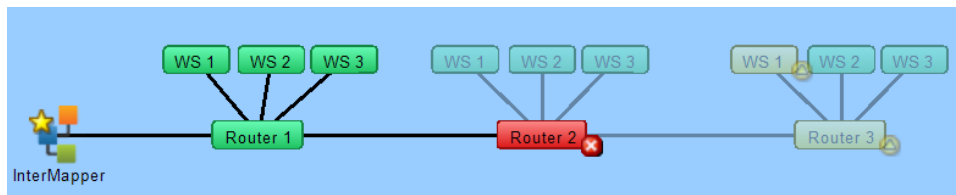
Example 1: All devices are up

The following example shows a map with several interconnected routers. The yellow star on the Intermapper icon shows that it is the map's vantage point.



Example 2: One device is down, shows dependent devices

In the following example, Router2 failed. Intermapper sends the normal notifications for Router2, but it suppresses notifications for any device that depends on it. Icons for the dependent devices are dimmed on the map to show they are shadowed by the failure.



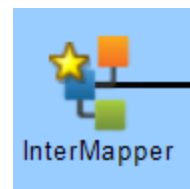
Setting a Vantage Point

To set a map's Vantage Point:

1. Make the map editable.
2. Select the device or network you want to use as the Vantage Point.
3. From the **Monitor** menu's **Set Info** submenu, do one of the following:
 - Select **Set Vantage Point**.

or

- Right-click (or Ctrl-click) a device or network and select **Set Vantage Point** from the context menu's **Set Info** submenu.



A small star is displayed next to the item.

Moving and Removing a Vantage Point

You can remove a Vantage Point or move it to a new item.

To move a Vantage Point to a new item:

Set the **Vantage Point** to the new item as described above.

To remove a Vantage Point:

1. Select the item to which the Vantage Point is currently assigned.
2. From the Monitor menu's **Set Info** submenu, do one of the following
 - Click **Remove Vantage Point**.
 - or
 - Ctrl-click the item to which the Vantage Point is currently assigned and select **Remove Vantage Point** from the **Set Info** submenu.

The star next to the item is removed and no Vantage Point is set. Notifications are sent for all map items.

How Vantage Points Work

When a device goes down (when no response has been received from it), dependencies determine whether to suppress the notification.

Starting at the Vantage Point, Intermapper follows the links to the device in question. If the only path to that device passes through a device, a link, or an interface that is already down, Intermapper knows that the device is shadowed, dims its icon, and suppresses the notifications.

If there is no failure along the path, or if there is no path at all (functional or not) to the device, Intermapper allows the notification to go through.

Even though a device is shadowed (and its notifications are suppressed), Intermapper continually probes the device to show its status.

One Vantage Point Per Map

You can define only one Vantage Point per map. Even if a map does not show the machine on which the server is running, you can use the Vantage Point to indicate the communication path from the Intermapper server to the devices on the map.

This allows Intermapper to know which devices are inaccessible if a switch or router goes down.

Managing Notifications for Dependent Devices

If a device fails but has not been polled, notifications for dependent devices can still be sent even though the failed device is responsible for the failure. This can result in unnecessary and inaccurate alerts.

If this happens, configure the notifiers for the dependent devices to have a delay that is longer than a single polling cycle of the devices. In this setup, the dependent devices do not send an alert if the device on which they depend goes down. An alert is sent only for the failed device.

Configuring Notifiers

Notifiers have the following attributes:

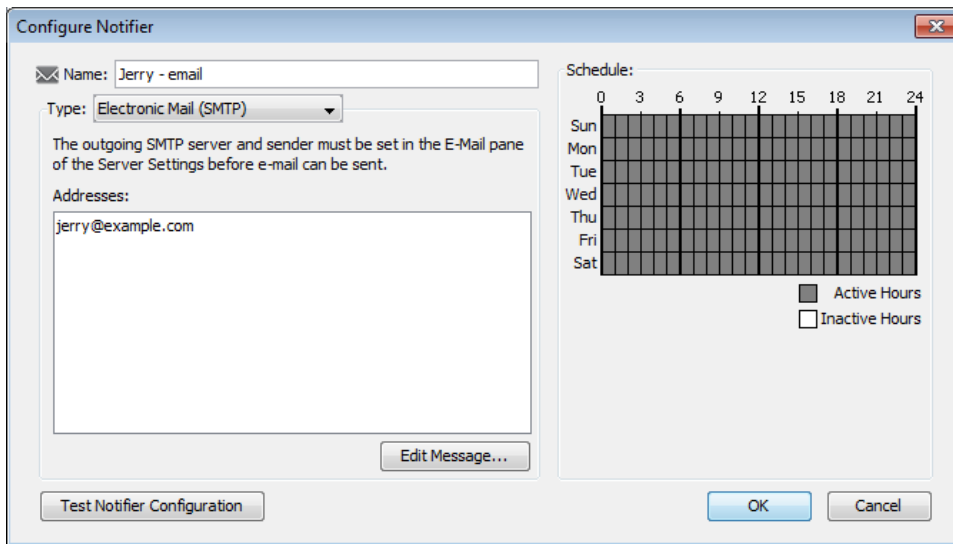
- A notifier name.
- The type of notification to send
- A schedule of hours during which the notification should be sent
- A set of parameters determined by the notification type. This information is required to allow the notification to be sent. For example, an E-mail notifier requires a valid email address.

To configure a notifier:

1. In the **Name** text box, type a notifier name.
2. From the **Notifier Type** menu, select a notifier type.
3. In the **Configuration** panel, specify the configuration information for the selected notifier type.
4. From the **Scheduled Hours** panel, choose the hours during which the notifier is active.
5. Click **Test Notifier Configuration** to send a test notification.

NOTE: The **Test Notifier Configuration** button checks to make sure that the notifier is configured correctly and that a notification is placed in the queue. The notification can fail to be delivered, even when the notifier is configured correctly.

6. Close the **Configure Notifier** window.



- Use the left side of the window to select the notification type and to set the notifier parameters.
- Use the right side of the window to edit the notification *schedule*.

When you select the notifier type from the Notifier Type menu, the left pane changes to show the parameters required for the selected notifier type.

Removing a Notifier

To remove a notifier:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed with a list of settings in the left pane.
2. From the **Server Configuration** section of the **Settings** list, select **Notifier List**. The Notifier List window is displayed.
3. Select the notifier you want to remove.
4. Click **Remove**. A confirmation dialog is displayed.
5. Click **Yes**. The selected notifier is removed from the Notifier List.

Configure Notifier Window Reference

Name

Enter a name in the Name text box. The name can be any descriptive text string.

Tip: If the notifier is active only at certain times of the day or week, you can include a description of the time period as well. For example, you could assign names such as Weekend Pager and Second Shift Pager to notifiers that had those time schedules.

Notifier Type

From the Configure Notifier window's Notifier Type menu, select a notifier type. For more information, see [Notifier Types \(Pg. 106\)](#).

Scheduled Hours

Select a range of hours during which this notification should be sent.

- Active hours are shown in gray.
- Inactive hours are shown in white.

To set a range of hours:

- Click and drag across a range of hours.
- Click and drag across all blocks to invert the selection.

To add or remove hours from the schedule:

Click an individual cell to make it active or inactive.

To activate or deactivate all hours in the schedule:

- Double-click the **Active Hours** legend to activate all hours in the schedule.
- Double-click the **Inactive Hours** legend to deactivate all hours in the schedule.

To edit the message sent with the notification:

Click **Edit Message**. The [E-mail Notification page \(Pg. 106\)](#) shows the editing interface.

NOTE: You can also use Intermapper variables and Javascript to insert information dynamically into a notifier message or subject. For more information, see [Dynamic Label & Alert Text](#).

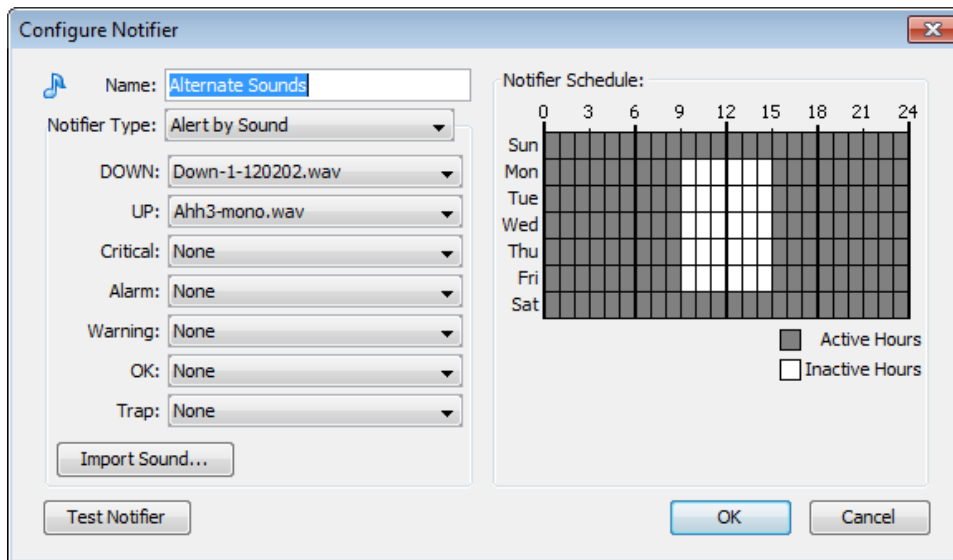
Test Notifier

From the **Configure Notifier** window, click **Test Notifier**. The notification is sent immediately, with the state of Test.

After you create notifiers, you can attach them to all devices (the default notifier is used for all new devices) or to one or more devices.

Configuring a Sound Notifier

A sound notifier plays a sound whenever a device enters a new state. For each state, you can assign a different sound.



To configure a sound notifier:

1. Create or edit the notifier you want to configure.
2. In the **Notifier Type** menu, select **Alert by Sound** if it is not already selected. The Sound Notifier configuration panel is displayed.
3. For each state, use the **Sound Name** menu to select the sound you want to play when the device changes to that state. If you do not want sounds to play for certain states, set those states to **None**. The states are described below.
4. If the sound you want to use for a particular state does not appear, click **Import Sound** to import a sound file containing the sound you want to use.

NOTE:

- On Microsoft Windows machines, available sounds are located in the Intermapper Settings/Sounds folder.
- On macOS machines, available sounds include any system sounds or the sound files in /System/Library/Sounds folder, as well as those in the /InterMapper Settings/Sounds folder.
- Supported sound file formats: .WAV, .AIF, and .AU.
- Intermapper RemoteAccess must download each sound file from the Intermapper server, but after it is downloaded, it is cached on the remote machine. Bear in mind that large sound files can affect system performance for remote users.
- Sounds are queued up for playing. One sound does not start until the previously queued sound is completely finished playing. Relatively short sound files are recommended.

Device States

The following device states are available:

- **Up** - Plays a sound when a device responds normally after being down.
- **Down** - Plays a sound when a device goes down (fails to respond to Intermapper's queries).
- **Critical** - Plays a sound when a device enters Critical state.
- **Alarm** - Plays a sound when a device enters Alarm state.
- **Warning** - Plays a sound when a device enters Warning state.
- **OK** - Plays a sound when a device is no longer in a critical, alarm, or warning state.
- **Trap** - Plays a sound when Intermapper receives an SNMP trap from the device.

The following states are default sound notifiers:

- **Down** - plays the Klaxon sound
- **Up** - plays the Yahoo sound
- **None** - all other states

What You Can Do With Sounds

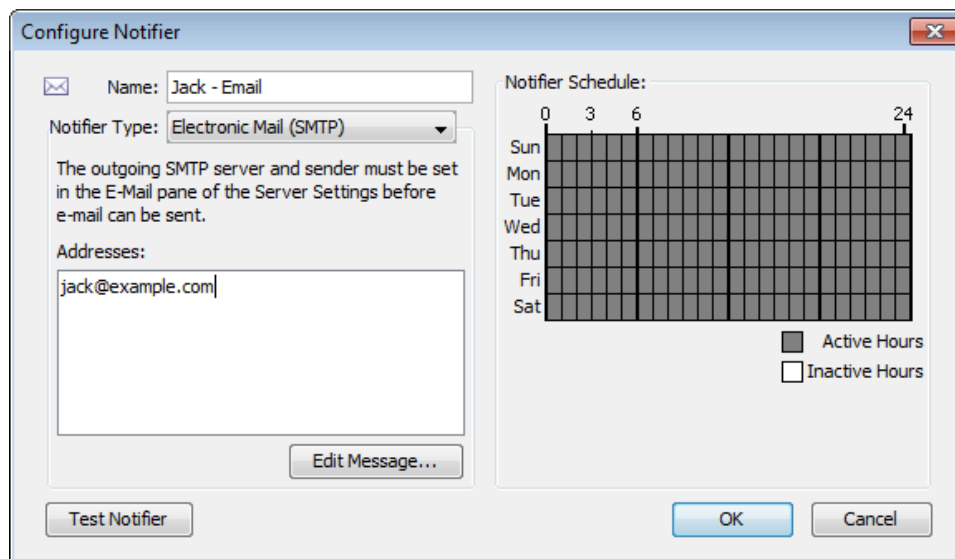
You can use sounds to help give you audible indicators the condition of your network in the following ways:

- **Create different sound sets for different times of da, or for different days** - creates different sound notifiers, each having a different notifier schedule. This can be helpful if you need to, for example, use certain notification sounds during working hours in a busy office, and have louder, more easily distinguishable sounds outside working hours, when you are working away from your computer.
- **Create different sound sets for certain devices** - creates sound notifiers for certain kinds of devices, and use different sounds. You can tell without looking if, for example, a certain machine or router goes down. It is also useful if you have trouble with a particular device.

Sound files must be placed in the Intermapper Settings/Sounds folder before they are available in the Server Configuration Notifier List panel of the Server Settings window.

Configuring an Email Notifier

Use an email notifier to send an email message to one or more recipients. The email message can provide detailed information about the device that triggered the notifier. The following example shows the Configure Notifier window for the Email notifier type:



To configure an e-mail notifier:

1. In the **Configure Notifier** window, select **Electronic mail (SMTP)** from the **Notifier Type** menu.
2. In the **Address** text box, type the email address you want to receive the notification. You can enter multiple addresses, separated by commas, spaces, tabs, newlines, or carriage returns.

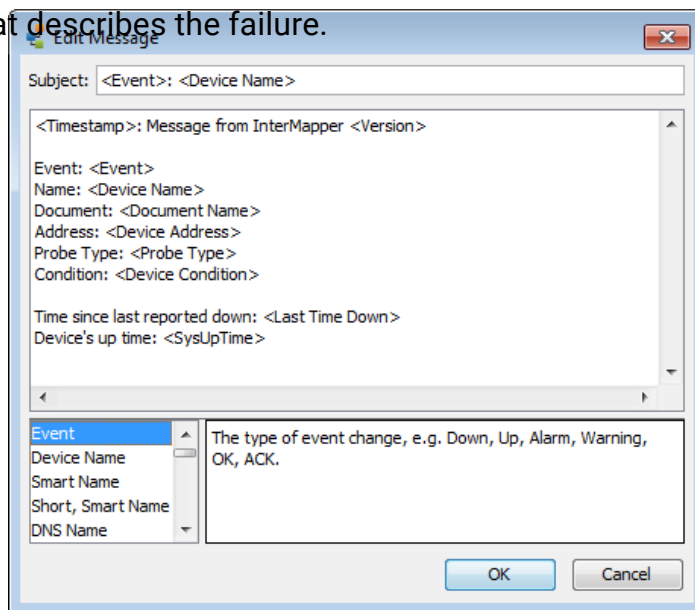
NOTE: Email messages are sent using an outgoing SMTP mail server. Before InterMapper can send email notifications, you must specify the SMTP host you want to use for sending email notifications. For more information on how to specify your outgoing SMTP mail server (and a backup server), see [E-mail Preferences \(Pg. 236\)](#).

Editing the Text of an Email Notification Message

An E-mail notifier sends a text message that describes the failure.

Use the Edit Message window to edit the message sent by the notifier. The example below shows the Edit E-mail Message window containing the default email message. The list at the lower left contains variables you can substitute in the text.

Double-click an item to insert it into the message text. When the notification is sent, the inserted item is replaced with its current value in the message text.



Subject : <Event>:
 <Device Name>

Message: <Timestamp>:
 Message from InterMapper <Version>
 Event: <Event>
 Name: <Device Name>
 Document: <Document Name>
 Address: <Device Address>
 Probe Type: <Probe Type>
 Condition: <Device Condition>
 Time since last
 reported down: <Last Down>
 Device's up time: <SysUpTime>

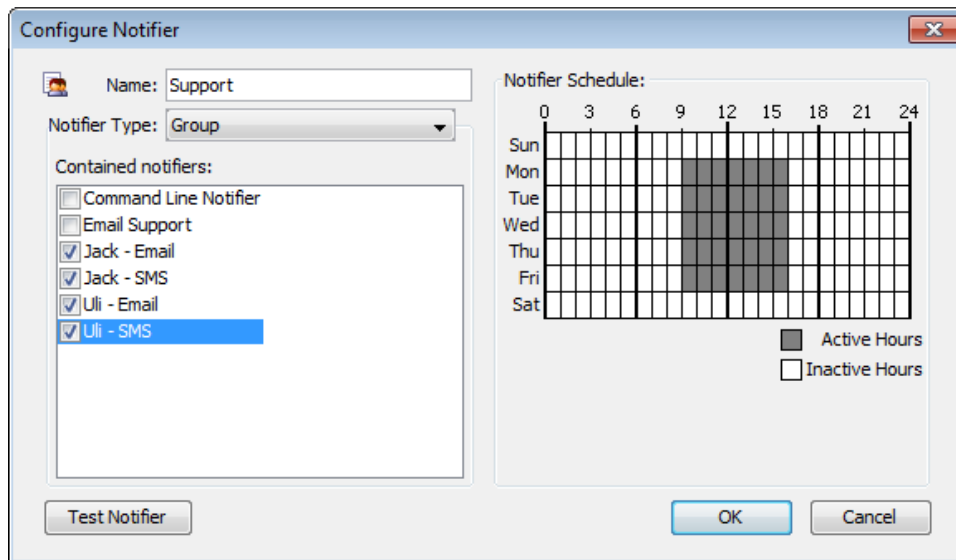
NOTE: You can also use InterMapper variables and Javascript to insert information dynamically into a notifier's subject or message text. For more information, see [Dynamic Label & Alert Text](#).

Using Group Notifiers

InterMapper can group notifiers together so that a transition to a particular device state

sends multiple notifiers, even of different types, for that event.

To create a Group notifier, select **Group** from the **Notifier Type** menu. A set of currently-defined notifiers is displayed, with a check box next to each. To create the group notifier, select the appropriate check boxes from the list.



How it Works

When the Group notifier is invoked, Intermapper first checks the time schedule. If the time is applicable, Intermapper invokes each of the checked notifiers. They then check their schedules and send the notification as appropriate.

NOTE:

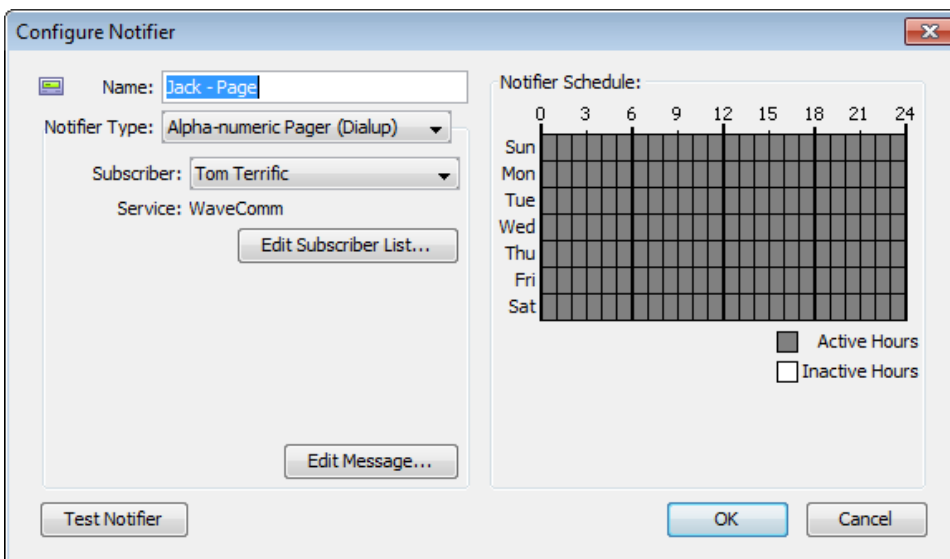
- It is normal for a group notifier's schedule to be 24 x 7, so that the underlying notifiers govern when they are sent.
- When attaching a group notifier to a device, clear its component notifiers' boxes. Otherwise, duplicate notifications are sent (once for the group and again for the component).

Configuring a Pager Notifier to Use an Analog Modem

Intermapper uses TAP, the Telelocator Alphanumeric Protocol, with an internal or external analog modem to connect to a page service, and to deliver a notification.

To use the built-in support for paging with analog modems:

1. [Create a new notifier \(Pg. 109\)](#).
2. From the **Notifier Type** menu, select **Alpha-numeric Pager (Dial-up)**. The example below shows the Configure Notifier window with the Alpha-numeric Pager (Dial-up) type.
3. From the **Subscriber** menu, select a **subscriber**, or select **Edit List** to add or edit paging services or subscribers.
4. Click **Edit Message** to edit the message that is sent to the pager. (See warning below.)
5. In the **Notifier Schedule** panel, choose the hours during which the page is sent.
6. Click **OK**.



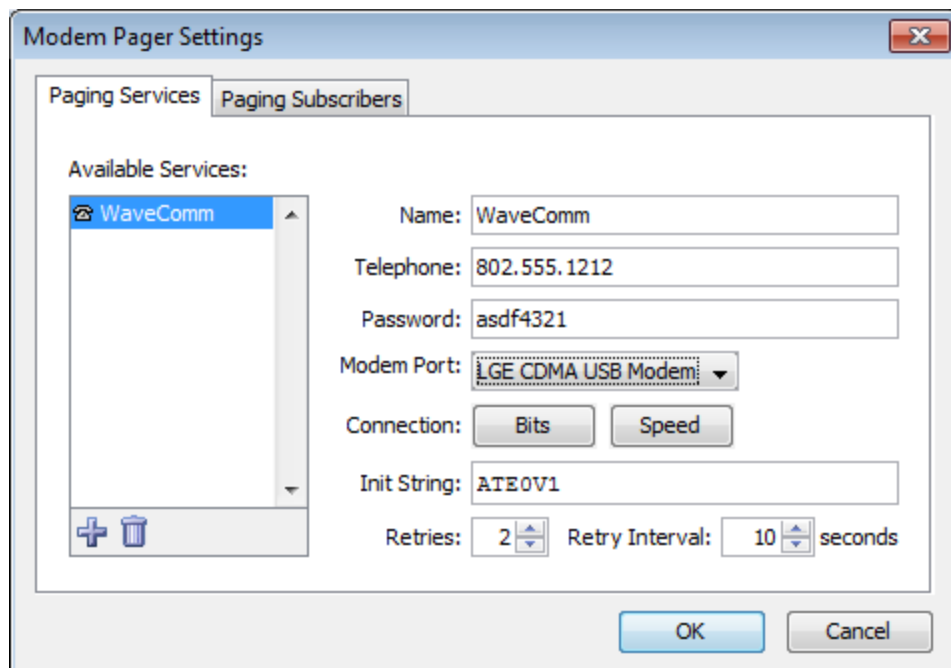
Warning: Many paging services limit the message length. Sending a longer message can cause multiple pages per event and can considerably increase your pager bill.

Configuring Paging Services and Subscribers

Before you can use the paging options, do the following:

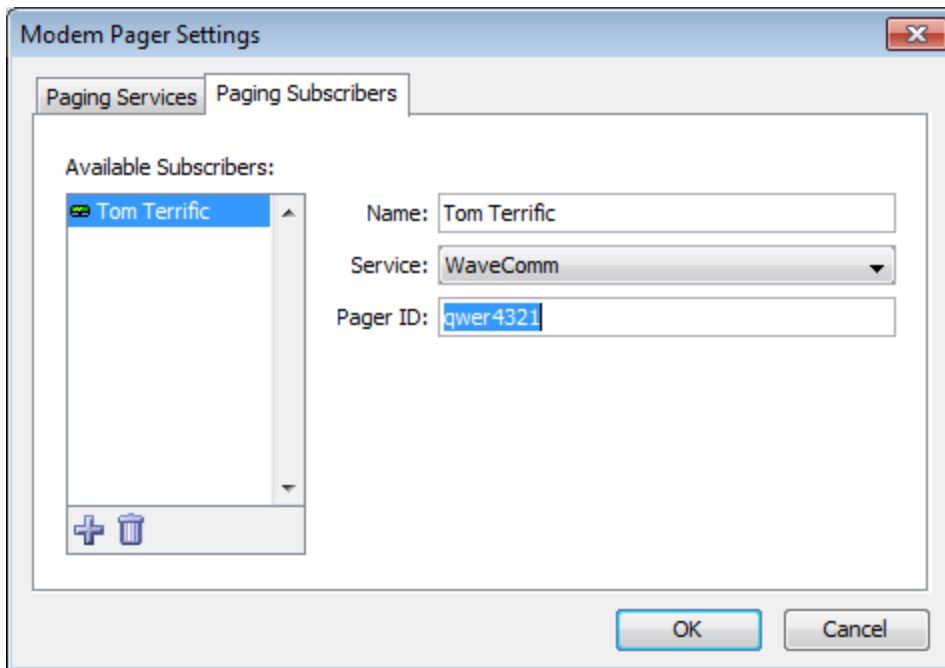
- Set up one or more paging services.
- Set up one or more subscribers for that service.

The window above assumes that you have already configured Intermapper for your pager service.



To add or edit paging services:

1. Choose **Edit List** from the **Subscriber** menu. The Paging Settings window is displayed.
2. Click the **Paging Services** tab. A list of paging services is displayed, if any are defined.
3. Click a service to edit, or click **Add**. The information for the paging service is displayed.
4. Specify the dialup information in the text boxes. Use the information about your paging service to enter the service name, telephone number, password, the port to which your modem is attached, and the modem configuration.
5. From the **Bits** menu, specify the values for your modem. Open the menu repeatedly to set the data bits, stop bits, and parity. By default, the values are set to 7 data bits, 1 stop bit, and Even parity.
6. In the **Retries** text box, specify the number of times you want the page to be sent if it fails. The default is 2.
7. In the **Retry Interval** text box, specify the number of seconds to wait between retries. The default is 10 seconds.
8. Click **Done**.



To add or edit paging subscribers:

1. Select **Edit List** from the **Subscriber** menu. The Paging Settings window is displayed.
2. Click the **Paging Subscribers** tab. A list of paging subscribers is displayed, if any are defined.
3. Click a service to edit, or click **Add**. The information for the paging service is displayed.
4. In the **Name** text box, type the name of the person you want to receive the page.
5. From the **Service** menu, select the user's Paging Service. If the user's paging service does not appear, you need to create it as described above.
6. In the **Pager ID** text box, type the person's pager ID. (This might be different than the Service phone number that you entered when creating the user's Paging Service definition above.)
7. Click **Done**.

Paging Log File

The paging log file is a special file that receives logging of all paging traffic and messages, including the details of the modem commands and written and read text. The information in this log can help you or InterMapper Technical Support to troubleshoot paging if it is not working correctly.

To start logging this traffic, use the Log Files server settings panel to create a log file named Paging (The log file name is called Paging<date>.txt). Logging continues until the log file is removed through the Log Files panel.

Modem Compatibility

macOS

Intermapper has been tested with macOS using various built-in modems, an external USB modem (MultiTech MT5634ZBA-USB), and an older external modem connected via a KeySpan Twin Serial adapter (using KeySpan's current macOS driver) on a beige G3. With the KeySpan serial adapter, Intermapper lists both serial ports in the Modem Page Settings dialog and you are responsible for selecting the correct one.

Microsoft Windows

A number of modems have been tested with Intermapper. While we cannot guarantee that a particular modem works, we believe that most modems that support V.34 or a later specification will work well.

Sending SMS/Text Alerts to a Cell Phone

Intermapper can send SMS or text message alerts to a cell phone, mobile phone, or wireless phone. These notifications are sent using an analog modem to dial a TAP paging terminal at your wireless provider.

NOTE: The methods described below depend on an analog modem dialing a TAP service or a cell phone. You can also use a cell modem to send SMS message directly to another cell phone. For more information, see [Configuring an SMS Notifier](#).

The following methods are available for sending alerts to a mobile phone.

Telelocator Alphanumeric Protocol (TAP)

Intermapper can send SMS or text messages using Telelocator Alphanumeric Protocol (TAP) with an internal or external analog modem. It connects to a paging service and delivers a notification or alert to your cell phone.

Using TAP to Send a Message

If your paging service provides a TAP paging terminal that forwards pages as SMS or text messages to your wireless phone.

To configure Intermapper to send alerts to your phone:

1. From the **Server Settings > Notifiers List** window, click **Add**. The Configure Notifier window is displayed.
2. From the **Notifier Type** list, select **Alpha-numeric Pager (Dialup)**.
3. Click **Edit Subscriber List**.
4. From the Paging Services tab, click **Add**. Type the name of the service, the phone number to dial (including any numbers you might need to access an outside line), and a password. Accept the default values for **data bits**, **stop bits**, **parity**, and **speed** unless your paging service provided you with different values.
5. From the Paging Subscribers tab, click **Add**. Type the **subscriber name** and select the paging service you created in step 4. In the **Pager ID** text box, type the subscriber's cell phone number.
6. Click **OK** to return to the Configure Notifier window.
7. Click **Edit Message** if you want to change the text message. Edit the message and click **OK**.
8. Edit the notifier schedule, if required.
9. Click **Test Notifier** to confirm that the message can be sent and received.
10. Click **OK**.

NOTE: This procedure has been tested using Verizon's TAP access to their SMS/text message system. The access number is 866-823-0501. Other cell providers might offer a gateway to their text/SMS message service.

Sending a Message if TAP is Not Available

If your cell phone provider does not provide a TAP interface for text messages, you can use an email-based service to deliver the message. You should contact your cell phone provider for details on sending alerts and notifications via email.

NOTE: Remember that sending an alert through email fails if your connection to the Internet is down. See below for a low-tech workaround.

Workaround: When Your Internet Connection Is Down

If your Internet connection is down, but your cell phone provider does not offer access to their text/SMS message system from an analog modem, you can still be notified about problems by creating a new Alpha-numeric Pager (dialup) notifier and enter the cell phone number as the paging service number. This method dials the phone directly. This does not initiate a voice or text/SMS message, but the CallerID lets the recipient know that Intermapper is calling.

Troubleshooting SMS/Text Alerts

If you encounter any problems, Intermapper can create a log file that shows the details of the paging mechanism. This is useful to review or send to tech support.

To create a log file that shows the details of the paging mechanism:

1. Open the **Server Settings > Log Files** window and click **Add** to create a new log file. Name the log file paging.
2. Click **OK**.
3. From the **Configure Notifier** window, test your notifier. The paging.txt file contains detailed logging for the test notification. You can find the paging.txt file in the InterMapper Settings > Intermapper Logs folder on the server. If the information contained in the paging log is not helpful to you, you can send the file with a description of the problem to support@Intermapper.com.

Notification Using a Numeric Pager

You can configure Intermapper to use alphanumeric modem paging to send messages to numeric pagers.

To send numeric pages:

1. Create a new paging service.
2. Create one or more paging subscribers to receive the numeric pages.
3. Edit the notification message as you normally would. Any non-numeric characters are removed.

Step 1: Creating a New Paging Service

To create a new paging service:

1. From the **Edit** menu, select **Server Settings**.
2. From the **Server Settings** window, select **Notifier List**.
3. Click **Add** to create a new notifier.
4. From the **Notifier Type** menu, select **Alpha-numeric Pager (Dialup)**.
5. From **Subscriber** menu, select **Edit List**. The Modem Pager Settings window is displayed.
6. From the **Paging Services** tab, click **Add**. A New Service is displayed in the Paging Services list and an information form for the new service is displayed on the right.
7. In the **Name** text box, type a name for the new service.

8. Leave the service telephone number blank. (This is what tells Intermapper to do numeric paging instead of alpha-numeric paging.)
9. **Data bits, stop bits, parity, and baud rate** are irrelevant and can be set to any valid value.
10. Accept the **modem init string** default of **ATE0V1**.
11. Select the desired modem. You can create more than one such service, if needed.

Step 2: Creating One or More Paging Subscribers

To create a one of more paging subscribers:

1. Click the **Paging Subscribers** tab and create the paging subscriber(s).
2. Set the service field to use the service created in the steps above.
3. Set the pager id to be the phone number used to dial the pager. To the pager id/phone number, append enough of your modem's pause characters (for most modems, this is a comma) to make sure that Intermapper waits until the call has been answered and any introductory message played to send the tones with the numeric message. This varies from service to service.

Step 3: Editing Messages

When creating a notifier based on numeric pager subscribers, edit the message as you normally would, using the Intermapper macros if needed. When the page is sent, all non-numeric characters are removed. For example,

DOWN: 192.168.1.132

becomes

1921681132

Paging Log File

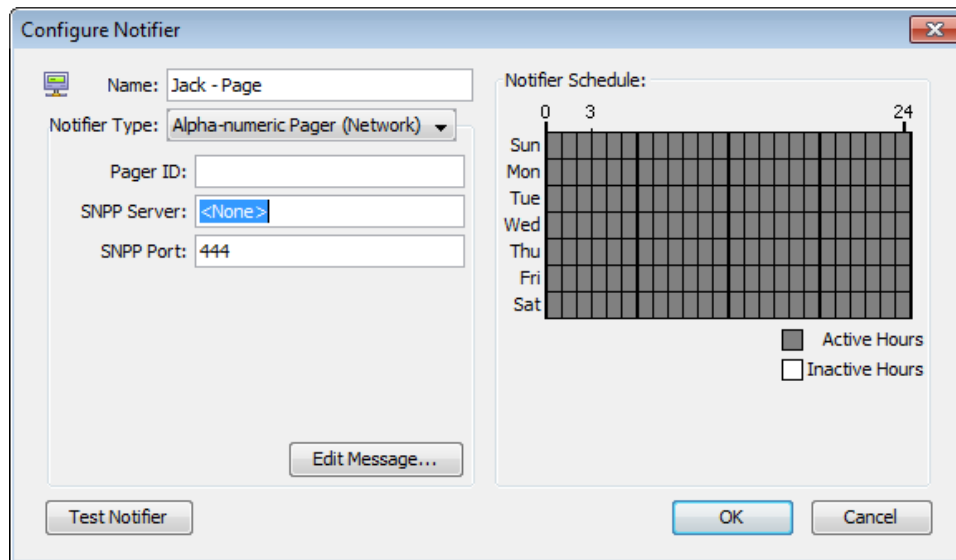
The paging log file is a special file which receives logging of all paging traffic and messages, including the details of the modem commands and text written and read. The information in this log may help you or Intermapper Technical Support to troubleshoot paging if it is not working correctly.

To start logging this traffic:

From the **Log Files** panel of the **Server Settings** window, create a log file called **Paging**. (The log file name becomes Paging<date>.txt.) Logging continues until the log file is removed through the Log Files panel.

Configuring a Page Notifier to Send a Page Using SNPP (Network)

Use Intermapper's Simple Network Paging Protocol (SNPP) feature to send pages over a network. Using this protocol, pages can be sent quickly and reliably, without using an analog modem or a separate telephone line.



To configure a page notifier to send a page using SNPP (network):

1. [Create a new notifier \(Pg. 109\)](#).
2. From the **Notifier Type** menu, select **Alpha-numeric Pager (Network)**. The example below shows the Configure Notifier window with the Alpha-numeric Pager (Network) type.
3. In the **Pager ID** text box, type the ID of the pager to call.
4. In the **SNPP Server** text box, type the IP address or domain name of the SNPP Server.
5. To use a port other than the default SNPP port, type the port in the **SNPP Port** text box.

Contact your pager provider for your IP address, domain name, and SNPP port information.

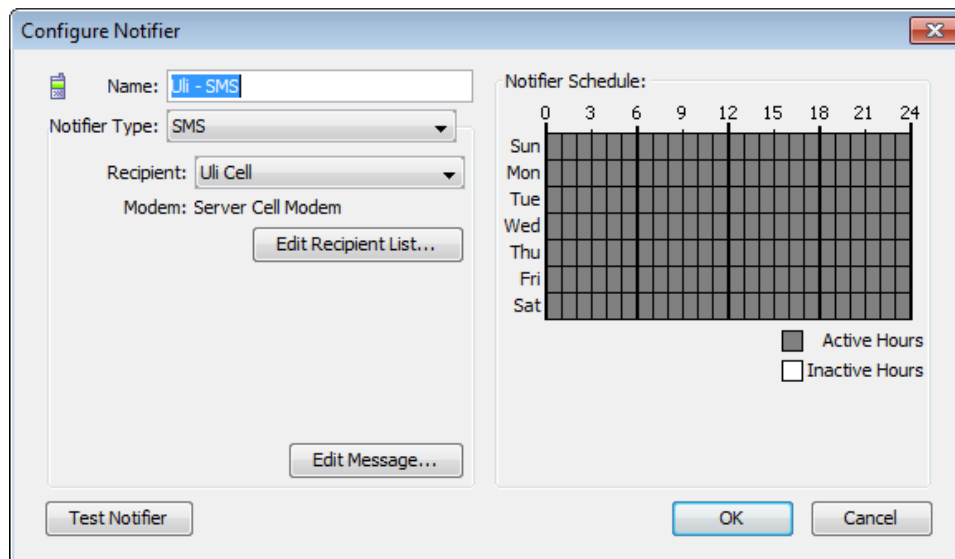
6. Click **Edit Message** to edit the message that is sent to the pager.
7. From the **Notifier Schedule** panel, specify the hours for sending the page.
8. Click **OK**.

NOTE: Intermapper might not be able to reach your SNPP-based paging service through the Internet if your WAN circuits or routers are down. Make sure that you have a backup notification mechanism for failures to critical services. See the workaround in [Alerts Via Cell Phone \(Pg. 129\)](#) for a possible approach.

Configuring an SMS Notifier

You can use an SMS notifier to send a text message directly to a cell phone using a cellular (GSM or CDMA) modem.

NOTE: The modem used to send SMS messages must be able to connect to a cellular network. If there is no coverage at the location of the SMS modem, the server cannot send notifications.

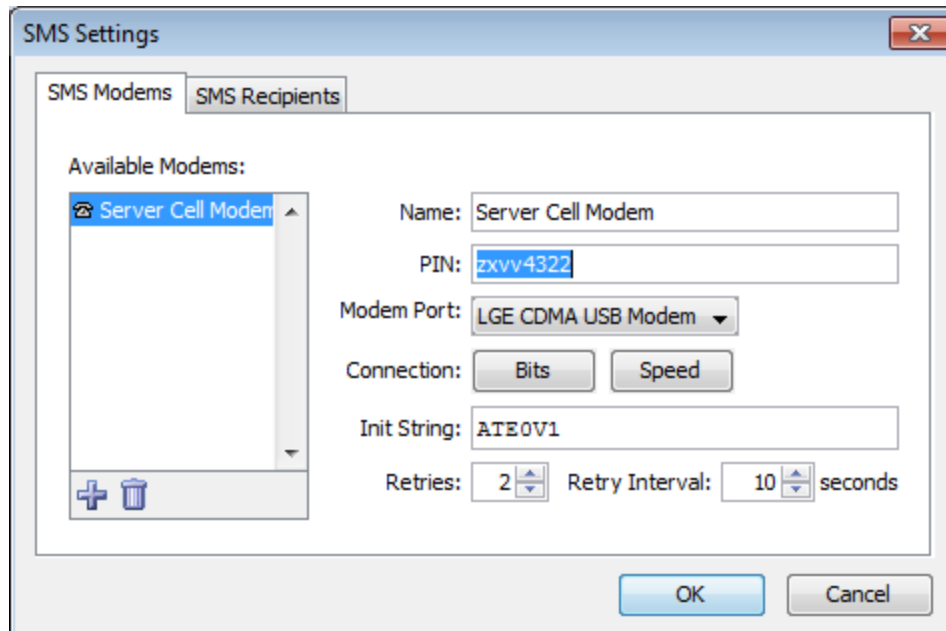


To configure an SMS notifier:

1. In the **Configure Notifier** window, select **SMS** from the **Notifier Type** menu.
2. In the **Recipient** text box, select the recipient from the menu. If there are no recipients in the list, click **Edit Recipient List...** to configure connection to an SMS modem and to add and configure SMS recipients. For more information, see [Adding and Removing SMS Modems \(Pg. 133\)](#) and [Adding and Removing SMS Recipients \(Pg. 134\)](#).
3. Click **Edit Message** to edit the message. For more information on editing messages, see [Editing the Text of an E-mail Notification Message \(Pg. 123\)](#).

Adding and Removing SMS Modems

Before you can send SMS messages, you must set up at least one SMS modem through which SMS messages are sent.



To add an SMS modem:

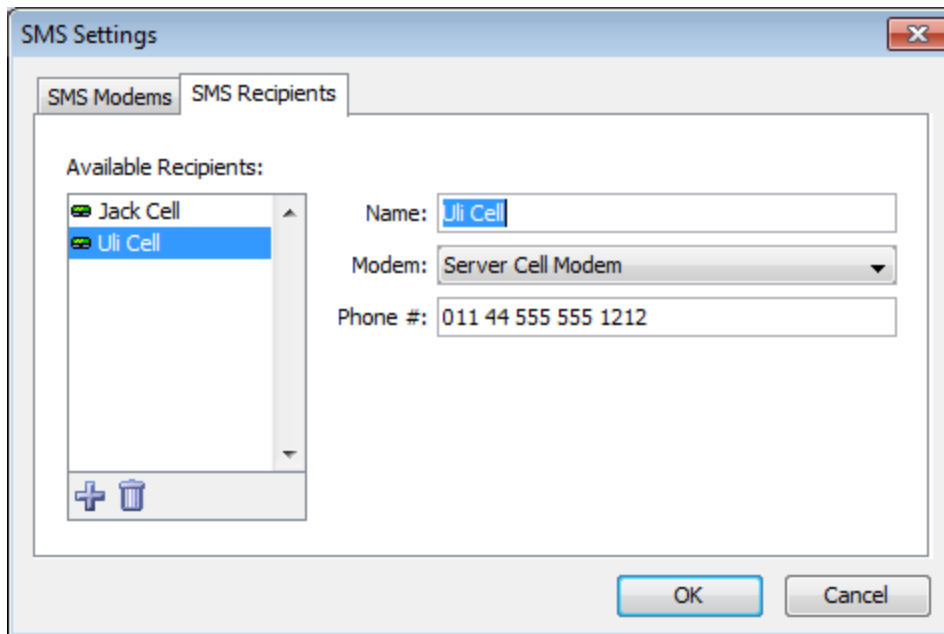
1. From the **Configure Notifier** window, with **SMS** selected as the **Notifier Type**, click **Edit Recipient List**. The SMS Settings window is displayed.
2. From the **SMS** window, click the **SMS Modems** tab. A list of available modems is displayed on the left.
3. Click **Add**. A new modem configuration form is displayed.
4. Type a **Name** and **PIN**, select a **Modem Port**, connection **Bits**, and **Speed**, and type a modem initialization string in the **Init String** text box.

NOTE: Not all cell carriers require a PIN.

5. Specify the **Retries** and **Retry Interval** values to edit the default retry specifications.
6. Click **OK**. The specified modems appear in the recipient's Modem menu.

Adding and Removing SMS Recipients

Before you can send SMS messages, you must set up at least one SMS recipient to receive the message.



To add an SMS recipient:

1. From the **Configure Notifier** window, with **SMS** selected as the **Notifier Type**, click **Edit Recipient List**. The SMS Settings window is displayed.
2. In the **SMS** window, click the **SMS Recipients** tab. A list of available recipients is displayed on the left.
3. Click **Add**. A new recipient configuration form is displayed.
4. Type a **Name**, select a **Modem**, and type the recipient's phone number in the **Phone #** text box.
5. Click **OK**. The specified recipients are displayed in the notifier's menu. The recipient's specified modem is displayed when you select the recipient from the notifier's Recipient menu.

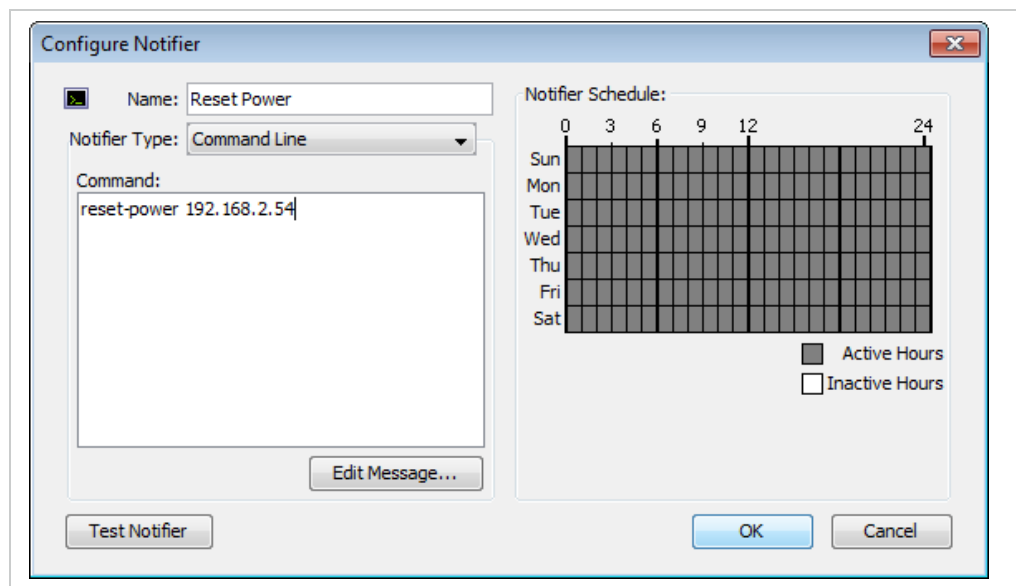
Command Line Notifiers

Use a command line notifier to specify a command (executable, shell script, batch file, and so on) to run as a notification.

To configure a Command Line notifier:

1. In the **Configure Notifier** window, select **Command Line** from the **Notifier Type** menu.
2. In the **Command** text box, enter the command. Include any arguments, exactly as you would type them on the command line.
3. Click **Test Notifier** to send a test notification.

Configuring the Command Line Notifier



Command Text Box

Specify the executable you want to run, including any arguments. Note that you need to specify the exact name, including any extensions such as .exe or .cmd.

If you want the message generated by Intermapper to be included in the command, place the text `${MESSAGE}` where you want the message to go.

NOTE:

Double quotation marks (" ") must be used for special environment variables, such as `"${MESSAGE}"`, when configuring the Command Line Notifier for Intermapper to accept the command.

To include the message escaped for use in an HTTP query string, use `${ESCAPED_MESSAGE}` instead.

NOTE: Intermapper allows an expanded command line (that is, the command line with the path added and the message inserted) up to 65535 characters, but you might find that your host platform limits the command-line size to only 255 characters. For Microsoft Windows users, you can work around this limitation by converting your command-line script to a PowerShell script and use a [PowerShell notifier](#).

Use `${STRIPPED_MESSAGE}` to strip the message of any punctuation that might cause trouble for the command line notifier.

Use `${URLESCAPE}` to escape the message for use as a URL.

NOTE: The command box must refer to an executable which resides in the Tools subdirectory of the InterMapper Settings directory, or a subdirectory. No other executables can be referred to. However, the executables in this directory can be links, shortcuts, or aliases to an executable elsewhere; they can be resolved and executed.

For an example of a command line notifier, see the [Examples page \(Pg. 137\)](#).

Example Notification From a Command Line Program

The following is a simple example of a command line notifier. This notifier does the following:

- Calls a Python script located in the InterMapper Settings\Tools folder.
- Passes the following script parameters:
 - The notification message, using the `${MESSAGE}` macro.
 - A log file filename.
- The script opens the specified file (also located in the Tools folder) and appends the message text to it.

Log.py Script

Place the following script in the Tools folder in a text file called `log.py`:

```
import sys
# options are: message logfile
if __name__ == '__main__':
    f = open(sys.argv[2], 'a+')
    f.write(sys.argv[1]+'\\n')
    f.close()
```

Configuring the Command Line Notifier

To configure a new notifier:

1. Create a new notifier.
2. Set the **Type** to **Command Line**.
3. Enter the following text in the Command text box:


```
${PYTHON} log.py "${MESSAGE}" test.log
```
4. Edit the message and schedule as needed.

5. Click **Test Notifier Configuration**.
6. Attach the notifier to one or more devices as described in [Attaching_A_Notifier.htm](#).

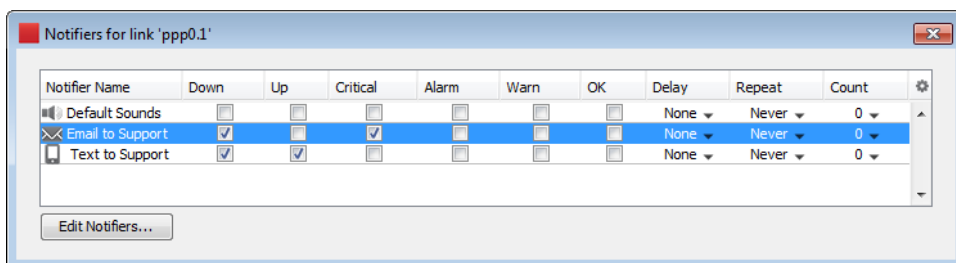
When the notifier runs, a file named `test.log` is created in the Tools folder. Message text is appended to the log file.

Interfaces and Notifiers

You can attach one or more notifiers to one or more interfaces. When the link status changes for any of the interfaces, an alert can be sent.

To attach a notifier to an interface:

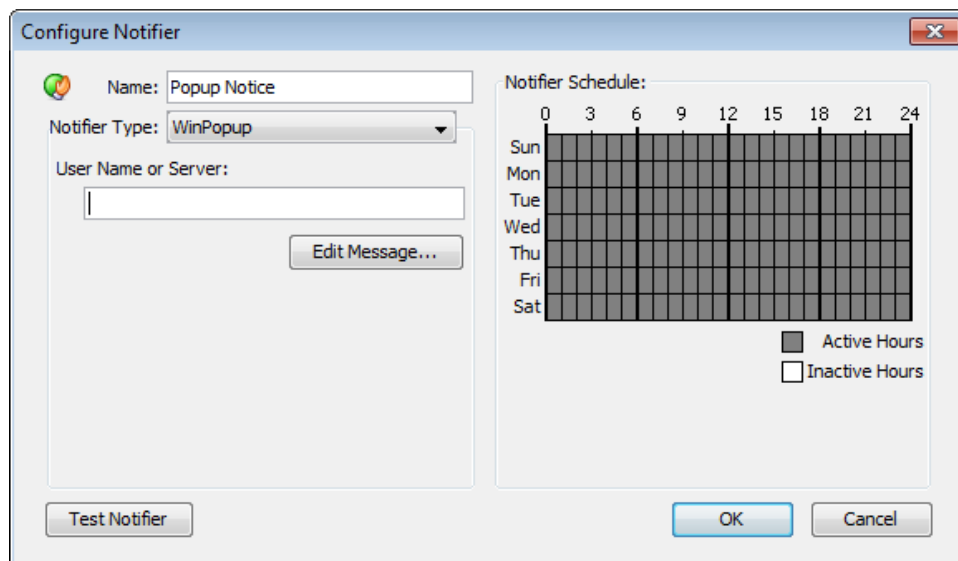
1. [View the Link Notifiers window](#) for the interface you want alerts from.
2. Click the row containing the interface you want to attach notifiers to. The row is highlighted. Select additional rows using Ctrl+click or Shift-click.
3. Right-click or Ctrl-click (Mac) the selected row and select **Notifiers Window** from the **Interfaces** submenu. The **Notifiers for link(s)** window is displayed, showing the notifiers currently attached to the selected interface(s).
4. For each notifier, select or clear the status levels check boxes. Alerts are sent from the selected notifiers when a link status changes to the selected status.
5. Alt-click or Cmd-click (Mac) a check box or choose a value from the dropdown in the **Delay** or **Repeat** column to set the notifiers for all links to the same value.



WinPopup (Microsoft Windows Only)

When the devices status triggers a notification, a WinPopup message is sent to the designated person.

NOTE: Windows Messenger Service is not supported in Microsoft Windows operating systems beyond Microsoft Windows XP, so the WinPopup notifier works only when both the server and the target user or server are running Microsoft Windows 2003 server or Microsoft Windows XP.



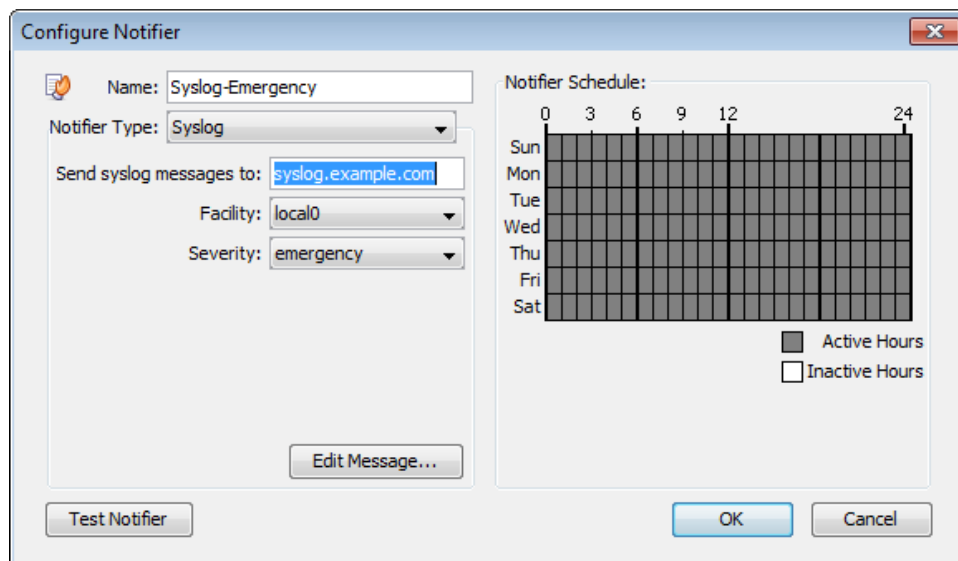
To configure a WinPopup:

1. In the **User Name** or **Server** text box, type the user name or server name of the person to contact.
2. Click **Edit Message** to edit the message.
3. From the **Notifier Schedule** panel, select the time for sending the page.
4. Click **OK**.

Configuring a Syslog Notifier

Syslog records information about significant events into a log file. It originated on Unix hosts that wrote the information to a local file (the system log file). This was later enhanced to write the data across a network to a server that collects the entries.

Intermapper can send a syslog message as a notification. When an event occurs, Intermapper can write the data to a specified syslog server on the network.



Send syslog messages to - the IP address or DNS name of the syslog server that should receive the message.

Facility - the syslog server administrator can specify that messages from a particular source be tagged with a certain facility code. Select the facility requested by your administrator.

Severity - syslog messages can be tagged with a severity so syslog files can be scanned for entries with different priorities. Set the severity to one of the following:

• Emergency	• Error	• Informational
• Alert	• Warning	• Debug
• Critical	• Notice	

Edit message - you can enter the format of the syslog message. For more information on this process, see [Editing the text of an E-mail Notification Message \(Pg. 123\)](#). Newline characters are converted to spaces so the message appears as a single line. Syslog messages contain Intermapper as the syslog tag.

SNMP Trap Notifications

An SNMP trap is an unsolicited SNMP message that is sent to another device. Traps are sent to immediate convey data, instead of waiting for that device to be polled at a future time.

Intermapper sends an SNMP Trap as a notification when a device goes into a particular state.

Configure Notifier

Name:

Notifier Type:

Send traps to:

Community:

Notifier Schedule:

	0	3	6	9	12	15	24
Sun							
Mon							
Tue							
Wed							
Thu							
Fri							
Sat							

☒ Active Hours
☐ Inactive Hours

To configure the notifier:

, do the following:

1. From the **Configure Notifier** dialog, do the following:
 - a. In the **Name** text box, type a name for the trap.
 - b. From the **Notifier Type** list, select **SNMP Trap**.
 - c. In the **Send traps to** text box, type the IP address or the DNS name of the device that is to receive the trap.
 - d. In the **Community** text box, type the user identifier or password that is sent with each SNMP request.

Traps don't usually require community strings, so you can leave this field blank unless the destination host requires a community to accept the incoming trap. The Community is usually blank in a received trap.

Intermapper sends six pieces of information in the trap. All are encoded as OCTET STRING. This information is also available in ASN.1 format. in the [Dartware MIB \(Pg. 151\)](#).

Timestamp:	The current date and time as a string. This field uses the following format: <i>MM/DD HH:MM:SS</i>
Message:	DOWN, UP, ALARM, WARN, OK, or TRAP (See the Dartware MIB (Pg. 151) .)
Device name:	The devices DNS name as a string.

Condition:		The condition of the device, as it is displayed in the log file.
Device Address:		The address of the device that triggered the notifier.
Probe Type:		The type of probe that triggered the notifier.

Intermapper's traps contain the following MIB variables, taken from the Dartware MIB (described in detail in [The Dartware MIB \(Pg. 151\)](#)):

```
IntermapperTimestamp = 1.3.6.1.4.1.6306.2.1.1.0
IntermapperMessage = 1.3.6.1.4.1.6306.2.1.2.0
IntermapperDeviceName = 1.3.6.1.4.1.6306.2.1.3.0
IntermapperCondition = 1.3.6.1.4.1.6306.2.1.4.0
```

AutoMate Notifier

Use the AutoMate Notifier to run an Automate task when specified conditions are met.

A Name:

Notifier Type:

AutoMate System: Local AutoMate Server

Task Path: My Tasks/My Task

Task ID: {91994F97-0615-4...}

Retry Limit:

Retry Interval:

Consolidation Limit:

Consolidation Period:

Connecting to the AutoMate Server

Before you can create an AutoMate notifier, you need to enable the connection to an AutoMate server. The AutoMate server must be running on the same machine as the Intermapper server. For more information, see the section on configuring [AutoMate](#) in the Server Settings.

To configure an AutoMate notifier:

1. From the **Notifier Type** menu, select **AutoMate**. The AutoMate Notifier configuration window is displayed.
2. Click **Edit Task**. The Notifier Task window is displayed.

3. Click **Select Task**.
4. In the **Run By** area, select **Path** or **ID** to specify how to execute the task. Fortra recommends using **ID** because it reduces the traffic between InterMapper and AutoMate.
5. In the **Password** text box, type a password if one is required by the AutoMate task's security configuration.
6. Click **OK**.
7. Specify the **Retry** and **Consolidation** settings.
8. Click **Test** to run the notifier and execute the task.

NOTE: If a task is disabled in AutoMate, the task still appears in the available task list, but does not run when a notifier is triggered.

Retry and Consolidation Settings

Use the Retry and Consolidation settings to specify when to run or retry a task.

- **Retry limit** - the number of times a task is retried after a failure. By default, the value is 0 and the task is not tried again.
- **Retry interval** - the number of seconds between retries.
- **Consolidation limit** - the maximum number of notifications sent before the task is executed. If it is set to 1, a task is executed each time the notification is sent. If it is greater than 1, the task is executed when the number of notifications reaches the Consolidation limit or the Consolidation period is reached.

- **Consolidation period** - the number of seconds to wait for additional notifications before running the task when the Consolidation limit is not zero. After a notification is sent by the notifier, the task is run when the Consolidation limit or the Consolidation period is reached.

NOTE: An AutoMate notifier does not run again until the selected Automate task is complete.

Accessing InterMapper Variables in an AutoMate Task

When an AutoMate notifier runs, InterMapper writes data about the triggering device to a CSV file and grants the AutoMate task access to it. Through this file, AutoMate can access InterMapper variables, which can be used by the task in a wide variety of ways.

Before AutoMate can access this data from an AutoMate task, the task should include the following steps:

1. Wait for exclusive access to InterMapper's CSV file. (A timeout of 30 seconds is recommended.)
2. Read the CSV file into a dataset.
3. Iterate over the rows of the dataset, gathering the data you need.
4. Delete the CSV file.

A sample task that completes these steps is supplied with InterMapper. The file, called `NotifierTest.aml` can be found in the following location:

```
%Installation Folder%\InterMapper\docs\samples\automate\
```

To run the test task:

1. Drag the file mentioned above into the **AutoMate Task Administrator**.
2. Create an Automate notifier.
3. Select the task to run by the AutoMate notifier.

A dialog that shows the received values for all parameters is displayed.

4. Edit the task in the visual editor to see how to access each parameter.

You can access these parameters using the following syntax:

```
%PARAMETERS.[InterMapper variable name]%
```

Available parameters are as follows:

- **Notifier** %PARAMETERS.NOTIFIER% - the name of the notifier.
- **Event** %PARAMETERS.EVENT% - the type of event that triggered the notifier. (Down, Up, Alarm, Warning, and so on.)

- **Name** %PARAMETERS.NAME% - the first line of the device label.
- **ProbeGroup** %PARAMETERS.PROBEGROUP% - the name of the probe group (if any) to which the probe that triggered the notifier belongs.
- **MemberProbe** %PARAMETERS.MEMBERPROBE% - the name of the member probe that triggered the notifier (if the probe is a member of a probe group).
- **Address** %PARAMETERS.ADDRESS% - the address of the device.
- **Status** %PARAMETERS.STATUS% - the status of the device and whether it has been acknowledged.
- **Condition** %PARAMETERS.CONDITION% - the condition of the device.
- **Previous condition** %PARAMETERS.PREVCONDITION% - the previous condition of the device.
- **Probe is** %PARAMETERS.PROBE% - the probe type used for polling.
- **MAC address** %PARAMETERS.MACADDRESS% - the MAC address of the interface associated with the device's address, if the MAC address can be found using SNMP.
- **SysUptime** %PARAMETERS.SYSUPTIME% - the amount of time the system has been up.
- **Last down** %PARAMETERS.LASTDOWN% - the last time the system went down.
- **Time** %PARAMETERS.TIME% - the time the notifier ran the task.
- **Document** %PARAMETERS.DOCUMENT% - the name of the document.
- **Intermapper version** %PARAMETERS.VERSION% - the Intermapper version that was running when the notifier was triggered.
- **SysContact** %PARAMETERS.SYSCONTACT% - the name of the person responsible for the device (if available).
- **SysLocation** %PARAMETERS.SYSLOCATION% - the location of the device.
- **Comment** %PARAMETERS.COMMENT% - a user-defined comment (if any) for the device.
- **Counts** - the total number of devices whose status matches the following states:
 - **down** - %PARAMETERS.DOWNCOUNT%
 - **critical** - %PARAMETERS.CRITCOUNT%
 - **alarm** - %PARAMETERS.ALRMCOUNT%
 - **warn** - %PARAMETERS.WARNCOUNT%
- **Acknowledge message** %PARAMETERS.ACKMESSAGE% - the message when the device was last acknowledged.

- **Send Counts** - the number of times this notifier has been triggered and the maximum number that will be sent.
 - **send count** - %PARAMETERS.SENDCOUNT%
 - **max** - %PARAMETERS.MAXSENDCOUNT%
- **Map ID** %PARAMETERS.MAPID% - the internal Intermapper ID of the map containing the device that triggered the notifier.
- **Device IMID** %PARAMETERS.DEVICEIMID% - the internal Intermapper ID of the device that triggered the notifier.
- **Param** %PARAMETERS.PARAM% - the parameters sent to the task.
- **Nickname** %PARAMETERS.NICKNAME% - the device's DNS name, SNMP SysName, or address, tried in that order. This is also called the Smart Name.
- **Shortened nickname** %PARAMETERS.SHORTNICKNAME% - the first part of the device's DNS name, SNMP SysName, or address, tried in that order. This is also called the Short, Smart Name.
- **Persist name** %PARAMETERS.PERSISTNAME% - the device's domain name.
- **Short name** %PARAMETERS.SHORTNAME% - the first label of the device's domain name.
- **SystDescr** %PARAMETERS.SYSDSCR% - the description of the device and its software as reported by the `systDescr` variable.
- **SysName** %PARAMETERS.SYSNAME% - the name of the device as reported by the `sysName` variable.
- **Enterprise ID** %PARAMETERS.ENTRPRID% - the enterprise ID of the device as reported by the `EnterpriseID` variable.
- **Enterprise serial** %PARAMETERS.ENTSERIALNUM% - the serial number of the device as reported by the `EntSerialNum` variable.
- **Enterprise manuf name** %PARAMETERS.ENTMFGNAME% - the manufacturer name of the device as reported by the `EntMfgName` variable.
- **Enterprise model name** %PARAMETERS.ENTMODELNAME% - the model name of the device as reported by the `EntModelName` variable.
- **Context** %PARAMETERS.CONTEXT% - an internal context description (this might include the IMID of the device, alarm point, current time, notifier type, notifier IMID, event time, event status, or send count).
- **Port Name** - %PARAMETERS.IFPORTNAME% - the name of the port that triggered the notifier.
- **Port Number** - %PARAMETERS.IFPORTNUM% - the number of the interface that triggered the notifier.
- **Interface Name** - %PARAMETERS.IFNAME% - the name of the interface that triggered the notifier.

- **Interface Index** - %PARAMETERS.IFINDEX% - the index of the interface that triggered the notifier.

PowerShell Notifier

Use the PowerShell notifier to execute a PowerShell script when a device meets specified conditions.

NOTE: Before you can run a PowerShell notifier, you must [configure PowerShell to work with Intermapper](#) on the local machine and any target machines you want to access with PowerShell. Use PowerShell probes to test the connectivity.

To configure a PowerShell notifier:

1. In the **Nlame** text box, type a name for the notifier.
2. From the **Notifier Type** menu, select **PowerShell**. The PowerShell Notifier configuration window is displayed.
3. Specify how to execute the script on the local machine (localhost) or a remote machine.
4. In the **PowerShell arguments** text box, enter the arguments to define how the PowerShell process executes. See below for more information.
5. In the **PowerShell command text** text box, type the command you want to execute. See below for more information.

PowerShell Notifier Settings

- **Execution** - Choose how the script or command is executed:
 - **Local** - the PowerShell command text is executed on the local machine.
 - **Alerting Device** - Powershell uses the selected **Authentication** method to connect to the machine that triggered the alert, and executes the specified command text.
 - **Other Device** - Powershell uses the selected **Authentication** method to connect to the machine specified in the **ComputerName** text box and executes the specified command text.
- **User** - For **Local** execution, leave this field blank unless you want to pass credentials to your script, (for example, to use Get-WmiObject). For **Remote** execution, use the credentials of a valid administrator on the remote computer. For networks that do not use a domain controller, a notifier must be created for each unique administrator.
- **Password** - type the password associated with the supplied user name.

- **PowerShell Arguments** - type the arguments to be passed to the PowerShell command. These are command-line arguments used when launching PowerShell. These arguments control how PowerShell executes and are not sent to your PowerShell script.
- **PowerShell Command Text** - type the command to be executed. These are the commands that PowerShell runs when the notifier is triggered.

NOTE:

- The PowerShell Command Text box is limited to 255 characters. Typically this field is used to execute an existing script in a file.
 - Command parameters are passed through STDIN and thus are not bound by a character limit. If you encounter a limit, you can use message variables as arguments, including sending the entire contents of the notifier message as an argument (`${MESSAGE}`). If you use one of these variables, make sure to enclose it in quotation marks, in case it contains whitespace.
 - Relative paths to PowerShell scripts must be relative to the InterMapper Settings\Tools folder.
 - Create additional folders hierarchy within the Tools folder if needed.
 - In the Command Text box, the path to the Tools folder is `./yourscript.ps1`. PowerShell also accepts a backslash, but it must be escaped: `.\yourscript.ps1`.
 - Signed scripts must be run from the InterMapper Settings\Tools folder or in a folder it contains.
-
- The PowerShell Command Text box is limited to 255 characters. Typically this field is used to execute an existing script in a file.
 - Command parameters are passed through STDIN and thus are not bound by a character limit. If you encounter a limit, you can use message variables as arguments, including sending the entire contents of the notifier message as an argument (`${MESSAGE}`). If you use one of these variables, make sure to enclose it in quotation marks, in case it contains whitespace.
 - Relative paths to PowerShell scripts must be relative to the InterMapper Settings\Tools folder.
 - You can create additional folders hierarchy within the Tools folder if needed.
 - In the Command Text box, the path to the Tools folder is `"../yourscript.ps1"`. PowerShell also accepts a backslash, but it must be escaped: `"..\yourscript.ps1"`.
 - Signed scripts must be run from the InterMapper Settings\Tools folder or in a folder it contains.

Available Variables

You can use many InterMapper variables, including \${address}, \${User}, \${Password*}, as well as any of the other information available to Command Line notifiers.

Selecting an Execution Method

The following execution methods are available. Each one determines how the script is executed and what device it is executed on.

- **Local** - the PowerShell command text is executed on the local machine.
- **Alerting Device** - Powershell uses the selected **Authentication** method to connect to the machine that triggered the alert and executes the specified command text.
- **Other Device** - Powershell uses the selected **Authentication** method to connect to the machine specified in the **ComputerName** text box and executes the specified command text.

Default Command Text

When you select an execution method, the **PowerShell Command Text** box is displayed with an appropriate command.

The defaults for each execution method are as follows:

- **Local**

```
./MyPowerShellNotifier.ps1 "${MESSAGE}"
```

- **Alerting Device**

```
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList  
"${MESSAGE}"
```

- **Other Device**

```
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList  
"${MESSAGE}"
```

Change the name of the **.ps1** script and change or add parameters as needed.

Execution: Local Device

The specified command text is executed on the local machine.

The screenshot shows a configuration window for a PowerShell notifier. The title bar says "Name: MyPowerShellNotifier-local". The "Type" dropdown is set to "PowerShell". Under the "Execution" section, the "Local" radio button is selected. The "User" field contains "Fred", the "Password" field is masked with dots, the "ComputerName" field contains "\${address}", and the "Authentication" dropdown is set to "Default". The "PowerShell arguments:" field contains "-ExecutionPolicy RemoteSigned -NoProfile". The "PowerShell command text:" field contains ". /MyPowerShellNotifier.ps1 "\${MESSAGE}"". An "Edit Message..." button is at the bottom right.

Execution: Alerting Device

The specified command text is executed on the machine that triggered the alert.

The screenshot shows a configuration window for a PowerShell notifier. The title bar says "Name: MyPowerShellNotifier-Alerting". The "Type" dropdown is set to "PowerShell". Under the "Execution" section, the "Alerting Device" radio button is selected. The "User" field contains "Fred", the "Password" field is masked with dots, the "ComputerName" field contains "\${address}", and the "Authentication" dropdown is set to "Default". The "PowerShell arguments:" field contains "-ExecutionPolicy RemoteSigned -NoProfile". The "PowerShell command text:" field contains "Invoke-Command -FilePath . /MyPowerShellNotifier.ps1 -ArgumentList". An "Edit Message..." button is at the bottom right.

Execution: Other Device

The specified command text is executed on the machine specified in the **ComputerName** text box.

Name: MyPowerShellNotifier-Other

Type: PowerShell

Execution: ☐ Local ☐ Alerting Device ☒ Other Device

User: Fred

Password: ••••••

ComputerName: \${address}

Authentication: Default

PowerShell arguments:
-ExecutionPolicy RemoteSigned -NoProfile

PowerShell command text:
Invoke-Command -FilePath ./MyPowerShellNotifier.ps1 -ArgumentList

Edit Message...

Dartware MIB

Fortra, LLC registered the Enterprise 6306 for its own SNMP variables. The remainder of this page shows the Dartware MIB in ASN.1 notation.

```
-- *****
-- DARTWARE-MIB for Intermapper and other products
--
-- May 2007
--
-- Copyright© Fortra, LLC
-- All rights reserved.
-- *****
```

```
DARTWARE-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, enterprises
    FROM SNMPv2-SMI
    DisplayString
    FROM SNMPv2-TC;
```

```
dartware MODULE-IDENTITY
    LAST-UPDATED "200507270000Z"
    ORGANIZATION "Dartware, LLC"
    CONTACT-INFO "Dartware, LLC
        Customer Service
```

Postal: PO Box 130
 Hanover, NH 03755-0130
 USA

Tel: +1 603 643-9600

E-mail: support@dartware.com"

DESCRIPTION

"This MIB module defines objects for SNMP traps sent by Intermapper."

REVISION "200705300000Z"

DESCRIPTION

"Updated descriptions to show timestamp format, correct strings for IntermapperMessage."

REVISION "200512150000Z"

DESCRIPTION

"Added IntermapperDeviceAddress and IntermapperProbeType."

REVISION "200507270000Z"

DESCRIPTION

"First version of MIB in SMIV2."

::= { enterprises 6306 }

notify OBJECT IDENTIFIER ::= { dartware 2 }
 Intermapper OBJECT IDENTIFIER ::= { notify 1 }

IntermapperTimestamp OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..255))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current date and time, as a string, in the format 'mm/dd hh:mm:ss'."

::= { Intermapper 1 }

IntermapperMessage OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..255))

MAX-ACCESS read-only

STATUS current

DESCRIPTION

```

    "The type of event - Down, Up, Critical, Alarm, Warning, OK,
or Trap - as a string."
    ::= { Intermapper 2 }

```

```

IntermapperDeviceName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The (first line of the) label of the device as shown on a
map, as a string."
    ::= { Intermapper 3 }

```

```

IntermapperCondition OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The condition of the device, as it would be printed in the
log file."
    ::= { Intermapper 4 }

```

```

IntermapperDeviceAddress OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The device's network address, as a string."
    ::= { Intermapper 5 }

```

```

IntermapperProbeType OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The device's probe type, as a human-readable string."
    ::= { Intermapper 6 }

```

```

-- For SMIv2, map the TRAP-TYPE macro to the
-- corresponding NOTIFICATION-TYPE macro:
--

```

```

-- IntermapperTrap TRAP-TYPE
--   ENTERPRISE    dartware
--   VARIABLES     { IntermapperTimestamp, IntermapperMessage,
--                   IntermapperDeviceName, IntermapperCondition }
--   DESCRIPTION
--       "The SNMP trap that is generated by Intermapper as a
notification option."
--       ::= 1

IntermapperNotifications OBJECT IDENTIFIER ::= { Intermapper 0 }

IntermapperTrap NOTIFICATION-TYPE
  OBJECTS { IntermapperTimestamp, IntermapperMessage,
            IntermapperDeviceName, IntermapperCondition,
            IntermapperDeviceAddress, IntermapperProbeType }
  STATUS current
  DESCRIPTION
    "The SNMP trap that is generated by Intermapper as a
notification option."
    ::= { IntermapperNotifications 1 }

END

```

Monitoring Your Network

After you arrange your map, you can switch it to monitor mode. You might have already noticed that devices are changing colors while you are arranging the map. This shows that Intermapper is already polling devices, even as you are editing the map layout.

Making the Map Editable

To change a map between Monitor mode and Edit mode:

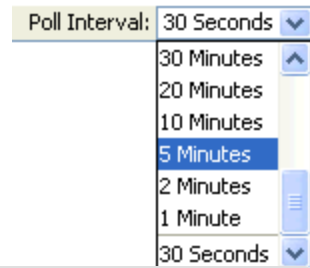
Click the lock button at the left end of the toolbar in the Map window or press **Tab** on your keyboard. The tool switches between locked and unlocked as shown.

Changing the Poll Interval

The Poll Interval menu specifies the polling interval for the map.

To change the Poll Interval:

From the **Poll Interval** menu, select a value.



NOTE:

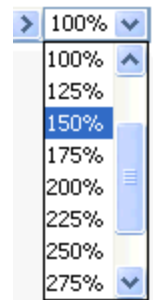
You can change the poll interval for one or more individual devices using the [Set Poll Interval \(Pg. 375\)](#) command, available on the Monitor menu. The poll interval affects only those devices that are using the default poll interval.

Zooming In On the Map

The Map Zoom menu specifies the zoom factor for the map. If you select Auto, the map zooms in automatically when you resize the window.

To change the Map Zoom setting:

Select a value from the **Map Zoom** menu.



Understanding the Map

Intermapper provides visual cues to help you understand the states of the devices on your map. The following visual indicators are available for your map:

- [Color Codes](#)
- [Status Badges](#)
- [Dotted lines \(or "moving ants"\)](#)
- [Boxes and Ovals \(or "bubbles"\)](#)
- [Line Styles](#)
- [Link States](#)

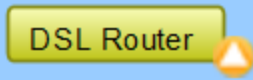
Color Codes

Devices change colors depending on the magnitude of the detected problem. Links can be haloed with yellow or orange as usage reaches 50 and 90 percent respectively. These are coupled with status badges, described below.










These are the default color assignments. You can redefine the colors in the [Server Settings](#) window.



Status Badges

Intermapper uses status badges as additional visual cues to increase the ease with which you can determine the status of devices or links.


 DSL Router

NOTE: You can specify which badges you want to appear in the [Intermapper User Preferences](#) window.

Badge	Color	Meaning
	Red (Flashing)	Down - No response has been received from the device or interface within the specified timeout period.
	Red (Solid)	Critical - The specified threshold for critical state has been met.
	Orange	Alarm - The specified threshold for alarm state has been met.
	Yellow	Warning - The specified threshold for warning state has been met.
	Green	Up - The device is working below the specified thresholds.
	Gray	Unknown - The device is not being polled, so its state is unknown.
	Purple	Searching - The device is searching for adjacent routers (during auto-discovery) or is tracking down unnumbered interfaces.
	Clock	Acknowledge - Timed - The problem with the device or link has been acknowledged and notifications are suppressed for a specified period of time.
	Wrench	Acknowledge - Timed or Indefinite - The problem with the device or link has been acknowledged and notifications are suppressed indefinitely.

	Check mark (devices)	Acknowledge - Basic - The problem with the device or link has been acknowledged, and notifications are suppressed until the device or link comes back up, at which time the check mark or X is cleared.
	Blue X (links)	

Dotted Lines (Moving Ants)

Intermapper draws dotted lines (known as ants) next to a link to indicate that its current traffic flow is above a user-settable threshold value. Use the Thresholds > Traffic panel of the Map Settings window, from the Edit menu to change the settings and to view a legend of the different varieties of ants. You see the ants only in Monitor mode (as opposed to Edit mode.) To toggle between the two modes, click lock in the upper left corner or press Tab on your keyboard.

Intermapper regularly polls all the visible interfaces for packets, bytes, errors, and discards.

NOTE: Intermapper uses SNMP to query the MIB of SNMP-enabled equipment to compute and display the traffic processed by each interface. Traffic indication appears only for SNMP-enabled devices.










Boxes and Ovals (Bubbles)

Boxes represent the physical equipment of your network. Ovals represent the networks which link the routers together. The numbers in the bubbles are network identifiers. For IP networks, the number is the network and the subnet portion of the IP addresses of all devices on it. For example, 192.0.16.0/24 is a network where IP addresses are between 192.0.16.0 and 192.0.16.254 and the subnet mask has 24 bits (it is a class C network). For more information, see [Subnet Mask](#) FAQ.

Click and hold on a router or network to see a status window with information about that item. (This only works in browse mode. Press Tab or click the lock in the upper left corner to lock it.)





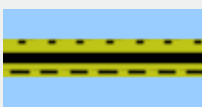

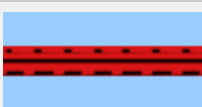

Line Styles

The style of the line corresponds to the type of interface.

	10 Mbit Ethernet
	100 Mbit Ethernet or FDDI
	Serial line - T3 Speed
	Serial line - T1 Speed
	Serial line - 56 K or other
	Frame-Relay Interface Type
	ATM Interface Type
	LocalTalk Interface Type
	Any type not specifically represented

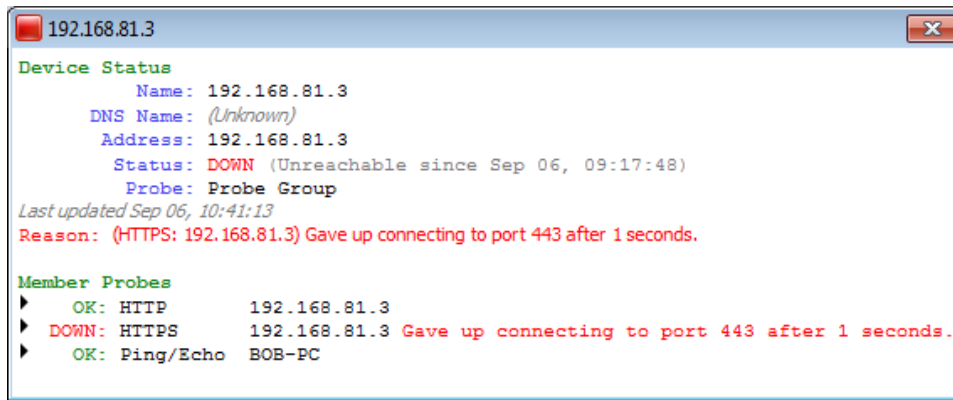
As with networks and devices, you can click and hold a link to see a Status window, containing information about the interface type and traffic statistics.

Link States

Badge	State	Meaning
	Red X	Link Down - No response has been received from the interface within the specified timeout period.
	Blue X	Basic Acknowledge - The link is down and is set to Basic Acknowledge.
	Clock, Blue link	Timed Acknowledge - The link is down, and has been set to Timed Acknowledge.
	Wrench, Blue link	Indefinite Acknowledge - The link is down, and has been set to Indefinite Acknowledge (Maintenance).
	Yellow link	Warning - The link is working, but has reached one of the specified warning thresholds.
	Orange link	Alarm - The link is working, but has reached one of the specified alarm thresholds.
	Red link	Critical - The link is working, but has reached one of the specified critical thresholds.
	Red X in circle	Admin Down - the device has responded saying that the interface's <code>ifAdmin</code> status is set to Down.

Viewing Status Windows

Intermapper shows detailed status about any item on a map (a device, a network, or a link) in a Status window.



To view device, network, or link status:

1. Make sure your map is in **Monitor** mode (click the lock at the upper left of map window to lock the map, or press **Tab** on your keyboard).
2. Click and hold a device, network, or link on the map, or right-click the device, network, or link, and select **Status Window**. The Status window for the selected device is displayed.
3. Release the mouse button to hide the Status window.

To keep a Status window open:

1. Make sure your map is in **Monitor** mode.
2. Click and hold the device, network, or link on the map.
3. Drag to a new location and release the mouse. You separated the window and it remains open, located where you released the mouse.

Customizing a Status Window

If you are using a custom TCP or SNMP probe, you can override the default contents of a Status window. For more information, see *Custom Probes* and *Customizing Status Windows* in the Developer Guide.

Device Status Window

- Click and hold the mouse on a device to open its device status window, or right-click the device and select **Status Window**.
- Click and drag to tear the window off and leave it open.

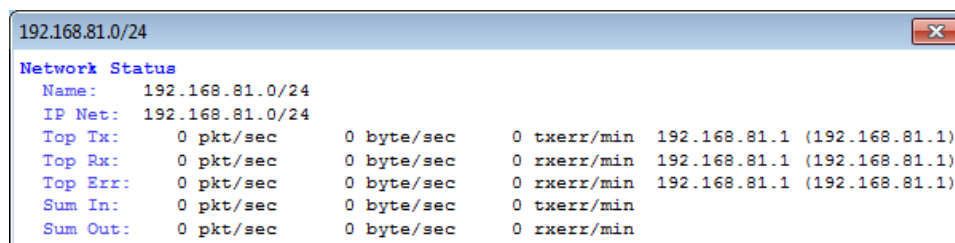
- Click the underlined **Reset** link to set **Packet Loss** to **0**. This also resets the device's availability measurement.

NOTE: The map must be in Edit mode to reset the Packet Loss value.

The window shows the device name, network address, device status, the probe used to poll it, up-time (such as SNMP sysUptime, if available), availability (the percentage of the time the device was available based on the number of packets lost while testing), round-trip time (in msec), and spanning tree status (if available).

When the device reports a problem, the reason for the most important error is shown in red at the bottom of the Status window.

Network Status Window



- Click and hold the mouse on a network oval to open its network status window, or right-click the network and select **Status Window**.
- Click and drag to separate the window and leave it open.

The network status window shows the network's IP address and subnet mask (if available) and information about the amount of traffic flowing on that network segment. This data comes from all the SNMP devices attached to that network oval.

- Top Tx** - shows which device is transmitting the most data.
- Top Rx** - shows which device is receiving the most data.
- Top Err** - shows which device is reporting the highest error rate for the link.
- Sum In/Sum Out** - shows the sum of all the transmitters and receivers connected to that network.

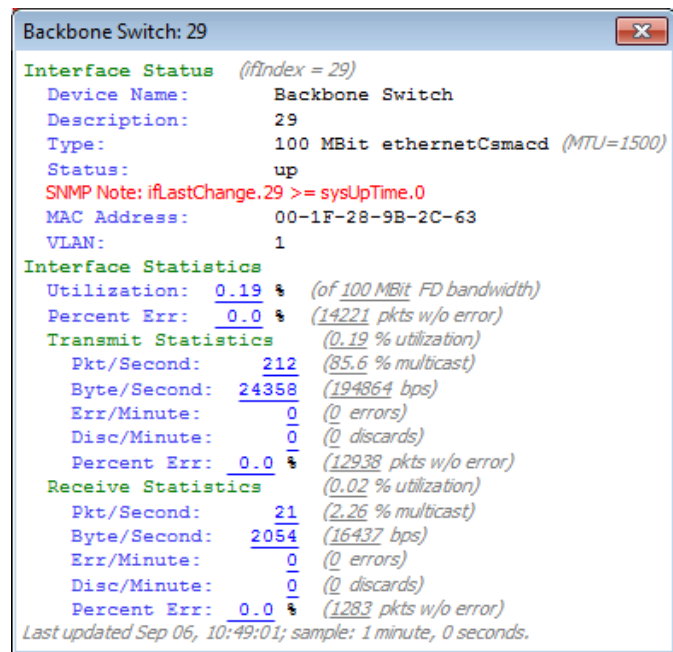
NOTE: The traffic statistics are only for devices connected to this network that speak SNMP: Ping/Echo or TCP-based devices (such as HTTP, FTP, and so on) do not have this information and are ignored when calculating the sums and maximums displayed in the Status Window.

Link Status Window

- Click and hold the mouse on a link or right-click the link and select **Status Window** to open its link status window.
- Click and drag to separate the window and leave it open.

The link status window shows the link's interface name and description, its type (10 or 100 Mbps, 1.5 Mbps T-1, and so on), its status and up-time, its IP and MAC addresses (when available), traffic statistics (transmitted from and received by the interface), and the time since the last poll.

Tip: Certain devices do not report their link speed accurately in their SNMP responses. This causes Intermapper to report a value which is not actually correct. To work around this, switch the map to Edit mode and right-click the link and select **Set Link Speed**. The Set Link Speed window is displayed, allowing you to set Transmit and Receive speeds.



Info Window

Use the Info Window, available from the Monitor menu or a device or network context menu, to view and edit information about a selected device or network.

The appearance and content of an info window varies, depending on whether the selected object is a device or network.

- For details on viewing and editing device info, see [The Device Info Window](#).
- For details on viewing and editing network info, see [The Network Info Window](#).

To open an info window:

Click the device or network and do one of the following:

- Press **Ctrl/Cmd-I** to open the info window.
- From the **Monitor** menu, select **Info Window**.

Alternatively, right-click the device or network and select **Info Window**.

After the window is open:

- Click the lock icon (lower left) to change the map to Edit mode.
- Click a info section on the left to view or edit that info type.
- Click **Apply** to save your changes.
- Click **OK** to save your changes and close the Info window.

Device Info Window

Use the Device Info window to view and edit information about a device.

The screenshot shows the 'Info for W' window with the following sections and fields:

- Left Sidebar (Info Sections):** General (selected), SNMP, Probes, Thresholds, Icon, Label, Advanced.
- General Section:**
 - Address: 192.168.81.2
 - Host Name: [Empty field]
 - Dropdown: Don't change address or name
 - Checkbox: ☐ Use as Map's Vantage Point
- Database Information:**
 - IMID: device.1.5.27
 - Kind: Unspecified
 - Retention Policy: 24 Hours
- Geographical Location:**
 - Latitude: [Empty field]
 - Longitude: [Empty field]
- Comment:** [Large text area]
- Bottom:** Lock icon (with callout 'Click to change to Edit mode'), OK, Cancel, and Apply buttons.

To use the device window:

- Click a section on the left to edit that info type.
- Edit the info as described below.
- Click **Apply** to save your changes.
- Click **OK** to save your changes and close the Info window.

General Pane

Use the Device Info window's General pane to edit general information about the device.

Editing General Info

- **Address** - the device address that is used when the device is polled.
- **Host Name** - the device's host name that is used to resolve the address.
- **Resolve** - select **address to set name**, **name to set address**, or **neither**.
- **Use as Map's Vantage Point** - select to use this network as the map's [Vantage Point](#).
- **IMID** - the Intermappers internal device ID. (This info is read-only.)
- **Kind** - the device type.
- **Retention Policy** - the Retention Policy to specify how data for this device is saved.
- **Latitude** - the device's latitude.
- **Longitude** - the device's longitude.
- **Comment** - device comments.

SNMP Pane

Use the Info window's SNMP pane to view available SNMP information. This is a read-only pane, so there are no options to edit.

Probes Pane

Use the Device Info window's Probes pane to view and edit the device's probes.

Editing Probe Info

From the Probes pane, you can add and remove probes, and edit a probe's information.

To edit a probe's information:

1. Make the map editable by clicking the lock icon at lower left.
2. To change the probe, right-click (or Ctrl-click) the probe you want to edit and select **Set Probe** from the context menu. The Set Probe window is displayed.
3. Select the probe you want to use and edit the settings as needed.
4. Click **OK** to close the Set Probe window.

To add a probe:

1. Click the plus icon (+) at the bottom of the **Probes** pane. The Set Probe window is displayed.

2. Select a probe from the probe list on the left.
3. Edit the probe settings as needed.
4. Click **OK** to close the Set Probe window.

NOTE: When you add a probe, the device becomes a probe group.

Thresholds Pane

Use the Device Info window's Thresholds pane to view and edit threshold settings for the device.

Editing Threshold Info

To edit the threshold information:

1. Open the **Info** window for the device you want to edit.
2. Make sure the map is in **Edit** mode.
3. Click **Thresholds** to view the Thresholds pane.
4. Select the **Ignore Outages** check box to suppress alerts for the device when it goes down or comes up.

NOTE: The Ignore Outages check box suppresses alerts with respect to outages, not to other state changes, thresholds, or any alerts triggers by probes attached to the device. This is useful if a device such as a laptop or mobile device goes up or down (or leaves the network completely) as part of its normal operation.

5. Clear the **Use Map Defaults** check box.
6. Edit the information as needed.
7. Click **Apply** to activate the changes without closing the window or click **OK** to activate and close the window. The selected device uses the new values.

Icon Pane

Use the Device Info window's Icon pane to change the icon for the device.

Editing Icon Info

To change the device's icon:

1. From the menu at the top of the pane, select an icon set.
2. Scroll through the set and select an icon. You can see what it looks like by clicking it. You can see what it looks like in different states by clicking the colored buttons below the preview area.
3. After you find an icon you want to use, click **Apply** to activate the icon without closing the window or click **OK** to activate the icon and close the window.

Label Pane

Use the Device Info window's Label pane to edit the device's label.

Editing a Label

A label can contain any combination of text, variables, and JavaScript. For detailed information on editing labels see [Editing Labels](#) and [Dynamic Label and Alert Text](#).

Advanced Pane

Use the Advanced pane to specify the mapping behavior of a device and whether to collect Layer 2 information.

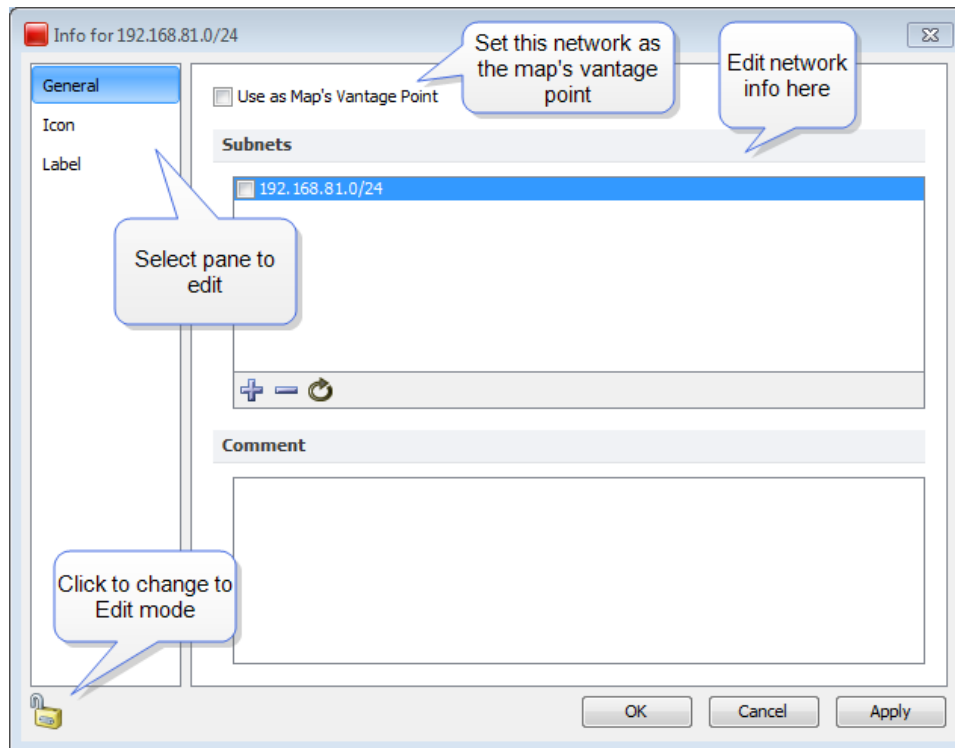
Mapping Behavior

- **Determine network information for each port separately** - use this option when mapping Routers.
- **Propagate all network number information from one port to all ports** - use this option when mapping switches.
- **Do not propagate network information about the ports** - use this option when mapping hubs and end systems.

Layer 2

- **Poll this address for Layer 2 information** - clear this check box to prevent this device's IP address from being polled for Layer 2 information. This is equivalent to the Remove switch from Layer 2 database command, available when you right-click a switch in the [Layer 2 view's Filter pane](#).
- **Allow Layer 2 connection** - clear this check box to prevent Intermapper from making a connection from this device to other devices on the map using Layer 2 information.

Network Info Window



General Pane

Use the General pane to view a list of subnets that are displayed on the map to control which subnets appear, to add and remove subnets, to set the network as the map's Vantage Point, or to add a comment.

- **Add a subnet** - click the plus sign (+) at the bottom of the **General** pane to add a subnet.
- **Remove a subnet** - select a subnet from the **Subnets** list and click the minus sign (-) at the bottom of the **General** pane to remove the subnet from the list and the map.
- **Add a Comment** - type text in the **Comment** text box to add a comment to the network.
- Click **Use as Map's Vantage Point** to use this network as the map's [Vantage Point](#).
- Click **Apply** to save the change without closing the Info window. Click **OK** to save the change and close the **Info** window.

Icon Pane

Use the Network Info window's Icon pane to change the icon that appears on the map for the selected network.

The Icon pane operates exactly as the [Device Info window's Icon pane](#).

Label Pane

Use the Network Info window's Label pane to edit the network's label.

The Label pane operates exactly as the [Device Info window's Label pane](#).

Interfaces Window

Intermapper can show the interfaces of a particular router or switch. This is convenient for viewing the specifics of those interfaces (for example, the Name or ifAlias assigned to each individual port) or for viewing the status of the port.

To view the Interfaces window:

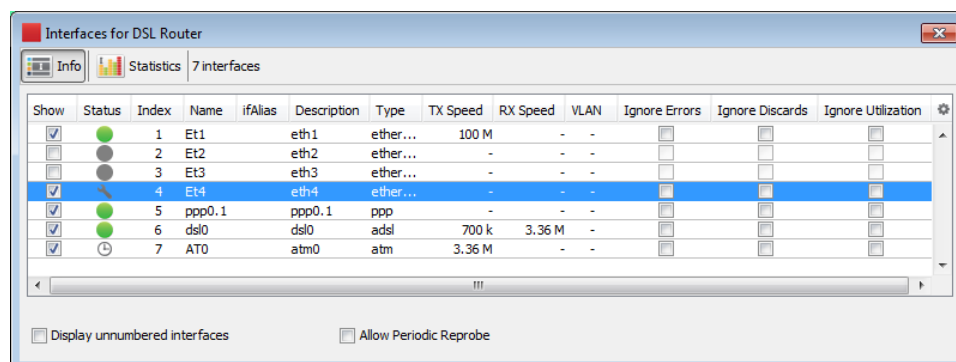
1. Right-click the router or switch for which you want to view the **Interfaces** window.
2. From the **Context** menu, select **Interfaces** window.

or

- From the **Monitor** menu, select **Interfaces** window.

NOTE: You can open as many Interfaces windows as you want. Each window is updated at the device's poll interval.

Info View



The screenshot shows a window titled "Interfaces for DSL Router" with a tabbed interface (Info, Statistics, 7 interfaces). The "Info" tab is active, displaying a table of interfaces. The table has columns: Show, Status, Index, Name, ifAlias, Description, Type, TX Speed, RX Speed, VLAN, Ignore Errors, Ignore Discards, and Ignore Utilization. The table lists 7 interfaces: Et1, Et2, Et3, Et4, ppp0.1, dsl0, and AT0. Et4 is selected, highlighted in blue. At the bottom, there are two checkboxes: "Display unnumbered interfaces" and "Allow Periodic Reprobe".

Show	Status	Index	Name	ifAlias	Description	Type	TX Speed	RX Speed	VLAN	Ignore Errors	Ignore Discards	Ignore Utilization
<input checked="" type="checkbox"/>	●	1	Et1		eth1	ether...	100 M	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	●	2	Et2		eth2	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	●	3	Et3		eth3	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	●	4	Et4		eth4	ether...	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	●	5	ppp0.1		ppp0.1	ppp	-	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	●	6	dsl0		dsl0	adsl	700 k	3.36 M	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	⏸	7	AT0		atm0	atm	3.36 M	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Interfaces window displays one row for each port or interface on the device. It shows the following information in columns:

- **Show/Hide Checkbox** - when selected, this interface is visible on the map. Clearing this check box hides the interface.
- **Status** - the status of the interface as determined by `ifAdminStatus` and `ifOperStatus`
 - If the interface has been acknowledged as indefinitely down, a wrench icon is displayed in this column.
 - If a timed acknowledgment is used, a clock icon is displayed.
- **Index** - the `ifIndex` of the interface.
- **Name** - the name assigned to the interface.
- **ifAlias** - the `ifAlias` assigned to the interface.
- **Description** - the description assigned to the interface.
- **Type** - the type of the interface, as defined in MIB-II.
- **TX Speed** - the Transmit Speed reported by the interface, in bits per second.
- **RX Speed** - the user defined value that is used when Intermapper calculates the utilization of the receive side of the interface. If the value is not set, Intermapper uses the TX Speed for the calculation. This is useful when the transmit and receive speeds are different (for example, in asymmetric DSL links). You can change both the RX Speed and TX speed using the **Set Link Speed** command, described below.
- **VLAN** - the VLAN ID assigned to the interface (if any).
- **Ignore Errors** - specifies if interface errors are ignored.
- **Ignore Discards** - specifies if interface discards are ignored.
- **Ignore Utilization** - specifies if interface errors are ignored.
- **Display unnumbered interfaces** - specifies if all the unnumbered interfaces on a switch are visible. By default, Intermapper does not display unnumbered interfaces.
- **Allow periodic reprobe** - specifies if a device is automatically reprobbed every 12 hours.

NOTE:

- The Display unnumbered interfaces and Allow periodic reprobe functions are also available in the Interfaces Behavior dialog, available from both the Monitor menu and Context menu. The setting applies a device or to all selected devices.
- These controls interact with each other. The Display unnumbered interfaces check box determines if an unnumbered interface is ignored during a periodic or manual reprobe. The Interfaces window does not change when you clear this check box until the next reprobe. This applies to a periodic reprobe described above and to a manual reprobe.

Statistics View

Status	Index	Name	Total Utilization %	Total Errors/min	Total Discards/min	Tx Utilization %	Tx Errors/min	Tx Discards/min	Rx Utilization %	Rx Err
Green	1	Et1	0.01	0	0	0.01	0	0	0.0	
Grey	2	Et2	0.0	0	0	0.0	0	0	0.0	
Grey	3	Et3	0.0	0	0	0.0	0	0	0.0	
Red	4	Et4	0.0	0	0	0.0	0	0	0.0	
Green	5	ppp0.1	0.0	0	0	0.0	0	0	0.0	
Green	6	dsl0	0.03	0	0	0.03	0	0	0.0	
Blue X	7	AT0	0.03	0	0	0.03	0	0	0.0	

Use the Statistics view of the Interfaces window to see the following statistics for all interfaces on a device:

- **Status** - the status of the interface as determined by `ifAdminStatus` and `ifOperStatus`.
 - If the interface has been acknowledged as indefinitely down, a wrench icon is displayed in this column.
 - If a timed acknowledgement is used, a clock icon is displayed.
- **Index** - the `ifIndex` of the interface.
- **Name** - the name assigned to the interface.
- **Total Utilization %, Errors/min, Discards/min** - the sum of TX and RX utilization, error, and discard statistics for a link.
- **TX and RX Utilization %, Errors/min, Discards/min** - statistics for TX and RX utilization, errors, and discards for the link.
- **Display unnumbered interfaces** - specifies that the unnumbered interfaces on a switch are displayed. By default, Intermapper does not display unnumbered interfaces.
- **Allow periodic reprobe** - specifies if a device is automatically probed every 12 hours.

Hiding and Deleting Interfaces

You can hide and delete interfaces.

To hide an interface:

Clear the check box next to the interface. If you hide an interface, any associated network to that interface is removed from the map. The interface is no longer polled, and data is no longer collected.

To delete an interface:

Click the line for the interface you want to delete and press **Delete** on your keyboard.

or

Right-click the interface line and select **Delete** from the **Context** menu.

Hiding Versus Deleting an Interface

Use the following information to help you decide whether you want to hide or delete an interface:

- **Probe rediscovery** - when you hide the interface, it is not displayed again until you unhide it. When you delete an interface, Intermapper rediscovers it and displays it again the next time it re-probes the device unless you clear the **Allow periodic reprobe** check box.
- **Data Collection** - when you hide the interface, data collection stops until you re-enable it. When you delete an interface, data collection resumes when it is rediscovered.
- **Polling** - when you hide the interface, polling for that interface stops until you re-enable it. When you delete an interface, it is polled and reappears when it is rediscovered.
- **Layer 2 Discovery** - when you hide the interface, Layer 2 discovery for that interface stops until you re-enable it. When you delete an interface, the interface is rediscovered and Layer 2 information is collected.

Acknowledging Down Interfaces

You can acknowledge one or more down interfaces from the Interfaces window.

To acknowledge down interfaces:

1. From the **Interfaces** window, select the rows for the interfaces you want to acknowledge.
2. Right-click one of the selected interfaces and select **Acknowledge**. The Acknowledge window is displayed.
3. Create an acknowledgment as described in [Acknowledging Device Problems](#).

Copying Data from the Interfaces Window

You can copy data from the Interfaces window for use in spreadsheet or other application.

To copy data from the Interfaces window:

1. Select the rows you want to copy. Shift-click to select contiguous rows, Ctrl-click to select non-contiguous rows.
2. Type **Ctrl/Cmd-C** on your keyboard. The selected rows are copied to the clipboard in tab-delimited format.

Setting the Data Retention Policy for an Interface

You can set the retention policy for an interface from the Interfaces window.

To set the retention policy for an interface:

1. Right-click the interface and select **Set Data Retention** from the **Context** menu. The Set Retention Policy window is displayed.
2. From the **Data Retention Policy** menu, select a retention policy. Data is collected as specified by the selected policy.

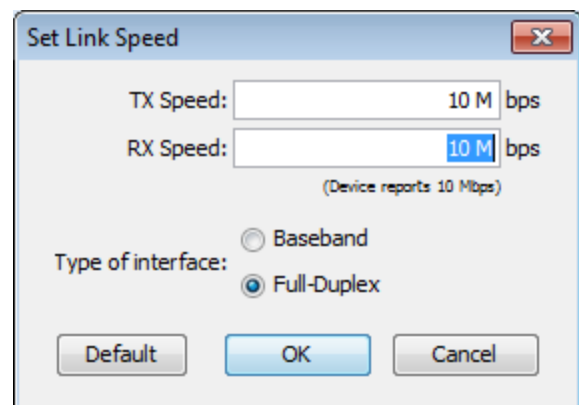
Setting the Link Speed

With the map editable, use the Set Link Speed window to set the TX Speed and RX Speed for a particular interface.

To open the Set Link Speed window:

Do one of the following:

- Right-click the link and select **Set Link Speed** from the **Context** menu.
- From the **Interfaces** window, right-click the interface whose speed you want to set and select **Set Link Speed** from the **Context** menu.



The following units are allowed:

- K (Kilo)
- M (Mega)
- G (Giga)
- T (Tera)
- (Peta)

The following values are allowed:

- 1000000
- 1000 K
- 1M

NOTE:

The RX Speed box is disabled when the interface Type is set to Baseband.

Detection Map

Use the Detection map to view devices that have recently been discovered on your network and to add those devices to a map.

NOTE: Before you can use the New Devices map, you must enable New Device Detection from the [server settings window](#).

The Detection map shows all devices that have been discovered through Scheduled Auto-Discovery or through the Flows server. The Detection map differs from the other maps in the following ways:

- It shows only devices that are not on other maps.
- All devices are non-polling by default.
- When you attach a notifier, you do not attach it directly to a device. You specify whether to trigger an alert when a new device is discovered and the source by which it is discovered (Scheduled Auto-Discovery or Flows server).

For more information, see [Using Detection Maps](#).

Using Detection Maps

Use the Detection Map to view all newly detected devices, and to move those devices onto maps.

Devices are displayed on the Detection Map from the following sources:

- **Scheduled Auto-discovery** - if scheduled Auto-discovery is enabled, any device that responds to a ping from Intermapper is displayed on the Detection Map. The Detection Map is updated only when a scheduled Auto-discovery runs.
- **Flows Server discovery** - if Flows Server discovery is enabled and the Flows server is connected to a correctly configured Flows exporter, devices that show any activity appear on the Detection Map. The Flows Server runs continuously.

Moving Devices to a Map

When a new device appears on the Detection Map, you can move it to an existing map.

To move one or more new devices to an existing map:

1. Select the devices you want to move. If you want to move only one device, you can skip this step.
2. From the **Move to** submenu, right-click the device and select the map you want to move them to. The selected devices are moved to the specified map.

NOTE: The devices on the Detection Map use the Non-polling probe. After you move a device, select the probes appropriate to the device.

Getting an Alert When a New Device is Added

Any notifier can be attached to the Detection map. Most notifiers are attached to devices, networks, or interfaces, and are triggered based changes in their states. For devices on a Detection map, you can specify whether to trigger a notifier based on the source of the detection:

- **The Flows Server** - the notifier is triggered when the Flows Server reports a new device.
- **Scheduled Auto-Discovery** - the notifier is triggered when a device is discovered through Scheduled Auto-Discovery.

Deleting Devices from the Detection Map

In some cases you may never want to monitor a particular device.

To delete devices from the Detection map:

1. Click the pencil icon to make the map editable.
2. Select the devices you want to delete.
3. Press **Delete** on your keyboard. The selected devices are removed from Detection map.

NOTE: The devices might reappear at some point, depending on how you configured New Device Detection:

- **Scheduled Auto-discovery** - if you delete a device that was detected through scheduled Auto-discovery, the device reappears when a new Auto-discovery cycle runs if the device is discovered during that cycle.
- **Flows Server discovery** - if you delete a device that was detected through the Flows Server, the device reappears only when the Flows Server is restarted and activity is detected from the device.

About Packet Loss

Intermapper can monitor both long-term and short-term packet loss. These are useful for detecting problems in your network.

Long term Packet Loss is measured from when Intermapper starts testing a device. Intermapper computes this from the total number of pings or SNMP queries sent, and the fraction of those that fail to respond.

Long-Term Packet Loss

The Long-term Packet Loss is displayed in the device's Status window, along with the total number of packets sent and responses received. It is possible to reset this value using the **Reset** link in the device's Status window.

Short-Term Packet Loss

Intermapper measures Short-term Packet Loss by counting the number of lost packets in the last 100 sent. To do this, each device retains the history of the last 100 packets sent/received.

Short-term packet loss is displayed in the device's Status window as a percentage of the number of dropped packets in the last 100. You can reset this value using the **Reset** link in the Status window (which resets all the device's statistics) or by selecting one or more devices and selecting **Monitor > Reset Short-term Packet Loss**.

Packet Loss Notifiers

Intermapper can send alerts and notifications when the short-term packet loss statistics exceed certain thresholds. That is, when short-term packet loss exceeds a warning, alarm, or critical threshold, the device turns the appropriate color and Intermapper sends the appropriate alert. These thresholds can be set in the following places:

- **Server Settings** - Device Thresholds apply to all devices on all maps.
- **Map Settings** - Device Thresholds apply to all devices on a particular map, overriding the Server Settings value.
- **Individual device - Set Thresholds** sets the thresholds for that particular device, overriding the map-wide or server-wide settings.

To disable alerts and notifications for high packet loss, set the packet loss thresholds to 100%.

Ignoring Lost Packets During Outages

When a device goes down, Intermapper stops updating the packet loss history (both short and long term) for the duration of the outage. This prevents packet loss statistics from continuing to increase during an outage. (If Intermapper continued to count lost packets while a device was down, the statistics incorrectly indicate there was high packet loss when the problem was most likely something else.)

In addition, Intermapper ignores the packets lost when determining that a device is down. For example, the default is that three successive lost packets indicate that the device is down (no longer responding). However, these three dropped packets are incorrectly shown as a 3% packet loss. Consequently, Intermapper removes the dropped packets from the history, so that it shows an accurate accounting.

When the device subsequently responds (after the problem has been corrected), Intermapper begins counting successful and lost packet responses again.

Acknowledging Device and Link Problems

Use the Acknowledge command, available from the Monitor Menu, to acknowledge failures or problems in the network. When you acknowledge a problem, Intermapper does the following:

- Changes the device icon or link color to blue to show that the problem has been acknowledged.
- Stops further notifications of the problem, either for the duration of this outage or for a specified time period.
- Logs your comments in the Event Log file, along with the name and IP address of the user who acknowledged the problem.
- Displays the comment in the device or link's Status window.

Why Are Acknowledgments Useful?

Acknowledgments allow the network administrator to see the state of the network, as well as the responses that have been made to the current set of problems.

Use Acknowledgements to do the following:

- **Indicate that someone has taken responsibility for a problem** - because acknowledging a problem turns the affected device's icon blue, it is easy to see that someone is aware of (and is presumably working on) the problem.
- **Emphasize new problems** - the normal color of icons on a map should be green (operating correctly) or blue (having trouble, but being worked on), When a new problem occurs, the affected devices are red, orange, or yellow, depending on the

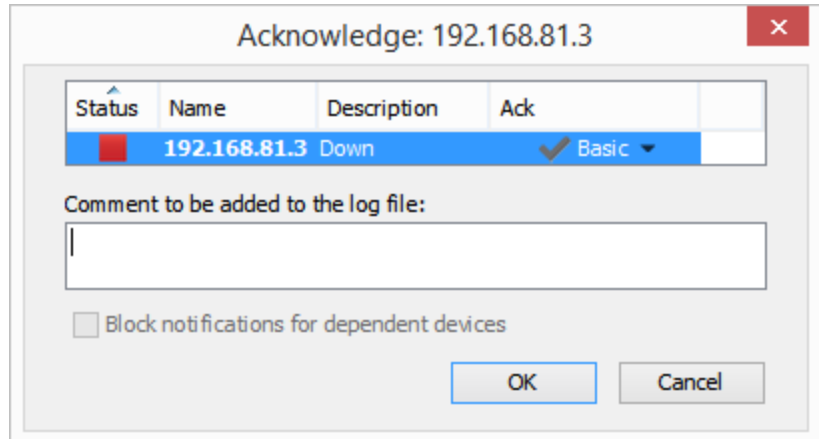
device status. This makes it easy to see where new troubles are. After acknowledgment, these devices are turned to blue.

- **Suppress notification for a problem device** - when a device has been acknowledged, no further notifications are sent.
- **Provide information about the problem and its management** - enter a comment to convey information about the failure, and/or the corrective action.

Acknowledging a problem

To acknowledge a problem with a device:

1. For devices, click or Right-click or Ctrl-click (Mac) the device(s) you want to acknowledge.
For interfaces, Right-click or Ctrl-click (Mac) the link.
2. From the Monitor menu or Context menu, select **Acknowledge**. The Acknowledge window is displayed.
3. To keep the device or link in Acknowledgment mode for a specific period of time, or for an indefinite period, select **Indefinite** or **Timed** in the **Ack** column.
4. To suppress notifications for devices that depend on this device, select the **Block notifications for dependent devices** check box.
5. Enter a comment and click **Acknowledge**. The selected device's icon changes to blue and your comment is written to the Event Log file. Notifications are canceled for the selected device for the duration of this outage.



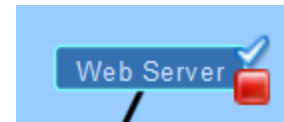
Basic, Timed, and Indefinite Acknowledgments

Intermapper offers the following device acknowledgments:

Basic

The device or link is acknowledged and notifications are suppressed until it gets better or worse. The device icon or link turns blue to indicate that someone has taken responsibility for it, and that no further notifications are sent.

As soon as the device or link state changes to another status, its acknowledge status is automatically cleared and notifications resume. After that, notifications are sent for any subsequent failures.



Down, with Basic Acknowledgment



Link, with Basic Acknowledgment

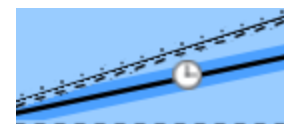
Timed

The device or link is acknowledged and notifications suppressed for the specified period of time. In this case, the device state is OK.

The icon or link turns blue if it is not okay and the clock badge is displayed to show that notifications are blocked for the specified time.



Up, with Timed Acknowledgment



Link, with Timed Acknowledgment

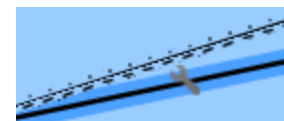
Indefinite

The device or link remains acknowledged until the operator unacknowledges it.

As with the **Timed** acknowledgment, the icon turns blue and the wrench badge is displayed to remind the operator that notifications are suppressed. In this case, the device is DOWN.



Down, with Indefinite Acknowledgment



Link, with Indefinite Acknowledgment

NOTE:

- When you acknowledge an interface outage, the interface's link turns blue, rather than the device itself, and an X, wrench, or clock is displayed on the link, depending on whether it is a Basic, Indefinite, or Timed Acknowledgment.
- With timed and indefinite acknowledgment, you can acknowledge a device even when it is up and okay (i.e., green). This is useful if you know that there may be future outages (for example, planned maintenance) with the device, and you want to avoid extraneous notifications. You cannot do this with Basic Acknowledge.
- The presence of the wrench badge is a safety measure. When you scan the map visually, the wrench indicates devices whose notifications are currently being blocked.

Acknowledgments and Dependencies

When you acknowledge a device, use the Block notifications for dependent devices check box to specify whether the acknowledged device should be considered in finding dependencies. Selecting this check box suppresses notifications for any device on the other side of the device being acknowledged.

To suppress notifications for all devices that are dependent on the selected device:

Select the **Block notifications for dependent devices** check box. Notifications are suppressed for any device that depends on the selected device.

For more information on dependencies and dependent devices, see [Using Notification Dependencies \(Pg. 114\)](#).

Unacknowledging a Device or Link

Use the Unacknowledge command to restore the device to its current notification state.

To remove a device acknowledgment:

1. Select a single or multiple devices.
2. From the **Monitor** menu, select **Un-Acknowledge**. The selected devices are returned to their current notification states and their notifications are no longer suppressed.

To remove a link acknowledgment:

1. Right-click or Ctrl-click (Mac) the link. The Context menu is displayed.
2. From the **Context** menu, select **Un-Acknowledge**. The selected link is returned to its current notification state, and notifications for the link are no longer suppressed.

Outage Alarms on Interfaces

Intermapper treats an outage on each device interface as a separate alert event. By default, each time an interface goes down, the affected interface gets a red X and alarm notifications for that interface are triggered.

Choosing Alarm Behavior for Interfaces

Select the **Set devices to Alarm status on down link** check box, available from the [Device Thresholds pane](#) of the Server Settings window to control the behavior of alarms when an interface goes down.

You can do the following:

- Trigger alarms for individual interfaces.
- Trigger an alarm for the device when any interface goes down.

Acknowledging Interface Outages

You can right-click an affected interface's link and select Acknowledge. The interface link gets a blue X and no other notifications for that interface are sent. Intermapper also writes a line in the Event Log file for these events. The format of the Event Log entries is as follows:

```
09/30 14:03:32 link DOWN : [1] switch.example.com - 1
...
09/30 14:03:49 link ACK : [1] switch.example.com - 1
```

If another interface subsequently goes down, the same process repeats as follows:

- The link gets a red X.
- An entry is written to the Event Log file.
- Notifications are sent.
- You can acknowledge the new interface.

If two interfaces go down at the same time, a set of alarm notifications is sent for each interface. No further notifications are sent.

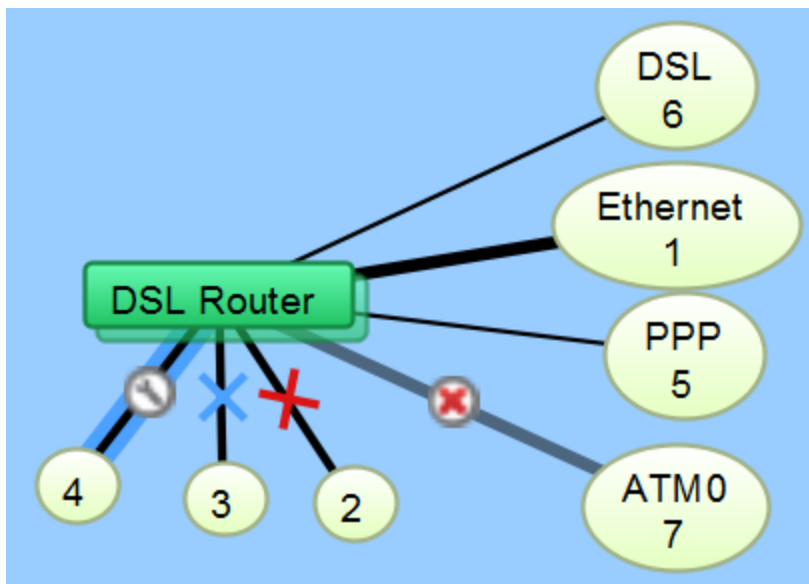
After it is acknowledged, the link's Status window show the interface's status as **ACK (down)**.

You can acknowledge and unacknowledge multiple interfaces from the device's Interfaces window.

To acknowledge multiple interfaces:

1. Select the device.
2. From the **Monitor** menu, or from the **Context** menu using Right-click or Ctrl-click (Mac), select **Window** from the **Interfaces** submenu. The interfaces window is displayed.
3. Select one of the interfaces you want to acknowledge.
4. Shift-click or Ctrl-click to select more interfaces to acknowledge.
5. Right-click or Ctrl-click (Mac) and select **Acknowledge** from the **Context** menu.

You can Un-acknowledge one or more links using Right-click or Ctrl-click (Mac) in the same way you acknowledge. This replaces the blue X with a red one, and re-enables any repeated notifications for that device.



NOTE: The red X in a circle in the image above shows a link where the status is supplied by the router is `ifAdminDown`. To see all available states for devices and links, see [Understanding the Map](#).

Approaches for Down Interfaces

- **Acknowledge the interface** as described above. This is good for outages on operational interfaces that are expected to return to service in the near future.
- **Hide the interface** - If you know that an interface will be down for a long time, you can hide it. This tells Intermapper not to monitor its status and removes it from the map to minimize clutter. To show or hide an interface, open the device's Interfaces window and select or clear the check box in the left column.

Setting Thresholds

You can set thresholds in Intermapper as follows:

- **Devices** - sets thresholds for lost packets, interface errors, and short-term packet loss.
- **Interfaces** - sets thresholds for interface errors, link utilization, and interface discards.

You can set thresholds as follows:

- **Individual thresholds** for devices and interfaces
- **Server Defaults** for device and interface thresholds
- **Map Defaults** for device and interface thresholds

Device Thresholds

For devices, you can set thresholds for the following:

- **Number of lost packets** - specify a number of lost packets between 1 and 10 required to set a device to a down state.
- **Interface errors** - specify the number of interface errors-per-minute required to set a device to warning, alarm, or critical state.
- **Short-term packet loss** - specify a number of packets out of the last 100 required to set a device to warning, alarm, or critical state. This metric applies only to packet-based probes. This statistic can be viewed from the device's Status window.
- **Response Time** - specify a response time in milliseconds required to set a device to warning, alarm, or critical state. This statistic can be viewed from the device's Status window.

Interface Thresholds

For interfaces, you can set Warning, Alarm, and Critical thresholds for the following:

- **Errors** - **Rx Errors (Received)** per minute, **Tx Errors (Transmitted)** per minute, and **Total Errors (Rx + Tx)** per minute.
- **Link Utilization** - **Rx Utilization (Received)** percentage, **Tx Utilization (Transmitted)** percentage, and **Total Utilization (Rx + Tx)** percentage.

- **Discards - Rx Discards (Received)** per minute, **Tx Discards (Transmitted)** per minute, and **Total Discards (Rx + Tx)** per minute.

As stated above, these statistics can be seen in the device's Status window.

Setting Thresholds for Individual Devices

Use the Monitor menu or the device's Context menu to set thresholds for a device.

To set thresholds for a device:

1. Right-click or Ctrl-click (Mac) the device and choose **Info Window** or click to select the device, then choose **Info Window** from the **Monitor** menu. The device's Info window is displayed .
2. From the left pane, click **Thresholds**. The Thresholds panel is displayed in the right pane.
3. Clear the **Use Map Defaults** check box.
4. Set the thresholds as needed and click **OK**. New thresholds are used to determine the device's status starting with the next poll.

Setting Thresholds for Individual links

To set thresholds for individual links:

Do one of the following:

- Set thresholds for each link separately, using the interface link's Context menu.
- Set thresholds for all of the device's links at once, using the device's Context menu.
- Set thresholds for some, but not all, of the device's links using the Interfaces window. In this case, use the Interfaces window to select the interfaces whose links you want to set, then use the Context menu to set them all at once.

Setting Thresholds for a Link

To set thresholds for a link:

1. Right-click or Ctrl-click (Mac) the link and select **Interfaces > threshold set** from the **Context** menu. The link's selected Threshold window is displayed.
2. Set the thresholds as needed and click **OK**. New thresholds are used to determine the link's status starting with the next poll.

Setting Thresholds for All of a Device's Links

To set thresholds for all of a device's links:

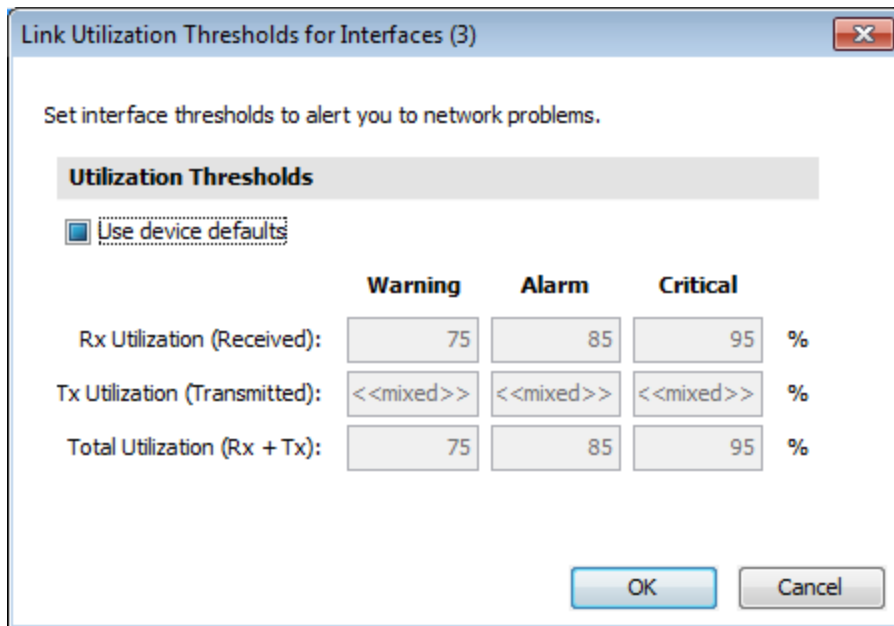
1. Right-click or Ctrl-click (Mac) the device and select **Interfaces > threshold set** from the **Context** menu
or
Click to select the device, and choose **Interfaces > threshold set** from the **Monitor** menu. The selected device's Interface Threshold window is displayed.
2. Set the thresholds as needed and click **OK**. New thresholds are used to determine the status of all the device's links starting with the next poll.

Setting Thresholds for Some of a Device's Links**To set thresholds for some of a device's links:**

1. Right-click or Ctrl-click (Mac) the device and choose **Interfaces > Window** from the **Context** menu. The selected device's Interfaces window is displayed.
2. Select the first interface you want to set. The interface line is selected.
3. Shift-click (for contiguous lines) or Ctrl-click (for non-contiguous lines) to select additional interfaces you want to set.
4. Right-click or Ctrl-click (Mac) the selected interfaces and select **Interfaces > threshold set** from the **Context** menu. The Thresholds window is displayed, showing values that are common among the links. Any values that are not the same show `<mixed>`.
5. Set the thresholds as needed and click **OK**. New thresholds are used to determine the status of the selected links starting with the next poll.

Viewing and Resolving Conflicts in Threshold Settings

You can set thresholds for several links at once. If you have already set thresholds for one of the links, select multiple links and open the Thresholds window, the conflicting are shown as `<<mixed>>`. For example,



The image above shows that the Tx Utilization threshold for one or more of the selected interfaces is different than the others. You can resolve the issue by making the settings the same for the selected interfaces. Hover your mouse over the conflicting value to see the value of the parent device's threshold setting.

Sending Alerts Based On Link Status

Use the same techniques as above to attach notifiers to links, sending alerts based on the status of one, some, or all links on a device.

Attaching a Notifier to a Link

To attach a notifier to a link:

1. Right-click or Ctrl-click (Mac) the link and select **Interfaces > Notifiers** window from the **Context** menu. The link's Notifiers window is displayed, showing a list of notifiers, with check boxes for each link's status levels. If any notifiers are attached to the link, check boxes are selected.
2. Select status level check boxes to indicate which notifiers should be run. When finished, close the window. Alerts are sent as specified when link thresholds reach the status associated with a notifier's check box.

Attaching a Notifier to Some or All Links on a Device

To attach a notifier to some or all links on a device:

1. Right-click or Ctrl-click (Mac) the device and select **Interface > Window** from the device's **Context** menu. The device's Interfaces window is displayed.
2. Select the interfaces for the links you want to attach notifiers to. Press Ctrl-A (or Cmd-A) on your keyboard to select all. Click a line and press Shift-click or Ctrl-click as described above to select additional interfaces. Then Right-click or Ctrl-click (Mac) and select **Notifiers Window** from the **Context** menu.
3. If notifiers are attached to any of the device links, status check boxes are selected for certain status levels.
4. Select status level check boxes to indicate which notifiers should run. When finished, close the window. Alerts are sent as specified when thresholds reach the status associated with a selected notifier's.

Setting Default Thresholds

You can set default thresholds for a server or a map. You can override the default settings and use default thresholds for a map instead. You can also override those thresholds for an individual device or interface.

You can set default device and traffic thresholds for a map using the Map Settings window, available from the Edit menu.

Setting Default Device Thresholds

You can use the Device Thresholds section of the Map Settings window to set default device thresholds for a map so that errors for all devices are reported at the same levels.

Set thresholds to alert you to network problems.

☒ Use Server defaults

Down Thresholds

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Interface errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/>	per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

To set the default device thresholds:

1. From an editable map, select **Map Settings** from the **Edit** menu. The Map Settings window is displayed.

2. From the left pane, click **Device**. The default thresholds for the map are displayed in the right pane.
3. Enter the settings you want to change and click **OK**. The map uses the new threshold settings.

Setting Default Interface Thresholds

For devices that have multiple interfaces, such as switches and routers, you can set thresholds for individual interfaces.

You can use the Traffic section of the Map Settings window to set traffic thresholds for a map. You cannot set traffic thresholds for a specific device.

You can set default interface thresholds for the server or for an individual map by doing the following:

- To set defaults for the server, select **Interface Thresholds** from the **Server Settings** window.
- To set defaults for the map, select **Interface Thresholds** from the **Map Settings** window.

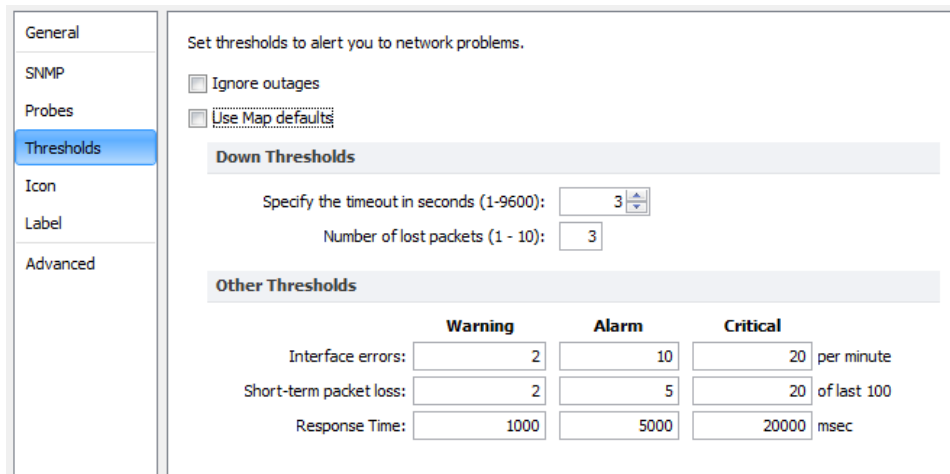
You can set any of the following thresholds:

- **Error thresholds** - sets thresholds for Rx Errors (Received), Tx Errors (Transmitted), and Total Errors (Rx + Tx).
- **Utilization thresholds** - sets thresholds for Rx Utilization (Received), Tx Utilization (Transmitted), and Total Utilization (Rx + Tx).
- **Discard thresholds** - sets thresholds for Rx Discards (Received), Tx Discards (Transmitted), and Total Discards (Rx + Tx).

Setting Thresholds for a Specific Device

From the Info window, you can set device thresholds for a specific device, with different values than the default map settings. You cannot set traffic thresholds for a specific network or link.

NOTE: When setting thresholds for a probe group, you can set the thresholds only for an individual probe or use the map default settings. For more information, see [Setting Thresholds for Probe Groups](#) **Setting Thresholds for Probe Groups on page 187**.



Set thresholds to alert you to network problems.

☐ Ignore outages

☐ Use Map defaults

Down Thresholds

Specify the timeout in seconds (1-9600):

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Interface errors:	<input type="text" value="2"/>	<input type="text" value="10"/>	<input type="text" value="20"/>	per minute
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

NOTE: Only SNMP probes have thresholds for all three parameters (response time, packet loss and interface errors); a ping/UDP-based probe monitors only response time and packet loss, and a TCP probe monitors only response time.

To set the device thresholds for a specific device:

1. With the map in **Edit** mode, right-click a device and select **Info** window. You can also access the **Info** window from the **Monitor** menu. The Info window is displayed.
2. From the left pane of the Info window, click **Thresholds**. The Thresholds pane is displayed.
3. Clear the **Use Map Defaults** check box.
4. If you want to suppress alerts for the device when it goes down, select the **Ignore Outages** check box.

NOTE: The Ignore Outages check box suppresses alerts only with respect to outages, not to other state changes, thresholds, or to any alerts triggers by probes attached to the device. This is useful if a device such as a laptop or mobile device goes up or down (or leaves the network completely) as part of its normal operation.

5. Enter new values and click **OK** or **Apply**. The selected device uses the new values.

Setting Thresholds for Probe Groups

When setting thresholds for a probe group, you can set the thresholds only for an individual probe or use the map default settings.

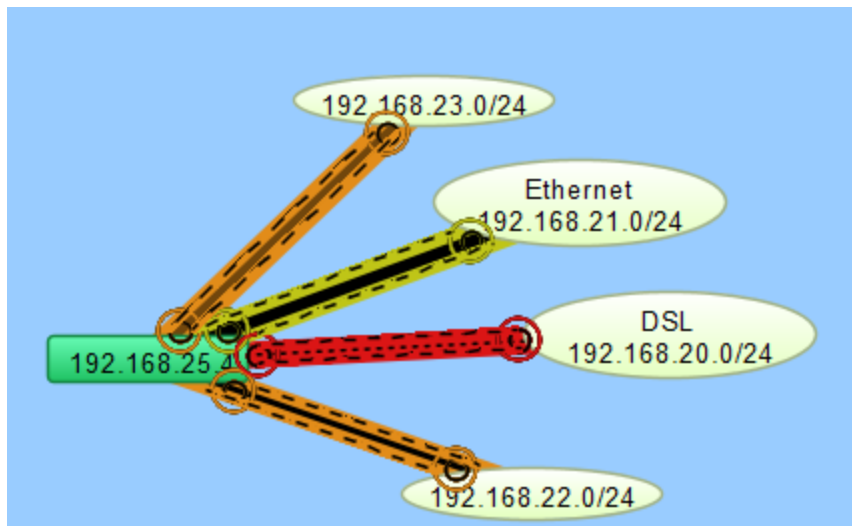
To set thresholds for a probe group:

1. Double-click a probe group. The Info window for the probe group is displayed.
2. From the left pane of the **Info** window, click **Probes**. A list of probes in the probe group is displayed.
3. Right-click or Ctrl-click (Mac) the probe for which you want to set thresholds and select **Info Window**. The Info window for the selected probe is displayed.
4. From the left pane, click **Thresholds**. The threshold settings for the selected probe are displayed.
5. Clear the **Use Map Defaults** check box and set the thresholds as needed.
6. Click **OK**. The thresholds for the selected probe are set.
7. Continue setting thresholds for each probe as needed and click **OK** from the probe group's **Info** window.

Setting Traffic Indicators

You can use traffic indicators to help you view network activity on a map. You can set the traffic levels at which moving ants are displayed to show you the level and direction of activity of a particular link.

You can use the Traffic section of the [Map Settings window](#) to turn on and configure traffic indicators for a map. You cannot set traffic indicators for a specific device or link.



NOTE: Traffic indicators are part of Intermapper's Animation feature set. By default, animations are not enabled as they require additional CPU resources. You can turn enable them from the Animation Settings pane of the [Preferences window](#).

Sending Feedback

Use the Send Feedback and Send a Screenshot commands, available from the Help menu, to send comments or report bugs. You can also use the Send Feedback window to [submit updates for an existing ticket](#).

NOTE: If the window is automatically displayed, you encountered a client-side bug. (A bug on the server is not visible from the client.) If you selected the Automatically E-mail Intermapper bug reports check box in the Server Preferences > E-mail panel, the server sends bug reports to Intermapper support when an error is encountered by the Intermapper server.

To send feedback:

1. From the **Help** menu, select **Send Feedback**. The Send Feedback window is displayed.
2. Enter or edit contact information as needed and enter a **Subject** for the feedback. This should be a short description of the comment or bug. If you are updating an existing support ticket, you can enter the ticket number and the content of your feedback submission is added to that ticket. For more information, see [To Update an Existing Support Ticket](#).
3. If you are reporting a bug, enter the steps required to reproduce the bug or condition into the **Steps to Reproduce** text box. If you are making a comment or suggestion, enter it in the box.
4. If you want to include a screenshot, select the **Include screenshot** check box.
5. To include additional information, click the **System**, **Files**, or **Logs** tab. See additional information below.
6. Click **Submit**.

Send Feedback

Thank you for sending this information. Please tell us what you wanted to happen, what actually happened, what steps we could take to reproduce it, and any other information you think might be relevant. You will receive an acknowledgement from our tracking system.

After submitting this information, you will be given a chance to quit the program or continue using the application.

Contact Information

Name: Tom Terrific Phone: 603-555-1212

Email: tom.terrific@example.com

Ticket: 113225 Subject:

☐ Include screenshot

Summary System Files Logs

Steps to Reproduce

Here's an update - I was able to reproduce the problem reliably with the following steps:

1. Open a map.
2. (etc.)

Submit Cancel

To send feedback with a screenshot:

From the **Help** menu, select **Send a Screenshot**. The Send Feedback window is displayed with a note that a screenshot is included. Enter information as appropriate as described above.

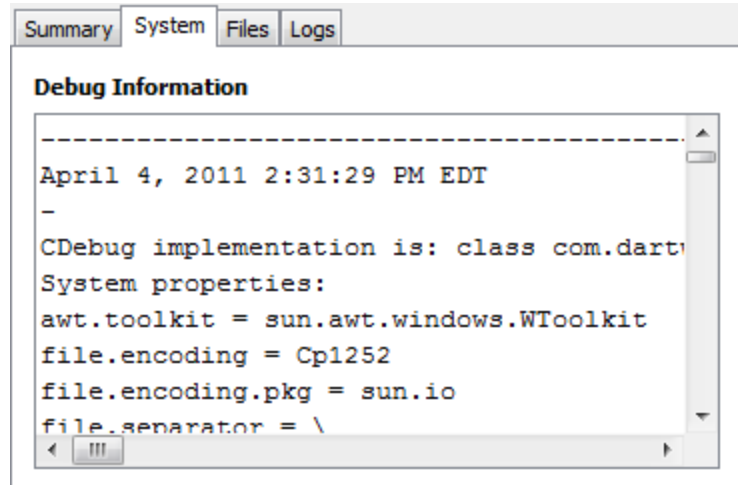
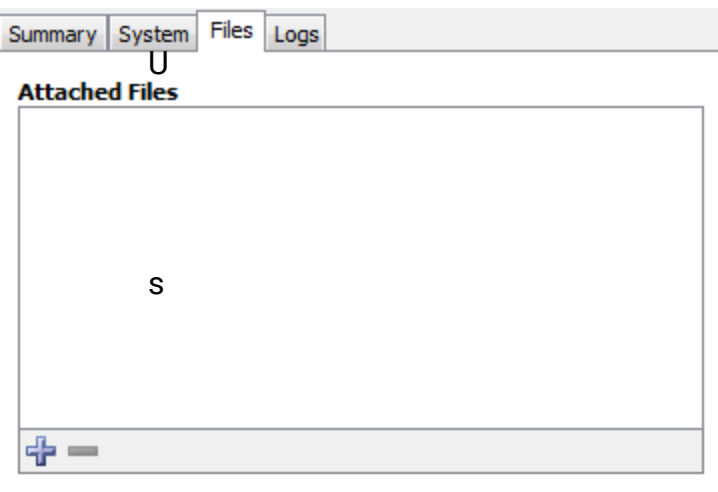
To update an existing support ticket:

1. From the **Help** menu, select **Send Feedback**. The Send Feedback window is displayed.
2. In the **Ticket** text box, type the ticket number.
3. In the **Summary** tab, attach additional files on the **Files** tab or send additional logs from the **Logs** tab.

System Tab

Use the System tab to view and edit the Debug information to send with the report.

Files Tab



Click the **Files** tab to include files with the report.

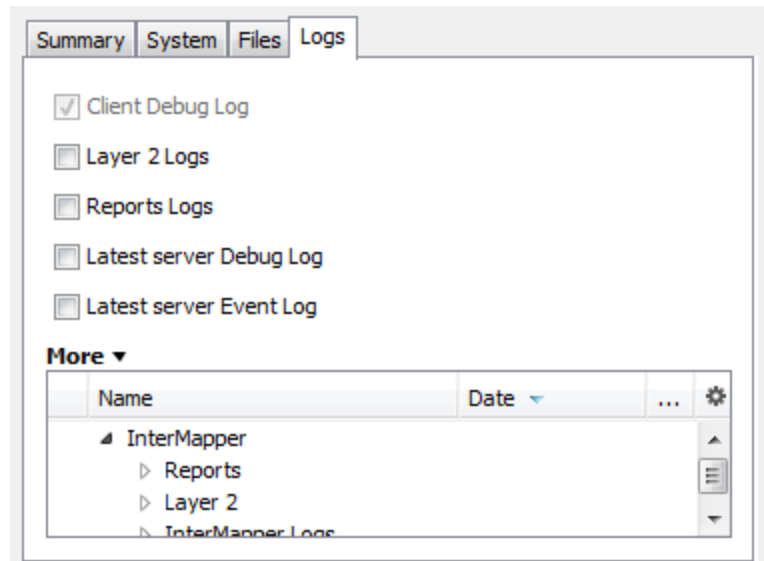
- Click **Add file** (plus icon) to add a file to send. The path to the file is displayed in the Attached Files list.

- To remove a file from the list, select a file line from the **Attached Files** list and click **Remove selected file** (minus icon).

Logs Tab

You can use the Logs tab to select which log files are included with the report.

- Select or clear the check boxes to select the log files you want to send.
- Expand the More list to view additional log files that you can send.

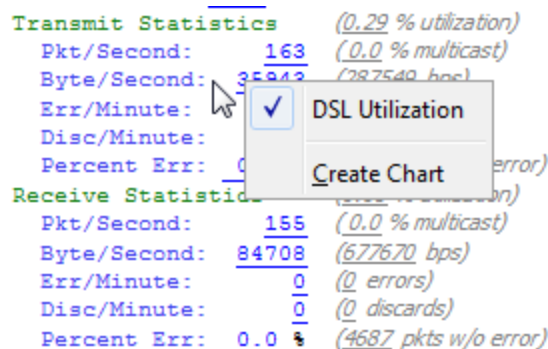


Creating Charts

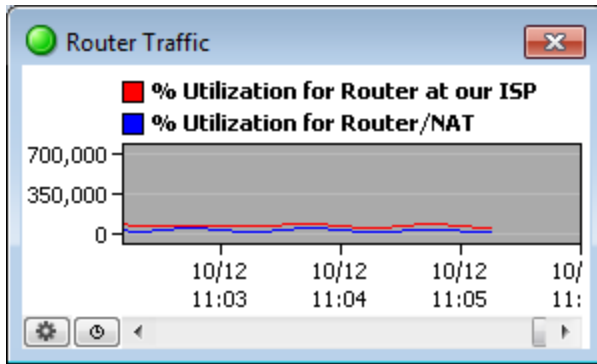
Intermapper charts display the history of one or more variables. This information can also be saved to a log file for further analysis.

To create a chart:

- Open one of the status windows as described in [Viewing Status Windows \(Pg. 159\)](#).
- Drag the status window to create a new window.
- Click any of the underlined values. If the underlined value is displayed on existing charts, a list of charts is displayed, along with a Create Chart option.



- Click **Create Chart**. A new chart is displayed.
- To add more variables to the chart, drag underlined values to the chart. For example,



For more information on charts, see [Using Charts. \(Pg. 192\)](#)

Using Charts

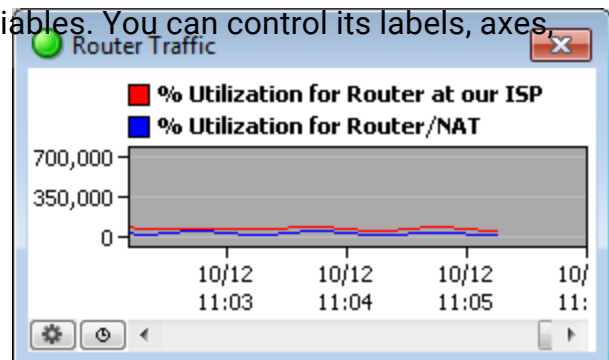
InterMapper displays historical information in a chart. Charts can hold an unlimited number of datasets for an unlimited time period. This data can also be written to a tab-delimited text file.

A chart is a persistent window that belongs to a particular map. All data that is displayed in a chart must come from devices or links of that map.

The figure on the right shows a chart with two variables. You can control its labels, axes, options, and time intervals, as described in the pages of this section.

You use the options available from the [Charts Menu \(Pg. 194\)](#) to view and hide charts.

You use the options available from the [Chart Options \(Pg. 195\)](#) menu to view and edit the parameters which control content and appearance of each chart.





You can also specify the file that logs the chart's data, and control options for creating new chart log files. For more information, see [Chart Log Files \(Pg. 201\)](#).

Viewing and Hiding Charts

You view and hide charts using the Charts command in the View menu or by selecting options from the [Charts menu at the bottom left of the chart's window. \(Pg. 194\)](#).

To show an existing chart:

Do one of the following:

- From the **Windows** menu, select the chart from the **Charts** submenu.
- Click  in the tool bar to view a list of charts associated with the map. Double-click a chart to view it.
- Right/Ctrl-click  in the tool bar to view a menu of charts associated with the map without changing to the Chart List view. From the menu, select a list.
- From the **Chart List** view, right-click or Ctrl-click a chart and select **Show Chart**.

To hide a chart:

Click the close box. The chart is hidden, but the chart's data is preserved and continues to be collected.

To scroll the chart:

Drag the chart background to scroll the chart right or left.

Creating and Adding Datasets to Charts

To create a chart:

1. Open one of the **Status** windows as described in [Viewing Status Windows \(Pg. 159\)](#).
2. Drag the **Status** window to create a new window.
3. Click any of the underlined values. If the underlined value appears on existing charts, a list of charts is displayed, along with a Create Chart option.
4. Click **Create Chart**. A new chart is displayed.

To add a dataset to an existing chart:

1. Open a **Status** window.
2. Drag an underlined value (blue or grey) from a status window into the chart. The variable is added to the chart.

NOTE: To see what device a dataset belongs to, right-click (or Ctrl-click) the dataset's legend in the Chart window and select Show Device. If you are viewing the Map window in Map view, the device is highlighted momentarily. In List view, the device is selected in the list.

Editing Charts

Edit the parameters that control a chart's content and appearance from the [Chart Options window \(Pg. 195\)](#), available from the [Chart menu \(Pg. 194\)](#).

Deleting Charts

Use the Delete Chart command, available from the [Chart menu \(Pg. 194\)](#) to delete a chart.

Chart Menus

Intermapper provides three menus you can use to view and edit charts.

Charts Menu

You can use the Charts menu to view and hide charts.

To show all charts:

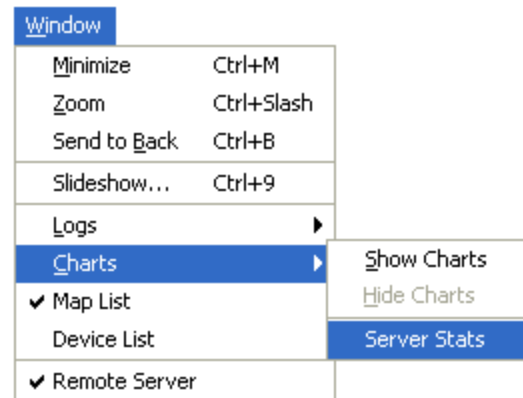
From the **Charts** submenu of the **Windows** menu, select **Show Charts**. All defined charts for the current map are displayed.

To hide all charts:

From the **Charts** submenu of the **Windows** menu, select **Hide Charts**. All defined charts for the current map are removed.

To view an individual chart:

From the **Charts** submenu of the **Windows** menu, select a chart. When the chart is visible, a checkmark is displayed in the submenu next to the chart name, as shown at the right.



NOTE: From the Charts list window, select one or more charts, then right/Ctrl-click a selected chart line and choose Show Chart.

Chart Menu

To view the Chart menu:



Do one of the following:

- Click the icon in the lower left to access the **Chart** menu.

- Right/Ctrl-click in the chart's data area.

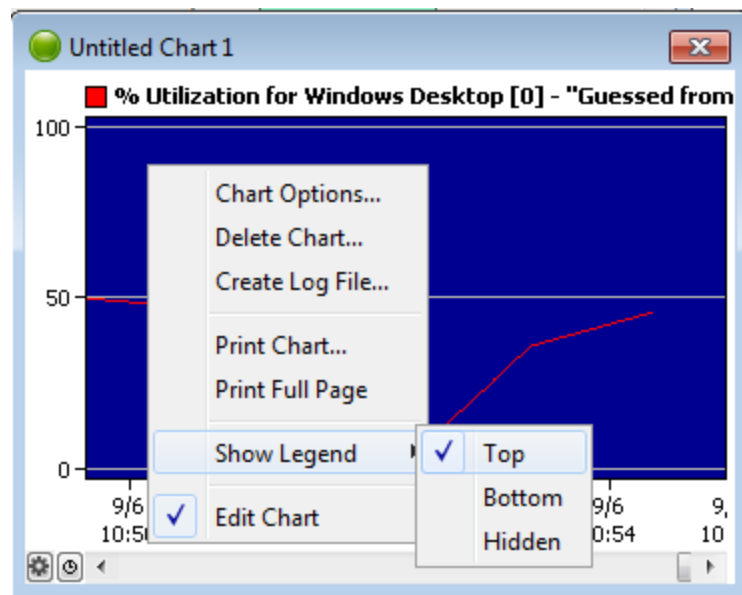
The Chart dropdown menu is displayed.

Delete Chart - deletes the current chart and its data.

Log File - creates a log file to receive the data for the current chart.

Show Legend - places the chart's legend at the top, bottom, or hides the legend completely.

Edit Chart - If the map is not in edit mode, this is the only available option. Select this option to edit the chart and view the Chart menu.



The Chart dropdown menu.

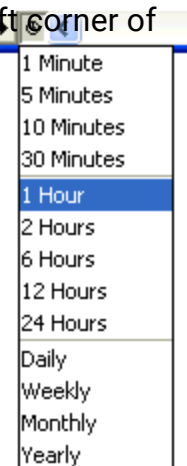
Time Interval Menu

Use the Time Interval menu, located next to the Chart menu icon in the lower left corner of the Chart window, to set the time between the tick marks on the chart's horizontal axis.

Chart Options

You can use the Chart Options window to view and edit the parameters that define a chart's appearance and content.

The Chart Options window is available from the [Chart menu \(Pg. 194\)](#), or by right-clicking within the chart window.



Applying Changes in the Chart Options Window

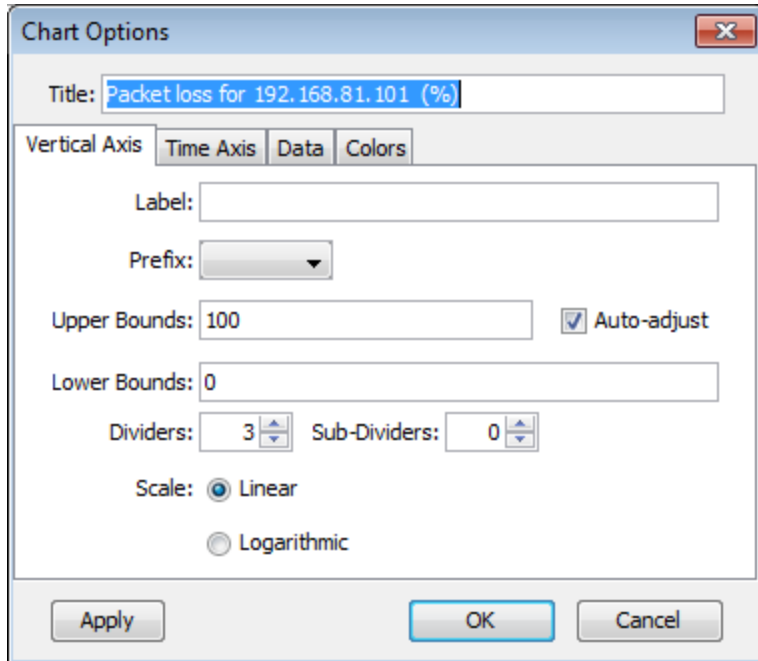
To apply changes to the Chart Options window:

1. Click **Apply** to apply changes you have made on any of the tabs, without closing the Chart Options window.
2. Click **Cancel** to undo any changes you've made and applied.
3. Click **OK** to apply any changes and close the window.
4. Close the window to save your changes.

Setting the Chart Title

The chart's title appears in the Charts menu and in the chart's title bar. Enter a title in the **Title** text box.

Vertical Axis Tab



The screenshot shows the 'Chart Options' dialog box with the 'Vertical Axis' tab selected. The 'Title' field contains 'Packet loss for 192.168.81.101 (%)'. The 'Vertical Axis' tab is active, showing fields for 'Label', 'Prefix', 'Upper Bounds' (100), 'Lower Bounds' (0), 'Dividers' (3), and 'Sub-Dividers' (0). The 'Auto-adjust' checkbox is checked. The 'Scale' is set to 'Linear'.

Vertical Axis Tab Parameters

- **Label** - adds a label for the vertical axis of the chart.
- **Prefix** - adds a prefix for the data displayed in the chart. Intermapper automatically scales the values to match this prefix, and inserts the prefix into the vertical axis label. (example: volts becomes μ -volts).

- **Upper Bounds, Lower Bounds** - controls the vertical scale of the chart. Valid values depend on the monitored variable.

NOTE: For larger values, use scientific E-notation. You can also enter these numbers in decimal notation (1000000, 1000000000). Larger numbers are displayed in the vertical axis in E-notation.

- To enter large values for the Upper or Lower Bounds, use the *nnEp* format, where *nn* = multiplicand, *E* = E-Notation, and *p* = power.
- To enter 1,000,000 (one million), type 1E6 (1×10^6).
- To enter 1,000,000,000 (one billion), type 1E9 (1×10^9).
- The largest unsigned 64-bit integer you can enter is just over 18.4E18 (18.4×10^{18} or 18,446,744,073,709,551,615).
- The largest signed 64-bit integer you can enter is just over 9.22E18 (9.22×10^{18} or 9,223,372,036,854,775,807).
- The largest negative signed 64-bit integer is -9.22E18 (-9.22×10^{18} or -9,223,372,036,854,775,808).
- If you type e or E, it is rendered as E.

- **Auto-adjust** - specifies if Intermapper automatically adjusts the scale of the chart. If the **Auto-adjust** check box is selected, the upper and/or lower bounds are adjusted automatically so data points are always displayed, no matter how much they increase or decrease.
- **Dividers, Sub-Dividers** - sets the number of horizontal dividers and sub-dividers that are displayed between the dividers.

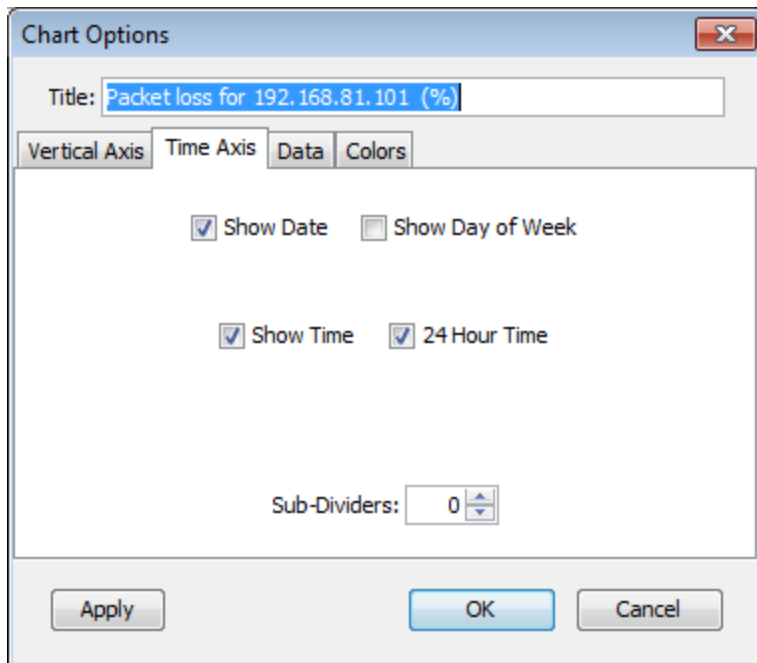
For example, to divide a chart into 10 parts, you need eleven dividers. You can do this in one of the following ways:

- Set the number of dividers to 11, with no sub-dividers.
- Set the number of dividers to 3, and the sub-dividers between each divider to 4.
- **Scale** - select **Linear** or **Logarithmic**. When you select *Logarithmic* scaling, you can set the Y-axis labels to powers of 10 by setting the desired upper and lower bounds and adjusting the number of dividers to match. A lower bound of 0 is converted to 1.

For example, to create a log scale with labels of 3000, 300, 30, and 3, do the following:

- Set the upper bound to 3000.
- Set the lower bound to 3.
- Set the number of dividers to 4.

Time Axis Tab

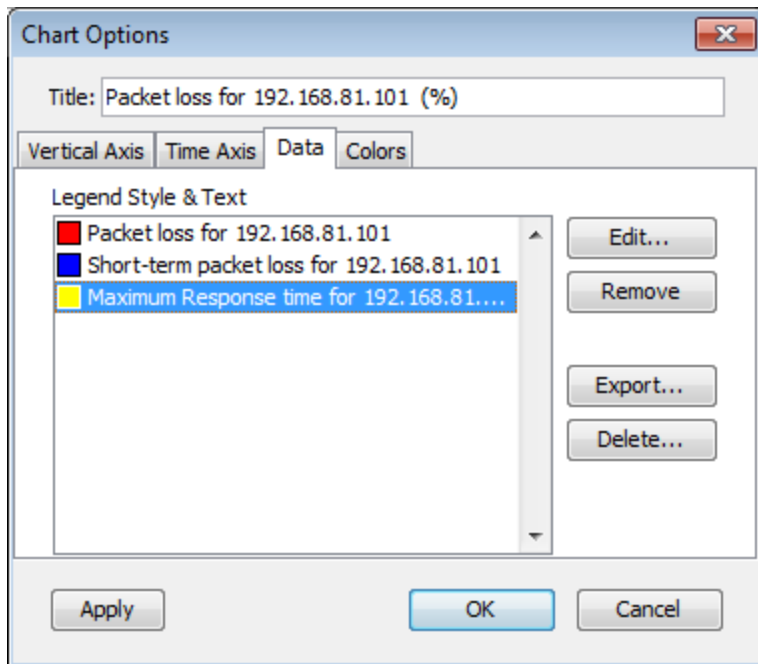


Time Axis Tab Parameters

- **Show Date, Show Day of Week, Show Time, 24 Hour Time** - specifies which labels are displayed on a chart's horizontal axis.
- **Sub-Dividers** - specifies the number of unlabeled vertical sub-dividers to draw between data points.

Data Tab

The Data tab displays a lists of datasets used in the current chart. Use the Data tab of the Chart Options window to export a dataset, to remove it from the chart, or to edit the appearance of a dataset's legend.



To remove a dataset from the chart:

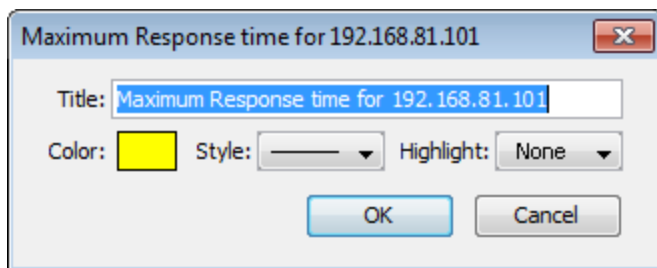
1. From the list of datasets, click the dataset you want to remove from the chart.
2. Click **Remove**. The dataset disappears from the list.

To export a dataset:

1. In the list of datasets, click the dataset you want to export.
2. Click **Export**. A standard file dialog is displayed.
3. Type a filename, select a location, and click **Save**. A tab-delimited text file is created, with one data value per line.

To edit the appearance of the legend for a dataset:

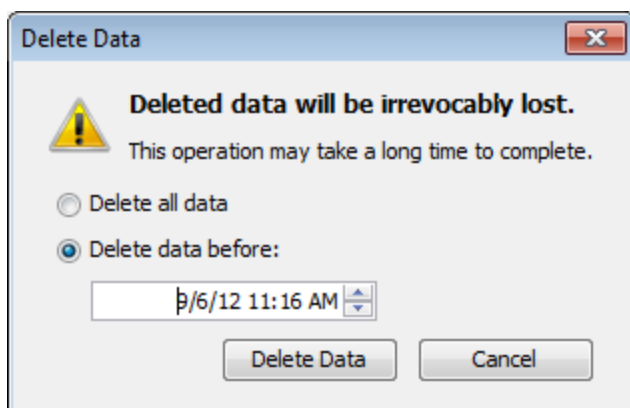
From the list of datasets, double-click the data for the set whose legend you want to edit. The edit window for the dataset's legend is displayed:



1. Click the **Color** rectangle and choose a color for the dataset.
2. Choose a line style for the dataset from the **Style** menu.
3. Choose a highlight icon for the dataset from the **Highlight** menu.
4. Edit the chart's title in the **Title** text box.
5. Click **OK** to save your changes.

To delete a range of data from a dataset:

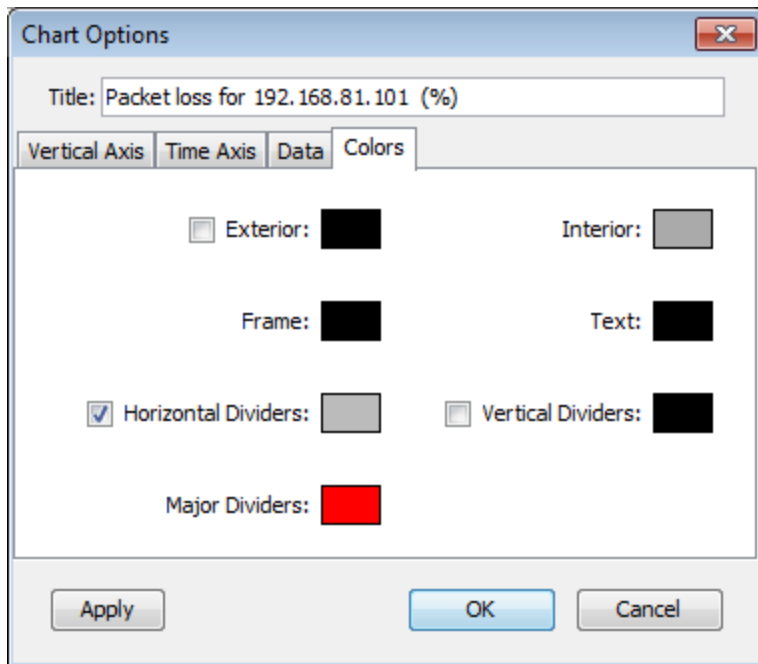
1. From the list of datasets, select the dataset containing the data you want to delete.
2. Click **Delete**. The Delete Data window for the dataset is displayed.



3. Set the date and time. Data before this date and time are deleted from the dataset.
4. Click **OK**. The data is deleted from the dataset.

Colors Tab

You can use the Colors tab of the Chart Options window to define the colors for various parts of the chart.



- **Exterior** - sets the color of the chart's background.
- **Interior** - sets the background color for the data area of the chart.
- **Frame** - sets the line color for the frame of the data area.
- **Text** - sets the color for the chart's text.
- **Horizontal Dividers** - sets the line color for the chart's horizontal dividers.
- **Vertical Dividers** - sets the line color for the chart's vertical dividers.

To change a color:

Select a color box. Use the system color picker to select a new color.

Chart Log Files

Intermapper can write chart data to a tab-delimited text file. You can specify separate log files for each chart, or you can send the data from several charts to a single log file.

To specify a log file to receive chart data:

1. From the [Chart dropdown menu \(Pg. 194\)](#), select **Log file**. The Create Log File window is displayed.
2. In the **Log File Name** text box, type the name of the new log file.
3. Set the preferences for the new log file using a window similar to the example on the right. For more information on creating log files, see [Log Files \(Pg. 231\)](#).
4. Click **OK**.

Each line of the tab-delimited file contains a date, timestamp, and the current values of the variables defined by the chart.

To stop logging data to a log file:

1. From the **Server Preferences** area of the **Server Settings** window, select the [Log Files \(Pg. 231\)](#). The Log Files panel is displayed.
2. Select the file for which you want to stop logging data.
3. Click **Remove**. The file is removed from the list and chart data is no longer written to that file.

Purging Chart Data

You can use a command line to purge data stored with charts. You can purge all chart data or you purge data from a specified number of days.

NOTE: Before running the purge command, Fortra recommends that you back up the Intermapper Settings folder (especially the Chart Data folder).

To purge chart data:

1. Stop the Intermapper server.
2. Run the purge command.
3. Start the Intermapper server.

The process for stopping and starting the Intermapper server varies, depending on your platform.

Purge Command Syntax

For Linux and macOS systems, the purge command includes the location of the Intermapper daemon configuration file. For example,

```
/usr/local/bin/intermapperd -f /usr/local/etc/intermapperd.conf --chart-purge [# of days]
```

Use the following syntax for Microsoft Windows systems:

```
"C:\Program Files\Intermapper\Intermapper.exe" --chart-purge [# of days]
```

The most recent `# of days` of chart data is retained; the rest is purged.

NOTE: Both of the commands above require administrative privileges.

- For Microsoft Windows systems, open the `cmd` window by clicking the **Windows** menu > **Windows System** > **Command Prompt** > **Misc** > **Run as Administrator**, or similar, depending on your operating system and how you access the `cmd` window.
- For Linux or macOS systems, preface the command with `sudo` or run the command as root.

Purging All Chart Data

To purge all chart data, type 0 for the **# of days**.

Purge Notes

- **Server must not be running** - specifies that the Intermapper server must not be running when you run the command.
- **Enabled maps only** - purges only charts from devices on enabled maps.
- **Administrative rights and write-access** - you must have administrative rights and write-access to the Intermapper Settings folder.
- For Microsoft Windows systems, open the `cmd` window by clicking the **Windows** menu > **Windows System** > **Command Prompt** > **Misc** > **Run as Administrator**, or similar, depending on your operating system and how you access the `cmd` window.

- For Linux or macOS systems, preface the command with `sudo` or run the command as root.
- If you have a large number of datasets with a substantial amount of accumulated data, the purge can take several hours to complete.

Log Window

Intermapper writes information about interesting events into [log files \(Pg. 231\)](#). These streams of information can be viewed in the Log window. This allows you to review log files without an external text editor.

Predefined Logs

[Audit Log on page 204](#)

Use this log to view changes that people make to Intermapper's data model. This log includes all of the information Intermapper stores about the network it monitors.

[Event Log \(Pg. 211\)](#)

Use this log to view all events generated during device monitoring. This log includes events where a device changes state, reasons for alarm notifications, and so on.

[Outages Log on page 222 \(Pg. 222\)](#)

Use this log to view a list of devices and networks that have been down and when they came back up.

[Debug Log \(Pg. 222\)](#)

Use this log to view a list of detailed debug messages that can be useful when debugging Intermapper.

You can create and control the preferences for log files from the Log Files panel of the Server Settings window. For more information on creating, viewing, and controlling the events that appear in log files, see [Server Preferences - Log Files. \(Pg. 231\)](#)

NOTE: Debug logs and Event logs are encoded in UTF-8 format. To edit these files, your text editor must support UTF-8 encoding to view foreign characters correctly.

Audit Log

Intermapper records changes that people make to InterMapper's data model, which includes all of the information InterMapper stores about the monitored network. This information is written to the log files and can be viewed in one of the Log windows. The Audit Log is a predefined log that is included with InterMapper.

If someone edits a map by moving, adding, editing, or deleting an item, those activities are recorded in the audit log. Information, such as the date and time, who made the change, from which computer they connected, and what was changed, are recorded in this log.

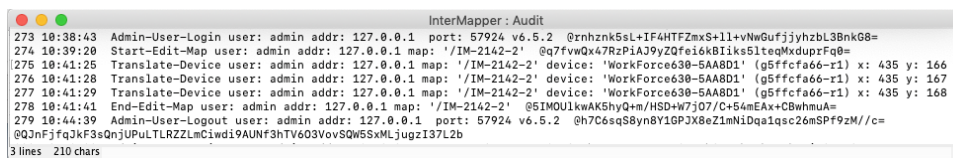
Bulk changes initiated by people can generate many entries in the audit log, such as the following:

- A user initiates an autodiscovery.
- A user initiates a network scan.
- A user imports data.

Other changes that are not initiated by a person, such as device or interface status changes or the sending of notifications are not written to the audit log because they are not initiated by a person. They are instead recorded in the Event Log.

To open the Audit log:

From the **Logs** submenu of the **Window** menu, select **Audit**.



```

InterMapper: Audit
273 10:38:43 Admin-User-Login user: admin addr: 127.0.0.1 port: 57924 v6.5.2 @rnhznk5sL+IF4HTFZmxS+1l+vNwGufjyjhzbL3BnkG8=
274 10:39:20 Start-Edit-Map user: admin addr: 127.0.0.1 map: '/IM-2142-2' @q7fwQx47RzPiAJ9yZQfeik8Iks5lteqMxduprFq0=
275 10:41:25 Translate-Device user: admin addr: 127.0.0.1 map: '/IM-2142-2' device: 'WorkForce638-SAA8D1' (g5ffcfaf66-r1l) x: 435 y: 166
276 10:41:28 Translate-Device user: admin addr: 127.0.0.1 map: '/IM-2142-2' device: 'WorkForce638-SAA8D1' (g5ffcfaf66-r1l) x: 435 y: 167
277 10:41:29 Translate-Device user: admin addr: 127.0.0.1 map: '/IM-2142-2' device: 'WorkForce638-SAA8D1' (g5ffcfaf66-r1l) x: 435 y: 168
278 10:41:41 End-Edit-Map user: admin addr: 127.0.0.1 map: '/IM-2142-2' @5IMOUlkWAK5hyQ+m/HSD+W7jO7/C+54mEAX+CBwhmuA=
279 10:44:39 Admin-User-Logout user: admin addr: 127.0.0.1 port: 57924 v6.5.2 @h7C6sqS8yn8Y16P3X8eZ1mNiDqa1qsc26mSPf9zM//c=
@QJnFjfQ3Kf3sQnJUPuLTLRZZLmCiwdi9AUNf3hTV603VovSQW5SxMLjugzI37L2b
3 lines 210 chars

```

Security

The Audit log cannot be edited, even by an administrator, without the change being detected.

Creation and Location of Audit Logs

Audit logs, along with other InterMapper logs, are stored in the InterMapper Settings/InterMapper Logs directory. The log filenames use the format of AuditYYYYMMDD.txt, where YYYY is the year, MM is the month, and DD is the day. New log files are created at midnight, or the first time the InterMapper server starts on a new day, so it can contain up to a day's worth of events.

Sample Audit Log Entries

```

1 15:41:59 Starting InterMapper Audit Log File (6.5.2b2/Build
14C153/i386/Darwin/64-bit). @J0GfOVGUNFvZIkYxUJ5NZrPO8H4+Mg+JsJ+ENT2yh1I=

2 15:42:12 Admin-User-Login user: Admin addr: 127.0.0.1 port: 59629 v6.5.2
@5BFu6dgkl3bIy/stBiW+HTNDjpaveK5k6kvTSvPjpzw=

3 15:46:54 Start-Edit-Map user: Admin addr: 127.0.0.1 map: '/My Island'
@BgmJ9yD+ip5NvfJxnkGZaVfyQSntRE/YtsM6WFohHlY=

4 15:47:20 Translate-Device user: Admin addr: 127.0.0.1 map: '/My Island' device:
'Tex-Ubuntu' (g5f3135c8-r9) x: 531 y: 97
@JJZVGPvchCHz7CILyonWXgi8Y704lgRPLCLBlvNHeSc=

5 15:47:30 End-Edit-Map user: Admin addr: 127.0.0.1 map: '/My Island'
@mpdQbP8akL+BDvghiIxwsS9/Mx4dG76EAx84haUFols=@9vbwYcHvamfYZwwK17G3mjj1qWy/2GOqRGN
PB2hLlGHpE94CPVvk2oQyH68xSWgEU

```

Log Entry Structure

The Audit log entries use the following structure:

The first line of the Audit log does not follow the standard log pattern. Instead, it indicates the time when the audit log file is created, InterMapper's version number, build number, computer information, and operating system.

Subsequent lines follow a consistent pattern; the first 5 fields are always present. The fields are as follows:

```

line number
timestamp
event type

```

The fourth and subsequent fields start with a field name and colon. The fields are as follows:

```

name:
addr:

```

where *name*: is the username that triggered the event and *addr*: is the IP address of the computer the user is connected from.

The next one or more fields indicate which object is affected by the event. In many cases, the object is a map, indicated by the field name map: followed by the name of the map in single quotation marks ('').

Commonly, the object is a device on a map. In this case, this includes 'map:', map name, device:, the nickname of the device, and the device ID in parentheses. For example, g5f3135c8-r9.

There might be other information beyond the object of the event, such as the x and y coordinates. This information is also in the form field_name: followed by the value.

All lines in the audit log end with a digital signature, which implements the security feature of the Audit log.

Events Recorded in the Audit Log

The following table shows the events that are recorded in the Audit log:

Event	Associated Object	Other Information
Admin-User-Login	none	port: and Intermapper client version
User-Login	none	port: and Intermapper client version
Failed-Admin-Login	none	port: and Intermapper client version
Failed-User-Login	none	port: and Intermapper client version
Admin-User-Logout	none	port: and Intermapper client version
User-Logout	none	port: and Intermapper client version
Create-Notifier	name:	type:
Edit-Notifier	name:	type:
Delete-Notifier	name:	type:
Create-CSR	CSR:	
Upload-SSL-Cert	none	
Create-Map	map:	
Delete-Map	map:	

Event	Associated Object	Other Information
Import-Map	map:	filename:
Export-Map	map:	filename:
Import-Data-Directive	file:	directive:
Export-Data-Directive	file:	directive:, maps:
Edit-Retention-Policy	policy:	newValues:
Remove-Retention-Policy	policy(s):	
Set-Retention-Policy	map:, device:	variable:, policy:
Set-Retention-Policy	map:, interface:	variable:, policy:
Set-Probe-Data	map:, device:	probeName:, type:
Set-Community-String	map:, device:	
Set-Timeout	map:, device:	timeout:
Set-Poll-Interval	map:, device:	pollInterval:
Set-Ignore-Outages	map:, device:	ignoreOutages:
Set-Address	map:, device:	address:
Set-Device-Threshold	map:, device:	useMapDefaults: maxAllowedLostPackets: criticalInterfaceErrs: alarmInterfaceErrs: warningInterfaceErrs: criticalPktLossThresh: alarmPktLossThresh: warningPktLossThresh: criticalRTTThresh: alarmRTTThresh: warningRTTThresh:

Event	Associated Object	Other Information
Set-Device-Threshold	map:	useServerDefaults: maxAllowedLostPackets: criticalInterfaceErrs: alarmInterfaceErrs: warningInterfaceErrs: criticalPktLossThresh: alarmPktLossThresh: warningPktLossThresh: criticalRTTThresh: alarmRTTThresh: warningRTTThresh:
Set-Device-Threshold	Server-Settings	maxAllowedLostPackets: criticalInterfaceErrs: alarmInterfaceErrs: warningInterfaceErrs: criticalPktLossThresh: alarmPktLossThresh: warningPktLossThresh: criticalRTTThresh: alarmRTTThresh: warningRTTThresh:
Reset-Short-Term-Packet-Loss	map;, device:	
Set-Data-Retention-Policy	map;, device:	
Set-remoteaccess-ACLs	map: ACL-for-user:	
Set-webaccess-ACLs	map: ACL-for-user:	
Acknowledge-Device	map;, device:	
Acknowledge-Interface	map;, interface:	
Maintenance-Device	map;, device:	
Maintenance-Interface	map;, interface:	
Translate-Device	map;, device:	
Translate-Network	map;, network:	
Add-Edge	map;, device:	end:
Remove-Edge	edge:	
Add-Network	map;, network:	

Event	Associated Object	Other Information
Remove-Network	map:, network:	
Hide-Edge	map:, interface:	
Show-Edge	map:, interface:	
Add-Device	map:, device:	
Remove-Device	map:, device:	
Remove-Subnet	subnet:	
Change-Poll-Interval	map:	pollInterval:

Securing Audit Logs

To secure the Audit log, encryption and mechanisms are used to prevent the following from occurring:

1. Removing or changing the last summary line.
2. Removing or changing the encrypted text (after @) on any line.
3. Removing or changing text lines before @.
4. Changing the timestamp or line number of a line.
5. Removing any lines or the first line.
6. Adding more lines after the original file.
7. Switching two lines (even when their timestamps are exactly the same).
8. Changing the numerical portion of the file name (other portions can be changed). For example, changing Audit202011240000.txt to Audit202011240000_A.txt is allowed. However, if you change the numerical portion to Audit202011250000.txt, the verification can fail.

Audit Log Verification Example

To verify an audit log file, you must first shutdown the Intermapper Sever, and then issue the following command:

```
Windows: Run as administrator
intermapper --verify-auditlog
"C:\ProgramData\InterMapper\InterMapper Settings\InterMapper
Logs\Audit202011250000.txt"
```

Linux: You need to be root or privileged user to run this command, use 'su' command. You also need to add the flag "--debug" in

```
additional to --verify-auditlog:  
intermapperd --debug --verify-auditlog "/var/local/InterMapper_  
Settings/InterMapper Logs/Audit202011250000.txt"
```

macOS: You need to be root or privileged user to run this command,
use 'su' command.

```
intermapperd --verify-auditlog "/Library/Application  
Support/InterMapper/InterMapper Logs/Audit202011250000.txt"
```

Encryption/Decryption and Hash Algorithms

The following are used:

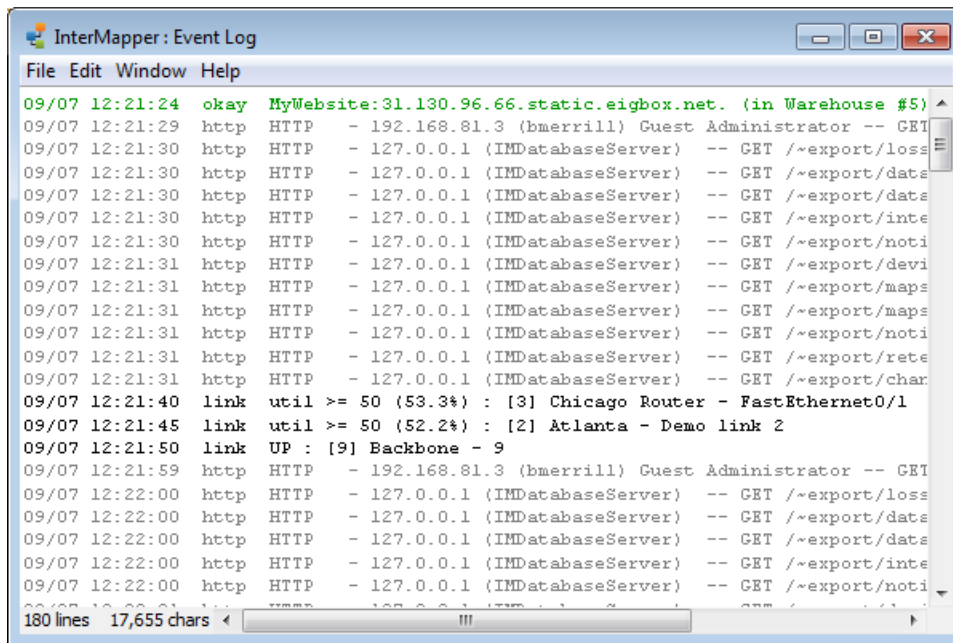
- Encryption/decryption algorithm
AES-256 encryption with OpenSSL library using CBC mode ciphers with 256-bit key and 128-bit IV
- MD5 Message-Digest Algorithm
Used to calculate log line hash and then encrypts the hash along with other parameters to form a line summary at the end of the line and a file summary at the end of the file.

Event Log

Intermapper writes information about interesting events into event logs. These streams of information are written to log files on disk and can be viewed in one of the Log windows. The Event Log is a predefined log file that serves as a default catch-all log file.

To open the Event Log:

From the **Logs** submenu of the **Window** menu, select **Event Log**.



The main Event Log window can show information about device ups and downs, high traffic on links, web, telnet, and InterMapper RemoteAccess server connections, as well as error messages.

As entries are written to the Event Log file, (stored in the InterMapper Settings/InterMapper Logs folder) they are also placed at the bottom of this window.

If you scroll to the bottom of the Event Log, it scrolls automatically as new events are appended to the log.

Event Log Messages

All event log messages use one of the following formats.

Message Format - Devices

```
<timestamp> <tag> <fullname>:: <message>
```

The <tag>s are:

```
"UP"      : <message> = "(Was down for <duration:3>)"
"DOWN":    <message> = "(Was up for <duration:3>)"
"okay":    <message> = <threshold-condition>
"warn":    <message> = <threshold-condition>
"alarm":   <message> = <threshold-condition>
"ACK"     : <message> = <acknowledge-message>
```



```
"UNAC": <message> = ""
"TRAP": <message> = <trap-message>
```

where the <duration:3> can be one of the following:

- [0-9]+ seconds?
- [0-9]+ minutes?, [0-9]+ seconds?
- [0-9]+ hours?, [0-9]+ minutes?, [0-9]+ seconds?
- [0-9]+ days?, [0-9]+ hours?, [0-9]+ minutes?

Message Format - All Other Events

```
<timestamp> <tag> <message>
```

Summary of Log Messages

This page lists all log messages that Intermapper writes to a log, with a description of each. Items shown in *italics* are variable names that are substituted with the proper value when the log message is created.

NOTE: Debug messages are not documented by Fortra, because they are subject to change and do not follow a specified format.

General Messages

The General messages describe Intermapper's actions as it starts up, enables and disables servers, and opens and closes map files. These messages are stored in the Event Log window.

```
**** Starting appName
```

Intermapper is starting. This entry contains the program's version number

```
**** Quitting appName
```

Intermapper is quitting.

```
**** Opening map docName
```

The named map is being opened.

```
**** Closing map docName
```

The named map is being closed.

http Starting web server on port *portnumber*

Intermapper is starting its web server on port *portnumber*.

http Stopping web server on port *portnumber*

Intermapper is stopping the web server.

imrm Starting Remote server on port *portnumber*

Intermapper is starting its Intermapper RemoteAccess server on port *portnumber*.

imrm Stopping Remote server on port *portnumber*

Intermapper is stopping the Intermapper RemoteAccess server.

tlnt Starting telnet server on port *portnumber*

Intermapper is starting its Telnet server on port *portnumber*.

tlnt Stopping telnet server on port *portnumber*

Intermapper is stopping the Telnet server.

Start-up error: Could not open *porttype* port *portnumber*.

Intermapper could not open the specified port during startup.

Error sending udp packet. (Err = *errNumber*)

Intermapper received an error attempting to send a UDP packet.

DNS-Related Messages

**** Address Change: "www" changed from x.x.x.x
to y.y.y.y. (DNS z.z.z.z)

The IP address for the device named www changed from x.x.x.x to y.y.y.y according to the DNS server at z.z.z.z.

**** No IP address for "www". (DNS z.z.z.z)

Intermapper could not determine an IP address for the device named www from the DNS server at z.z.z.z.

```
**** Name Change: "w.w.w.w" changed from "xxx"
to "yyy". (DNS z.z.z.z)
```

The IP address w.w.w.w changed its DNS name from xxx to yyy according to the DNS server at z.z.z.z.

```
**** No domain name for x.x.x.x. (DNS z.z.z.z)
```

Intermapper could not determine a DNS name for x.x.x.x from the DNS server at z.z.z.z.

```
**** "No response from DNS x.x.x.x when resolving 'yyy' to
an address.
```

The DNS server at x.x.x.x did not respond when attempting to resolve the DNS name yyy to an address.

```
**** "No response from DNS x.x.x.x when resolving
'y.y.y.y' to a name.
```

The DNS server at x.x.x.x did not respond when resolving the address y.y.y.y to a name.

```
dbug "DNS packet with bad format from y.y.y.y"
```

Intermapper received a DNS response with an invalid format.

```
dbug "Error ### while processing DNS reply from y.y.y.y"
```

Intermapper received an error while processing a DNS response.

```
**** Connected to
> Intermapper DataCenter at 127.0.0.1
```

Intermapper connected successfully to Intermapper DataCenter.

```
**** Disconnected from
> Intermapper DataCenter at 127.0.0.1
```

Intermapper disconnected successfully from Intermapper DataCenter.

Probe File Error Messages

The following messages describe problems with the Custom Probe files. Many of them are self-explanatory.

```
debug "MyProbe: Can't match "MyProbe"",
      cFileName, lineStr
```

```
debug "xxxx: Invalid Probe ID."
```

The probe xxxx contains an invalid ID (for example, the package is not a valid string).

```
debug "MyProbe: Invalid Probe Name.", cFileName
```

```
debug "MyProbe: Invalid Probe Human Name.", cFileName
```

```
debug "MyProbe: Probe definition does not contain a
      valid <description> section.", cFileName
```

```
debug "MyProbe: Probe definition does not contain a
      valid <snmp-device-variables> section.", cFileName
```

```
debug "xxxx: Probe definition does not contain a valid
      <snmp-device-display> section."
```

The xxxx probe file does not contain a valid <snmp-device-display> section.

```
debug "MyProbe: Probe definition does not contain a
      valid end tag for <MyProbe>.", cFileName, endTagStr
```

Telnet Server Messages

```
**** x.x.x.x denied access to tcp server.
```

An attempt to connect to the Telnet server from address x.x.x.x was refused.

```
tlnt TELNET - x.x.x.x denied access.
```

An attempt to connect to the Telnet server from address x.x.x.x was refused.

```
tlnt TELNET - x.x.x.x denied access because there are too
      many connections.
```

An attempt to connect to the Telnet server from address x.x.x.x was refused because there are too many connections already established.

```
tlnt TELNET - Accepted connection from x.x.x.x
```

A user at x.x.x.x successfully connected to the Telnet server.

```
tlnt TELNET - Accepted user connection from x.x.x.x
```

The Telnet server accepted a user connection from x.x.x.x

```
tlnt TELNET - x.x.x.x authenticated as "username".
```

The Telnet server accepted a connection from an authenticated user.

```
tlnt TELNET - Closed connection from x.x.x.x
```

The user at address x.x.x.x disconnected from the Telnet server.

Trap-Related Messages

```
trap "y.y.y.y (not on map) :: text-msg"
```

Intermapper received a trap from device y.y.y.y containing the *text-msg*.

```
trap "An error occurred while processing a SNMP trap
from y.y.y.y. (err = ###)"
```

Intermapper encountered an error processing a trap from y.y.y.y.

Notification Messages

```
ntfy "Silenced e-mail notification to "username"."
```

Intermapper suppressed an e-mail notification to the listed user because of the Snooze Alarm

```
ERR! "Failed to send e-mail notification to "username"
for "message: devicename" event. Check e-mail configuration.
(err = ###)"
```

Intermapper was unable to send an e-mail notification to the named person because of the error code ###

```
ntfy "Sent e-mail notification to "username"
for "message: devicename" event. (n
of m)"
```

Intermapper sent an e-mail notification as indicated. The "n of m" indicates that the n'th repeated message has been sent

```
ntfy "Silenced pager message notification to "username"."
```

Intermapper suppressed a page to the listed user because of the Snooze Alarm

```
ERR! "Failed to send pager notification to "username"
for "message: devicename". (err = ###)"
```

Intermapper was unable to send a page to the named person because of the error code ###

```
ntfy "Sent pager message notification to "MyProbe"
for "MyProbe: MyProbe".", itsUserName, eventMesg, deviceName
```

```
**** "Silenced sound notification to "MyProbe".",
itsUserName
```

```
ERR! "Failed to send sound notification to "MyProbe".
(err = %d)", itsUserName, err
```

```
ntfy "Silenced SNMP trap notification to "MyProbe".",
itsUserName
```

```
ERR! "Failed to send SNMP trap notification to "MyProbe"
for "MyProbe: MyProbe". (err = %d)", itsUserName, eventMesg,
deviceName, err
```

```
ntfy "Sent SNMP trap notification to "MyProbe"
for "MyProbe: MyProbe".", itsUserName, eventMesg, deviceName
```

```
ERR! "Failed to send e-mail notification to MyProbe.
Check user configuration.", itsUserName
```

```
ERR! "Failed to send pager notification to MyProbe.
(err = %d)", itsUserName, err
```

```
**** "Silenced all notifications until MyProbe.",
timeStr
```

```
ERR! "SMTP Failure: Can't connect to "MyProbe".
Error = %d", itsMailServer, err
```

```
ERR! "SMTP Failure: Server connection to "MyProbe"
idle for more than 4 minutes. Disconnecting...", itsMailServer
```

```
ERR! "SMTP Failure: Server "MyProbe" won't
  accept mail from MyProbe. (Reply = %d)", itsMailServer,
reversePath,
  replyCode
```

```
ERR! "SMTP Failure: Server "MyProbe" rejected
  recipient MyProbe. (Reply = %d)", itsMailServer, emailAddr,
replyCode
```

```
ERR! "SMTP Failure: Server "MyProbe" failed
  when sending mailto MyProbe. Mail not sent. (%s Reply = %d)",
itsMailServer,
  emailAddr, cmdName, replyCode
```

Web Server Messages

```
http HTTP - address (user)          authLevel --
commandargument
```

Intermapper received a *command* request for *argument* from *address*.

```
http HTTP - ERROR: JPEG compression failed. Compressed length
  = xxx. (Error = yyy)
```

Intermapper received an error code of *yyy* when attempting to compress the JPEG image whose length is *yyy* bytes.

```
http HTTP - ERROR: JPEG compression failed. Can't obtain/lock
  PixMap
```

Intermapper was unable to compress a JPEG image because it was already compressing an image. If this problem persists, quit Intermapper and relaunch it.

```
http HTTP - ERROR: JPEG compression failed. Can't create graphics
  offscreen. (Error = yyy)/dt>
```

Intermapper received the *yyy* error code when attempting to compress a JPEG image.

```
http HTTP - ERROR: PNG compression failed because there is not
  enough memory. (yyy K available)
```

Intermapper failed to compress the PNG image.

```
http "HTTP - ERROR: PNG compression failed. (Error
= ###) "
```

Intermapper received an OS error ### when attempting to compress the PNG image.

```
http "HTTP - y.y.y.y -- Unknown HTTP Version: xxx"
```

Intermapper received an unknown version - xxx - in an HTTP request from y.y.y.y.

```
http "HTTP - y.y.y.y -- Missing HTTP Version."
```

No HTTP version was included in the HTTP request from y.y.y.y.

```
http "HTTP - y.y.y.y -- Unknown HTTP Command: xxxx"
```

An HTTP request from y.y.y.y contained an unknown xxxx command.

```
http "HTTP - y.y.y.y -- Disconnected before response
was sent."
```

The HTTP client at y.y.y.y disconnected before Intermapper sent the entire response.

```
http "HTTP - ERROR: Unable to create ### x ### JPEG
image. (Error = err) "
```

Intermapper received an *err* OS error code when attempting to generate a ### x ### JPEG image.

```
http "HTTP - ERROR: Unable to create ### x ### PNG
image. (Error = err) "
```

Intermapper received an *err* OS error code when attempting to generate a ### x ### PNG image.

```
link "msg (util%) : [ifIndex] device-name - ifDescr"
```

Logged to the event log when the utilization crosses some threshold. The msg uses the "util < nn" or "util >= nn" format where nn is the threshold. The actual link utilization follows in parentheses. ifIndex, device-name, and ifDescr identify the individual interface.

```
dbug "device-name UTIL[ifIndex]=util? type: upTimeNow=nn,
upTimePrev=nn;inOctetNow=nn, inOctetPrev=nn; outOctetNow=nn,
outOctetPrev=nn;
bps=nn"
```


Logged to the event log when the interface utilization calculated is greater than 110%. In general, a value greater than 100% indicates an erroneous value for one of the inputs; this log message prints out all the inputs to the calculation for later analysis. *device-name* and *ifIndex* indicate the interface, *util* is the utilization percentage, *type* indicates the type of calculation: FullDuplex or Baseband. The other numbers are the values of *sysUpTime.0*, *ifInOctets*, *ifOutOctets*, and *ifSpeed*.

```
dbug Saved backup copy of mapname in "Intermapper
  Settings:Old Maps" folder.
```

Intermapper saved a copy of the original file (*mapname*) in the Old Maps folder before saving a version of the file in a newer format. This allows you to retrieve the earlier file and use it with an older copy of Intermapper.

```
dbug An error occurred while attempting to save backup
  copy of mapname
```

Intermapper could not create a backup copy of the named map.

```
dbug Can't locate backup folder to save backup copy of
  mapname
```

Intermapper could not locate or create the Intermapper Settings:Old Maps folder.

```
dbug Device 'devicename' was using non-existent
  probe 'probename', now set to non-polling.
```

The named device was set to be probed with a non-existent probe type. It has been set to non-polling and is no longer probed.

Intermapper RemoteAccess Server Messages

```
imrn "Accepted user connection from y.y.y.y."
```

An Intermapper RemoteAccess user connected from y.y.y.y.

```
imrn "Closed connection from y.y.y.y."
```

Intermapper closed the connection to the Remote client at address y.y.y.y.

```
imrn "y.y.y.y denied access."
```

The Intermapper RemoteAccess client at y.y.y.y was denied access.

```
imrn "y.y.y.y denied; too many connections."
```

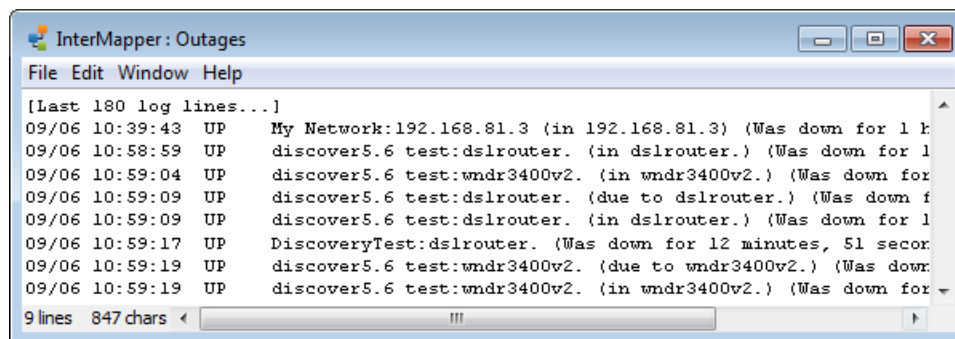
Intermapper denied access to an Intermapper RemoteAccess client because it already had too many connections operating.

Outages Log

Intermapper summarizes outages that have occurred in the Outages Log. An outage is a device that has gone from the UP state to the DOWN state and returned back to the UP state. Intermapper tracks the start and end time of the outage and computes the duration. Each time a device goes DOWN and then comes back UP, an entry is added in the Outages log.

To open the Outages log:

From the **Logs** submenu of the **Window** menu, select **Outages**.



The Outages window shows the start and end time and the duration of outages.

The controls in the Outages window are identical to the [Event Log \(Pg. 211\)](#) window.

Debug Log

Intermapper contains the following debug logs:

- **The Server Debug Log** - available from the Logs submenu of the Window menu.
- **The Client Debug Log** - available from the Diagnostics submenu of the Help menu.

Server Debug Log

The Server Debug log contains details of the Intermapper server's operations that can help troubleshoot various configuration problems. It stores messages generated by the server.

```

InterMapper: Debug
File Edit Window Help
14:44:35 Saving Map "g4fff5446-discover5.6 test" took 0.95 seconds (36 records, 153.80 K)
14:44:45 Saving Map "g4fff5446-discover5.6 test" took 0.93 seconds (36 records, 153.80 K)
14:44:55 Saving Map "g4fff5446-discover5.6 test" took 0.95 seconds (40 records, 154.12 K)
Loading probes took 1.700 seconds.
      header      232  0.017  0.98%
      description  232  0.050  2.94%
      parameters  213  0.033  1.96%
      script       82  0.150  8.82%
      script-output 53  0.000  0.00%
      snmp-device-variables 90  0.167  9.80%
snmp-device-variables-ondemand 6  0.033  1.96%
      snmp-device-thresholds 77  0.017  0.98%
      snmp-device-alarmpoints 16  0.000  0.00%
      snmp-device-notifiers 1  0.000  0.00%
      snmp-device-display 91  0.067  3.92%
      snmp-device-properties 40  0.000  0.00%
      command-line 22  0.000  0.00%
      command-exit 22  0.000  0.00%
      command-display 22  0.000  0.00%
      files-and-versions 0  0.000  0.00%
      autorecord 43  0.000  0.00%
      datasets 0  0.000  0.00%
      tool 21  0.000  0.00%
      postflight 0  0.000  0.00%
      Time remaining 0.150  8.82%
Probe which loaded the longest: "com.dartware.automatic". Loading time: 0.017 seconds.
180 lines 8,277 chars

```

The following are examples of information that is stored:

- A series of messages generated when the server is started or stopped.
- A message when a map is opened or saved.
- A series of messages when probes are reloaded.
- Most messages contain an indicator of how long a particular operation took.

To open the Server Debug log:

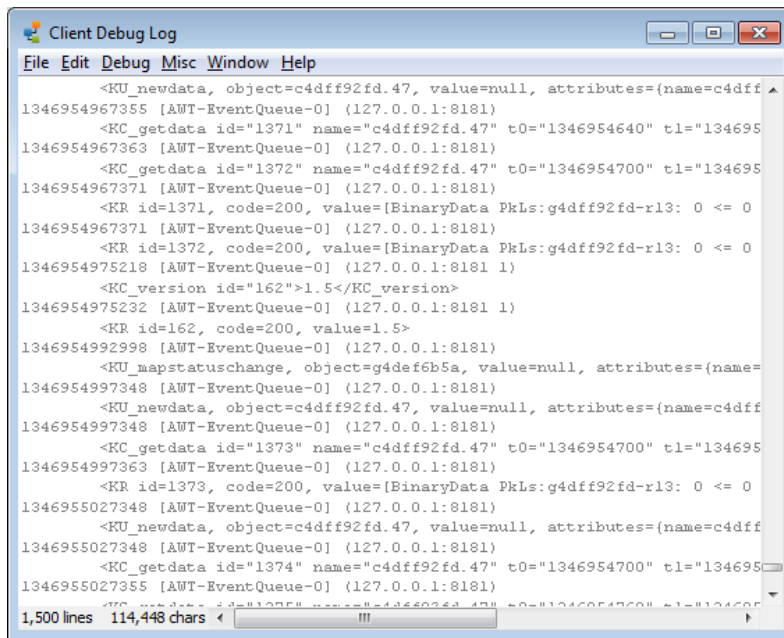
From the **Logs** submenu of the **Window** menu, select **Debug**.

Client Debug Log

The Client Debug Log shows details of InterMapper's operations that can be valuable for debugging problems with the program. If you have trouble with InterMapper, the support staff might ask you to [Send Feedback](#). The Send Feedback form sends the Client Log by default.

Client Debug Log Window

The Client Log Window shows the contents of the Client Log.



To open the Client Debug Log:

From the **Diagnostics** submenu of the **Help** menu, select **Client Debug Log**.

macOS:	Command + Option + Shift + Z
Microsoft Windows:	Control + Alt + Shift + Z
Linux:	

The Client Debug Log window is displayed and the **Debug** and **Misc** menus are displayed in the menu bar at the top of the window.

In general, Fortra does not document the information shown in the Client Debug Log window, because its messages change from version to version.

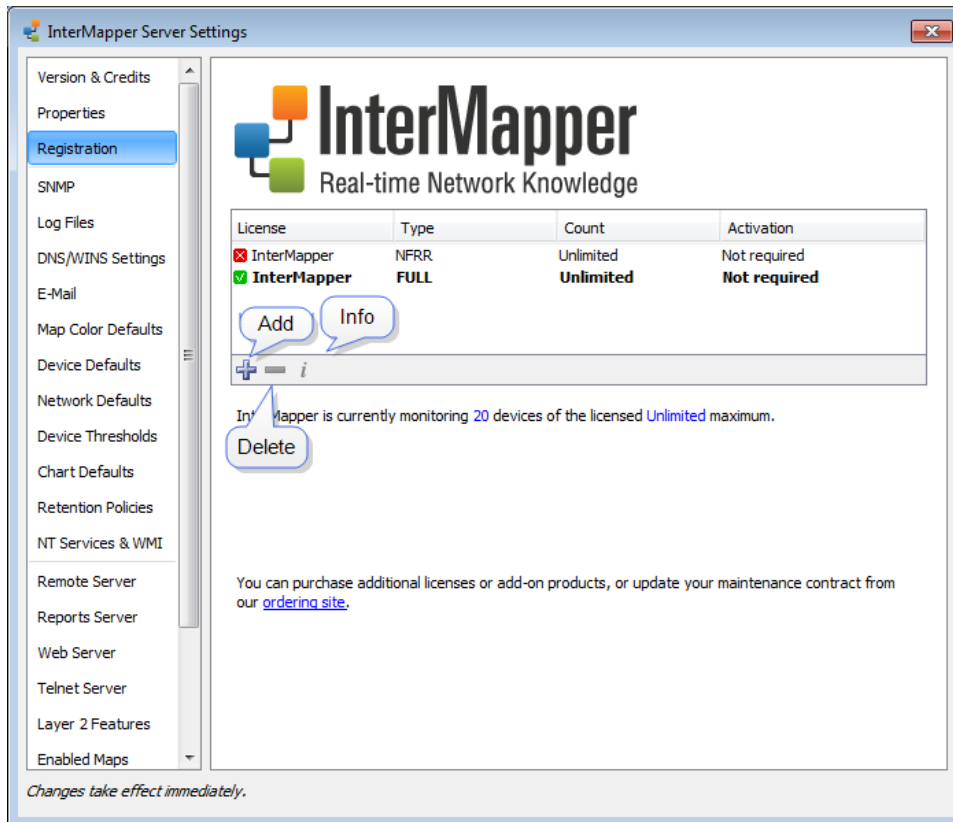
NOTE: Opening the Client Debug Log window creates two new menus. Certain items in these menus are designed to test Intermapper's crash recovery facilities. Others exercise portions of the program that might crash.

Server Settings

Use the Server Settings window to view and edit the settings of an Intermapper server. You must have administrator privileges to access the Server Settings window.

The Server Settings documentation in this manual is divided into the following topics:

- [Server Information Panels \(Pg. 225\)](#) - view information about the Intermapper version. View and edit the server name and software licenses.
- [Server Preferences Panels \(Pg. 228\)](#) - set defaults and other preferences for your server.
- [Server Configuration Panels \(Pg. 249\)](#) - set up the web, telnet, reports, and Intermapper remote servers, enable and disable maps, create users and groups and set up map access, define notifiers, and set up an SSL certificate for the Intermapper server.



Use the Server Preferences section of the Server Settings window to view and edit default Intermapper's server settings.

To view and edit Intermapper server settings:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed, showing three sections of settings on the left. On the right is a panel in which the selected settings are displayed.
2. Click the subsection for the settings you want to edit. The selected settings are displayed in the right panel.

Server Information Panels

Use the Server Information panels of the Server Settings window to view and edit information about the current version of Intermapper and your system.

Intermapper Version and Credits

Use the Version & Credits panel to view the following information:

Version	View the version of Intermapper that is currently running.
Built On	View the date when the Intermapper software was built.

Properties

Use the Properties panel to view information about the Intermapper host system. You can also set the server name from this panel.

Server Name	The name of the machine where Intermapper is running. This name is displayed in the Map List window.
Hardware ID	The hardware ID of the machine Intermapper is licensed and running on.
<OS type> System Version	The type of operating system and version number.
<OS type> Running Time	The length of time the operating system has been running.
Server Running Time	The length of time the Intermapper server has been running.
Network Interfaces	The network interfaces available on the machine where Intermapper is installed.

Registration

Use the Registration panel to view information about your monitored devices, to view a list of licensed products, and to add new licenses.

License List	A list of licenses and add-on products.
---------------------	---

Monitoring information	<p>The number of monitored devices and your licensed monitoring limit are shown below the Intermapper logo.</p> <div data-bbox="396 310 1421 436"> <p>NOTE: Some Intermapper licenses specify the number of devices that you can monitor. Demo probes do not reduce the number of devices available for monitoring.</p> </div>
-------------------------------	---

Registering Your Software

After you install and run Intermapper, the License Key Required dialog is displayed. From this dialog, you can register your copy of Intermapper.

To register Intermapper:

1. From the **License Key Required** dialog, select one of the following:
 - **Enter a license key now** - if you already have a key, you can enter that key now.
 - **Request a trial license key** - if you do not have a key and want to request one. The Request Trial License window is displayed.
 - **Order now** - to purchase the product.

Requesting a Trial License

To request a trial license:

1. Click **Request a trial license key**.
The Request Trial License dialog is displayed.
2. Click **Send Request**.
Intermapper contacts to retrieve a trial key. The new key is displayed in the area shown above.
3. Click **Register**.
The Register InterMapper Server dialog is displayed.
The license shows the registered name, type of license, and the number of devices and other licenses associated with the key.
4. Click **Register**.
The license key is registered.

Entering Multiple Licenses

You can enter multiple serial numbers to unlock additional Intermapper functionality. The Registration pane in the Intermapper Server Settings window shows the licenses that are currently registered.

To enter multiple licenses:

Click the Registration tab and select one of the following options to add, delete, or view your license information:

- **+** - to add a new license or serial number.
- **-** - to remove the selected license or serial number.
- **i** - to view detailed information about the selected license or serial number.

Server Preference Panels

Use the following panels of the Server Settings window to set global preferences for the selected server.

You can view and edit the following settings from the left pane of the Server Settings window:

- [SNMP \(Pg. 228\)](#)
- [Log Files \(Pg. 231\)](#)
- [DNS/WINS settings \(Pg. 235\)](#)
- [E-Mail \(Pg. 236\)](#)
- [Map Default Colors \(Pg. 238\)](#)
- [Device Defaults](#)
- [Network Defaults \(Pg. 239\)](#)
- [Chart Defaults \(Pg. 243\)](#)
- [Device Thresholds \(Pg. 241\)](#)
- [NT Services & WMI \(Pg. 249\)](#)

NOTE: You can also set preferences for a particular map using the **Map Settings** panel, available from the Edit menu. For more information, see [Map Settings \(Pg. 68\)](#).

SNMP Preferences

You can use the SNMP subsection of the Server Preferences section to set the default SNMP settings for each SNMP access method. These settings are used for all new devices.

SNMP Versions

Intermapper can retrieve data from devices using SNMP version 1, version 2c, or version 3. Each of these can access the same SNMP information, but through the following means:

- **SNMPv1** is the original version and provides a simple means for retrieving data. Security is provided through community strings that act like passwords to allow or deny access to the information. The Read-Only community string provides permission to the requester to read data and the Read-Write community string provides permission to modify data. All data transmissions (including the community string) are sent in the clear (unencrypted).
- **SNMPv2c** provides additional, more efficient methods to request data and adds new data types (such as 64-bit counters) so the monitoring system can gather more accurate data. SNMPv2c is like SNMPv1 in that it uses the same community string system and transmits data in the clear (unencrypted).
- **SNMPv3** provides the same data retrieval facilities as SNMPv2c, but with additional security. This is a secure method of providing authentication information (so the device knows whether to respond to the query or not), as well as a privacy function that encrypts the entire transmission so that eavesdroppers cannot discern the data.

What is an SNMP Community String?

The SNMP Read-only Community string is like a user id or password that allows access to a router's or other device's statistics. Intermapper sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device ignores the request and does not respond.

NOTE: SNMP Community strings are used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

Community String Types

The following community strings are available for SNMPv1-v2c-speaking devices:

- **SNMP Read-only community string** - enables a remote device to retrieve read-only information from a device. Intermapper uses this information on its maps.
- **SNMP Read-Write community string** - used when requesting information from a device and when modifying settings on that device. Intermapper does not use the read-write community string, since it never attempts to modify any settings on its devices.

- **SNMP Trap community string** - included when a device sends SNMP Traps to InterMapper. InterMapper accepts any SNMP Trap community string.

By convention, most SNMPv1-v2c equipment ships from the factory with a read-only community string set to public. It is standard practice for network managers to change all the community strings so that outsiders cannot see information about the internal network. (In addition, network managers might employ firewalls to block any SNMP traffic to ports 161 and 162 on the internal network.)

SNMP Server Settings Pane

InterMapper remembers the default settings for each of the various SNMP access methods. These are set in the **Server Settings > SNMP** preference pane.

These options control how InterMapper interacts using the Simple Network Management Protocol (SNMP).

SNMP Version: SNMPv1

SNMPv1-2c Community:

SNMPv3 Authentication: MD5

User name:

Privacy: None

☒ Listen for SNMP traps on UDP port 162

☐ Also listen for SNMP traps on port: 161

☐ Verbose trap logging

This pane allows you to specify the following:

- **SNMP Version** - the default SNMP version to be used for new devices in autodiscovery. InterMapper attempts to use the selected version when it discovers a new device. If it gets a response, it continues to use that version. If that fails, it pings the device.
- **SNMPv1-2c Community** - if the selected SNMP version is SNMPv1 or SNMPv2c, InterMapper uses this community string to attempt communication with the device.
- **SNMPv3 Authentication** - if the selected SNMP version is SNMPv3, InterMapper uses the specified authentication method (SHA, MD5, or None) with the indicated password on the right to authenticate with the device.
- **User Name** - the SNMPv3 user name used for authentication and privacy.

- **Privacy** - When using SNMPv3, the privacy method (DES, AES, or None) is used with the encryption password on the right.
- **Listen for SNMP Traps on UDP Port 162** - select this check box if you want Intermapper to listen for SNMP traps sent from devices to the standard port 162.
- **Also listen for SNMP traps on UDP port** - Intermapper can listen for traps on a second, non-standard port (in addition to port 162). Select this check box and enter the port number in the text box. Traps received on this alternate port are handled in the same manner as those received on port 162.
- **Verbose trap logging** - select this check box to display the full OID and contents for all varbinds of a trap, instead of simply the varbind contents.

Setting SNMP Preferences for Specific Devices

The panel shown above sets the default SNMP preferences that Intermapper uses when querying devices. You can also set SNMP preferences for individual devices on your map using the **Set Community...** (SNMPv1-v2c) or **Set Probe** (all three SNMP versions) commands, available from the Monitor menu. You can set various parameters for one or more devices at a time by selecting the devices you want to change before executing the command.

Log File Preferences

Intermapper writes information to log files about various events. Use the log files to review the events surrounding a particular problem, helping you to troubleshoot the problem more effectively.

To view an existing log file:

From the **Logs** submenu of the **Windows** menu, select the file you want to view.

To view and edit the preferences for log files:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
2. Click **Log Files**. A list of log files is displayed in the right panel, showing the current Log File preferences for the selected log file.

Setting Preferences for Log Files

Name	Rotate Interval
Audit	Daily at 00:00
Debug	Daily at 00:00
Event Log	Daily at 00:00
Outages	Daily at 00:00
Paging	Daily at 00:00
SMS	Daily at 00:00

Log File Name: Audit **<date>.txt**

Start New Log File: Once a Day

Every day at 00:00

☒ Delete log files after 7 days

☐ Also send messages to syslog server

IP Address:

Facility: local0

Severity: emergency

[Delete this Log](#)

This log file is recording all Audit events.

The Log File preferences pane shows a list of currently defined log files with properties for the selected file.

- To see a brief explanation of the function of a log file, click the log file. The explanation is displayed in the lower panel of the Preferences pane.
- To add a log file, click **Add New Log**. The [Log File Preferences \(Pg. 233\)](#) for the new log file are displayed.
- To edit a log file definition, select a log file definition. The properties for the selected log file are displayed. The [Log File Preferences \(Pg. 233\)](#) for the selected log file are displayed.
- To delete a log file, select a log file definition and click **Delete this Log**. The log file definition is removed from the list.

NOTE: The Audit Log, Debug Log, Event Log, and Outages Log cannot be deleted.

Log File Preferences

The example above shows typical log file preferences (names of the log files and their rotation intervals).

To add a new log file:

1. Click **Add New Log**. The [Log File preferences \(Pg. 233\)](#) for the new log file are displayed.
2. [Set the log file preferences \(Pg. 233\)](#) as described below.

To edit preferences for an existing log file:

1. Select the log file. The [Log File preferences \(Pg. 233\)](#) for the selected log file appear.
2. [Set the log file preferences \(Pg. 233\)](#) as described below.

Setting Log File Preferences

Log File Name - the filename prefix of the log file. This field is limited to 14 characters (see [Log File Naming and File Format \(Pg. 234\)](#) below.) The file is given a .TXT extension and can be edited with any text editor.

Start New Log File - the frequency and at what point in a log cycle the current log file is closed and a new one is opened. This allows you to break the log files down into convenient sizes and/or time epochs. The following options are available:

- Never
- Once daily
- Twice daily
- Once weekly
- Twice weekly

Delete log files after __ days/weeks - when selected, forces Intermapper to delete old log files automatically after a certain date.

NOTE: Each time Intermapper starts a new log file, it checks to see if any log files should be deleted. On platforms where the file creation date is available, it is used to determine whether a log file should be deleted. If the creation date is not available, the file's last modification date is used.

Also send messages to syslog server - specifies that all log file entries are sent to a syslog server. Set the values for the following:

- **IP Address** - the IP address for the syslog server.
- **Facility** - select a value to match your local system conventions.
- **Severity** - select a value to match your local system conventions.

Redirecting Log Entries

By default, all entries are stored in the built-in Event Log file. You can redirect streams of log entries from Intermapper's remote server, web server, or Telnet server to a particular log file

(and syslog server). This can be useful, for example, for sending all web access events to one file and all outage events to a different file.

To redirect a log entry stream:

1. Create a new log file definition for the file you want to receive the log entries.
2. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
3. From the left panel of the **Server Settings** window, select the server (**Remote**, **Web**, or **Telnet**) whose log entries you want to send to a different log file. The panel for the selected server is displayed.
4. In the **Send Log File Entries to** menu, select the log file you created to receive the log entries. All log file entries for the selected server are redirected to the new log file.

Log File Naming and File Format

Log files are saved in text format in the InterMapper Settings:Intermapper Logs folder. Each file has a user-defined prefix that describes its function, and ends with a suffix of `.yyyymmddhhmm.txt`, where the suffix is the (four-digit) year, month, day, hour, and minute when the file was created. The prefix is limited to 14 characters.

Log File Sources

Log information comes from several sources, including the following:

- Up and down entries for the devices being logged
- Hits on the built-in web server
- Connections to the InterMapper RemoteAccess and Telnet server
- InterMapper's own internal status and error messages

The following built-in log files are always present and cannot be deleted:

- **Audit Log** - when you first launch InterMapper, the Audit log file receives records of changes that people make to InterMapper's data model, which includes all of the information InterMapper stores about the monitored network.
- **Event Log** - when you first launch InterMapper, the Event log file receives all entries from all sources. You can divert certain streams to other log files.
- **Outages** - contains entries that describe the start and end times of outages, as well as their duration. This stream of entries cannot be redirected to any other log file.
- **Debug** - displays certain debugging information, as described in [The Debug Window \(Pg. 222\)](#).

DNS/WINS Settings

Use the DNS/WINS Settings section to specify the DNS server(s) and WINS server(s) that Intermapper uses. Intermapper uses your current DNS servers as its default.

Intermapper can use one or more Domain Name Service servers (DNS) to convert DNS names to addresses and back. Intermapper checks the listed DNS servers at regular intervals to make sure that the DNS name and IP address for a device match.

When you start Intermapper on a macOS or Microsoft Windows machine, the DNS servers specified by the current network configuration are used. On Linux machines, you must manually enter one or more DNS server addresses.

DNS addresses are optional: if the preference is empty, Intermapper does not attempt to convert DNS servers to and from IP addresses.

For example, when Intermapper polls a device that has a name assigned, it looks up the corresponding IP address in the DNS. If the resulting address changed since the device was added to a map, Intermapper logs an error message.

InterMapper will use the Domain Name Servers listed below to look up device names and IP addresses.

Comma-separated list of DNS server addresses:

192.168.81.1

Search Domain:

Minimum interval between DNS checks: 5 Minutes

☒ Use WINS name resolution

InterMapper will use the WINS Servers listed below to look up device names and IP addresses.

Comma-separated list of WINS server addresses:

☒ Use broadcast if lookup fails

WINS Scope:

Setting DNS Monitor Preferences

To set DNS Monitor preferences:

Do one of the following:

- **Comma-separated list of Domain Name Server addresses** - a list of Domain Name Server addresses, separated by commas (,).
- **Search Domain** - names to append to a partial domain name to make a fully-qualified domain name.
- **Minimum interval between DNS checks** - the amount of time to wait between successive queries for a host. Use a larger value to reduce the number of times the DNS is checked.

Setting WINS Preferences

You can specify one or more WINS servers that Intermapper uses for WINS lookups. Intermapper can also fall back to broadcast lookups for WINS/NetBIOS name lookups. Unless instructed by your network administrator, you should usually leave the WINS Scope blank.

- **Use WINS name resolution** - allows Intermapper to use the specified WINS servers to look up device names and addresses.
- **Comma-separated list of WINS server addresses** - a list of addresses, separated by commas (,).
- **Use broadcast if lookup fails** - allows Intermapper to use broadcast lookups for WINS/NetBIOS lookups if the WINS lookup fails.
- **WINS Scope** - WINS Scope. This should only be necessary if instructed by your network administrator.

Email Preferences

You can use this panel to enter the information required to send email notifications.

InterMapper sends e-mail notifications to these SMTP servers using the sender information specified.

Primary SMTP	Host:	<input type="text"/>	Port:	<input type="text"/>
	User:	<input type="text"/>		
	Password:	<input type="text"/>		
Back-up SMTP	Host:	<input type="text"/>	Port:	<input type="text"/>
	User:	<input type="text"/>		
	Password:	<input type="text"/>		

The From: line and Errors-To: line of the message will be set to the values below.

From address:	<input type="text"/>
Errors to:	<input type="text"/>

☐ Automatically e-mail InterMapper crash reports

Send crash reports to:

Setting Email Preferences

- **Primary SMTP** - the host name. If your SMTP server requires authentication, enter a User, Password, and Port for the primary SMTP host. Port 25 is typically used for outgoing email servers.
- **Back-up SMTP** - the host name. If your SMTP server requires authentication, enter a User, Password, and Port for the back-up SMTP host. If you are unsuccessful sending emails through the primary host, InterMapper attempts to deliver email messages through the back up host.

NOTE:

InterMapper supports the PLAIN and CRAM-MD5 authentication commands. You can use different email accounts and passwords for the primary and back up SMTP servers.














- **From address** - the email address you want to appear as the From line of the message.
- **Errors to** - the address you want to use in the Errors-To line of the message. Bounced messages are returned to this address.
- **Automatically e-mail InterMapper bug reports** - allows InterMapper to automatically send reports of errors and bugs to the staff at Fortra.
 - **Send bug reports to** - the email address you want to use when sending bug reports.

Default Map Colors

When Intermapper creates a new map, it uses a set of default colors for the items and features on the map. Use the Map Colors preferences to set the default colors for a map.

You can use the Default Map Colors preference to view and edit the default colors for all map items and features.

Click a color below to change the default color of the corresponding map feature.

Background: 	Links: 
Ants: 	Labels: 
Networks: 	Discovery: 
Up: 	Warning: 
Alarm: 	Critical: 
Down: 	Unknown: 
Acknowledged: 	

Click any of the colors to open the Color Picker and select a different color for that device/link.

To view and edit the Default Map Colors preference:

From the **Server Preferences** section of the **Server Settings** window, click **Map Color Defaults**. The Map Color Defaults preferences are displayed in the right pane.

Changeable Colors

The following colors can be defined.

- **Background** - the map's background color. This is overridden by a background image.
- **Ants** - the color of the traffic flow indicators that appear on a link. These are often referred to as marching ants. Traffic flow indicators only appear in links to SNMP devices.
- **Networks** - the default color of network ovals.
- **Up** - the color of devices that are in the Up state.
- **Alarm** - the color of devices that are in Alarm state.
- **Down** - the color of devices that are in the Down state.
- **Acknowledged** - the color of devices that have gone down and the outage has been acknowledged.
- **Links** - the color of links, the connections between devices, networks, and interfaces.
- **Labels** - the default color of device and network labels.
- **Discovery** - the color of a network that is the target of the discovery process.
- **Warning** - the color of devices that are in the Warning state.
- **Critical** - the color of devices that are in the Critical state.
- **Unknown** - the color of devices that are in an Unknown state.

To change a map color:

1. Click in the feature area. The Color Picker is displayed.
2. Select a color.
3. Click **OK**.

NOTE: Changing the default colors changes the colors assigned to an existing map only if the Use server defaults check box is selected in the map's settings (it is selected by default). You can change an individual map's colors from the [Map Settings \(Pg. 68\)](#) window.

Default Device and Network Preferences

When devices and networks are first added to the map, Intermapper shows devices as rectangles and networks as ovals.

You can use the Device Defaults and Network Defaults Preferences to change the default appearance of devices and networks.

NOTE: The Device Defaults and Network Defaults Preferences are identical in appearance and function. One affects the default appearance of devices, while the other affects the default appearance of networks.

Device Defaults

Device defaults are as follows:

New Devices on a map will have the appearance specified below.

Shape: Color:

Label Font:

Label Style: ☐ Bold ☐ Italic

Label Size:

Position:

Network Defaults

Network defaults are as follows:

New Networks on a map will have the appearance specified below.

Shape: Color:

Label Font:

Label Style: ☐ Bold ☐ Italic

Label Size:

Position:

Numbered Networks:

Setting Default Device and Default Network Parameters

To view and edit the default Device and Network parameters:

1. From the **Map List** window, select any map on the server whose settings you want to edit.
2. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
3. From the **Server Preferences** section, click the **Device Defaults** or **Network Defaults** subsection. The default settings for the selected subsection are displayed.
4. Edit the preferences as described below.
5. Click **OK**.

	Shape	the default shape for the device or network from the menu.
	Color	the default color for the device or network from the menu.
	Label Font	the default font for the device or network's label.
	Label Size	the default font size for the device or network's label.
	Position	the default position for the label text, relative to the device or network icon. NOTE: The Position parameter affects only Wire and Icon shapes.
	Edit Label...	the default labels for numbered and unnumbered networks, as described in Editing (Pg. 86) Labels (Pg. 86) .

Default Device Thresholds

You can set default device thresholds any new device added to a map.

NOTE: Only SNMP probes have thresholds for all three parameters (round-trip time, packet loss, and interface errors), a ping/UDP-based probe monitors only round-trip time and packet loss, and a TCP probe monitors only round-trip time.

For more information on device thresholds, see [Setting Error and Traffic Thresholds](#).

InterMapper Server Settings

Set interface thresholds to alert you to network problems.

Error Thresholds

	Warning	Alarm	Critical	
Rx Errors (Received):	10	20	30	per minute
Tx Errors (Transmitted):	10	20	30	per minute
Total Errors (Rx + Tx):	10	20	30	per minute

Utilization Thresholds

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

Discard Thresholds

	Warning	Alarm	Critical	
Rx Discards (Received):	15	25	35	per minute
Tx Discards (Transmitted):	15	25	35	per minute
Total Discards (Rx + Tx):	15	25	35	per minute

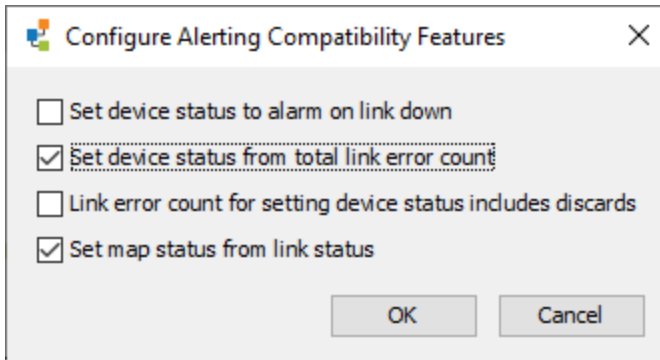
Compatibility Settings

Device/Interface alerting and map status interactions

Interface Alarm Behavior

To select a behavior:

1. From the **Intermapper Server Settings** dialog, select or clear the **Set device status to alarm on link** check box to control the behavior of alarms when an interface goes down.



2. Do one of the following:
 - Select the **Trigger an alarm for the device** check box to trigger an alarm when any interface goes down.
 - Select the **Trigger an alarm for an individual interface** check box to trigger an alarm when an individual interface goes down.

Default Server Interface Thresholds

You can set default thresholds for interfaces on any new device added to a map.

For more information on interface thresholds, see [Setting Error and Traffic Thresholds \(Pg. 181\)](#).

InterMapper Server Settings

Set interface thresholds to alert you to network problems.

Error Thresholds

	Warning	Alarm	Critical	
Rx Errors (Received):	10	20	30	per minute
Tx Errors (Transmitted):	10	20	30	per minute
Total Errors (Rx + Tx):	10	20	30	per minute

Utilization Thresholds

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

Discard Thresholds

	Warning	Alarm	Critical	
Rx Discards (Received):	15	25	35	per minute
Tx Discards (Transmitted):	15	25	35	per minute
Total Discards (Rx + Tx):	15	25	35	per minute

Compatibility Settings

Device/interface alerting and map status interactions

OK Cancel

Chart Defaults

Charts can show historical data for values received from one or more devices. You can use the Chart Defaults panel of the Server Preferences section of the Server Settings window to view and edit the default settings for a newly-created chart. For more information, see [Creating Charts \(Pg. 191\)](#) and [Using Charts \(Pg. 191\)](#).

To view and edit Chart Default preferences:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed, showing the list of available settings. Selected settings are displayed on the right.
2. Click **Chart Defaults**. The Chart Defaults panel is displayed in the right panel of the Server Settings window.

Axes Tab

You can use the Axes Tab of the Chart Defaults panel to define the appearance and behavior of newly-created charts.

Upper Bounds, Lower Bounds - controls the vertical scale of the chart. The range of values depends on the variable being monitored.

Auto-adjust - specifies if Intermapper adjusts the scale of the chart automatically. If the **Auto-adjust** check box is selected, the upper and lower bounds are adjusted automatically so data points are always displayed, no matter how much they increase or decrease.

Dividers, Sub-Dividers - click the up and down arrows or enter the number of dividing lines to set the number of horizontal dividers and to set the number of sub-dividers you want to appear between the dividers. For example, set the number of dividers to 3 and the number of sub-dividers to 4. This gives a total of 11 dividers. (Three dividers - top, bottom, and center, with four dividers between each. Eight sub-dividers and three dividers.)

Show Date, Show Day of Week, Show Time, 24 Hour Time - select or clear these check boxes to specify which labels appear on a chart's horizontal axis by default.

Default Interval - use the menu to select a default interval between timestamps on the X-axis (horizontal) of new charts. Shorter intervals show finer detail; longer intervals show a longer history.

NOTE: Because Intermapper saves all data points, there is no limit to the amount of memory needed to save a chart. Selecting a longer time interval does not save memory. All data points are saved.

Sub-Dividers - click the up and down arrows to specify the number of vertical sub-dividers to draw between data points.

Data Tab

You can use the Data tab of the Chart Defaults panel to specify line and data point styles.

The screenshot shows the 'Axes' tab of the 'Chart Defaults' panel. It is divided into two main sections: 'Vertical Axis' and 'Horizontal Axis'.
 In the 'Vertical Axis' section:
 - 'Upper Bounds' is a text input field containing '100'.
 - 'Lower Bounds' is a text input field containing '0'.
 - There is a checked checkbox for 'Auto-adjust'.
 - 'Dividers' is a spinner control set to '3'.
 - 'Sub-Dividers' is a spinner control set to '0'.
 In the 'Horizontal Axis' section:
 - There are four checkboxes: 'Show Date' (checked), 'Show Day of Week' (unchecked), 'Show Time' (checked), and '24 Hour Time' (checked).
 - 'Sub-Dividers' is a spinner control set to '0'.
 - 'Default Interval' is a dropdown menu currently showing '1 Minute'.


AxisDataColors

Data plots in new charts will have the following line styles and highlights.

Line Style: Highlight: None

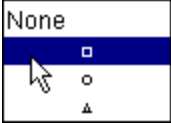
Style

Use the **Line Style** menu to specify a line thickness for the default line.



Highlight

Use the **Highlight** menu to select the icon to be drawn at the end of each line segment.



Colors Tab

You can use the Colors tab of the Chart Defaults panel to specify line and data point styles.

AxesDataColors

New Charts will have the following color scheme.

Exterior:

Interior:

Frame:

Text:

☒ Horizontal Dividers:

☐ Vertical Dividers:

Major Dividers:

To change a color:

Select a color. A color-selection window is displayed.

For more information on colors and how they are used, see the [Colors Tab \(Pg. 200\)](#) section of Chart Options.

Retention Policies

You can use the Retention Policies pane to create and edit retention policies that specify how data is stored for a device or map.

Data Retention Policies affect how much data is stored for charts and reports.

Unless otherwise specified, InterMapper will apply this Data Retention Policy to data when first added to a chart.

Data Retention Policy for new Charts: 24 Hours ▼

Name	Original	5 Min.	Hourly	Daily	Chart Data
24 Hours	1 Day	1 Day	1 Day	1 Day	Forever
autorecord	1 Day	1 Month	1 Week	355 Days	Forever
Chart Only	None	None	None	None	Forever
Critical Data	1 Day	2 Months	355 Days	Forever	Forever
Forever	Forever	Forever	Forever	Forever	Forever
IM46Charts	Forever	Forever	Forever	Forever	Forever
None	None	None	None	None	None
Server Default	1 Day	2 Weeks	6 Months	1,775 Days	Forever
SLA Data	1 Day	2 Months	6 Months	355 Days	Forever

Add - Delete - Edit

+ - ✎

Each row shows a Retention Policy and its setting for retaining Original, 5-minute, Hourly, and Daily data from devices, as well as data from charts.

Daily and maintenance operations require at least the same amount of free disk space as there is in the database itself, providing enough disk space is essential to prevent maintenance operations from hanging or failing.

Using the Retention Policies Pane

- **Default Retention Policy for new Charts** - the default policy.
- **Policy list** - the policy you want to delete or edit.
- **Add Policy** - adds a new policy. Click +.
- **Delete Policy** - the policy you want to delete. Click -.
- **Edit Policy** - the policy you want to edit. Click the Pencil tool.

Creating and Editing a Retention Policy

You can use data retention policies to consolidate raw data, reducing the amount of stored data. Data retention policies control how often and how much data is averaged and reduced.

A data retention policy can be applied to a specific map, to one or more devices or interfaces on a map, to an individual dataset, or to all maps on an Intermapper server. Policies also affect the way Intermapper stores chart data.

Creating Retention Policies

Use the Create Retention Policy window to define a new retention policy. The same window is used for editing an existing policy.

To create a retention policy:

1. Click the plus sign (+) to open the **Create Retention Policy** window.
2. In the Policy Name text box, type a name for the policy.
3. Specify how long you want to keep **original data**, **5-Minute**, **Hourly**, and **Daily** samples.
4. From the **Server Storage type** area, select one of the following:
 - **None** - data is polled, but is not saved for charting or exporting.
 - **Limited** - data is retained for the specified period. Enter a number and select **day**, **week**, **month**, or **year**.
Up to 24 hours of additional data can be retained until the next time data is purged.
 - **Forever** - all charted or exported values are saved to a local disk file.

To edit a retention policy:

1. From the **Retention Policies** pane, click the retention policy you want to edit.
2. Click the pencil tool. The Edit Policy window for the selected policy is displayed.

NOTE:

Daily and maintenance operations require at least the same amount of free disk space as large as the database itself, providing enough disk space is essential to prevent maintenance operations from hanging or failing.

NT Services and WMI

Intermapper can monitor and send notifications for NT Services running on another computer. Intermapper uses the Service Control Manager facilities of the underlying Microsoft Windows host to communicate with a remote computer to track the state of its services.

NOTE:

- You must be running the Intermapper server on a Microsoft Windows computer to use this capability.
- The Intermapper server computer must be able to log onto the target Microsoft Windows computer as a service. For more information, see [Authentication for NT Services Probe \(Pg. 593\)](#) in the topic Monitoring NT Services with the Windows NT Services Probe.
- If a command-line probe contains the NTCREDENTIALS flag, Intermapper runs the probe as the user specified here.

Use the NT Services panel of the Server Preferences section to set the User and Password for the machine. If you are running Intermapper server on a Microsoft Windows machine, Intermapper can build a list of services the machine is running.

Please enter the username and password of an account with Administrator privileges on the InterMapper machine.

Administrator privileges are necessary in order that the NT Services and WMI probes be able to establish connections to the target machines.

InterMapper is not currently running under an administrator account; it will use the username and password you supply to elevate its privileges each time it needs to poll an NT Services or WMI device.

User:

Password:

Server Configuration Panels

Intermapper provides three built-in servers you can use to view and retrieve information about the status of the network from remote computers. Each server's built-in firewall must

be configured before it can be used. By default, each server's firewall is set up so access is denied.

You can use the Server Configuration panels of the Server Settings window to view and edit settings for the built-in servers, to manage users and groups, to control map access, and to manage a list of [notifiers/alerts \(Pg. 108\)](#).

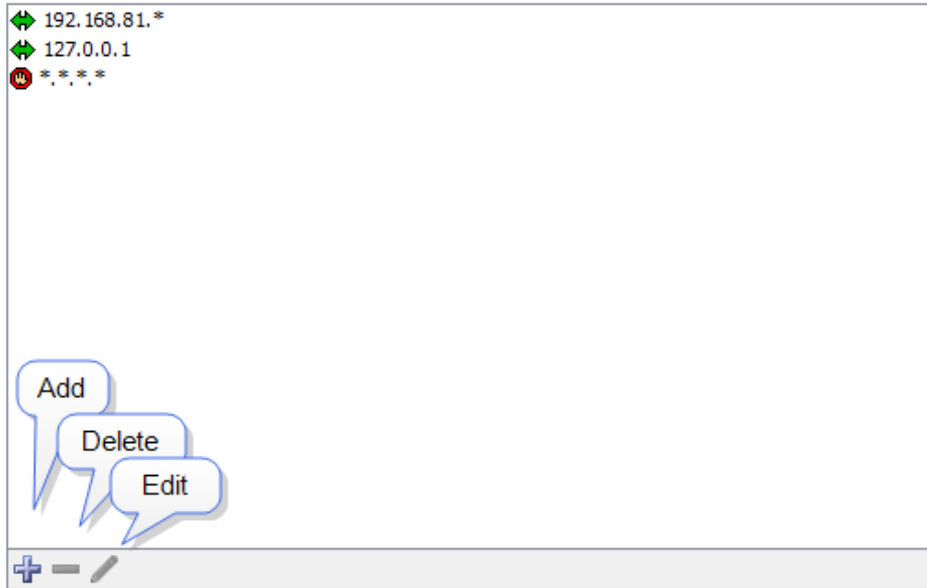
From the left pane of the Server Settings window, you can view and edit the following settings:

- [Remote Server \(Pg. 253\)](#) - start, stop, or edit the Intermapper remote access server settings.
- [Reports Server \(Pg. 255\)](#) - start, stop, or edit the Intermapper reports server settings.
- [Web Server \(Pg. 258\)](#) - start, stop, or edit the Intermapper Web server settings.
- [Telnet Server \(Pg. 260\)](#) - Start, stop, or edit the Intermapper Telnet server settings.
- [Layer 2 \(Pg. 263\)](#) - Turn on and configure Layer 2 scanning for your server.
- [Enabled Maps \(Pg. 264\)](#) - view a list of available maps, enable or disable maps, and import or export maps.
- [Users \(Pg. 272\)](#) - view, add, and edit users and groups, and control access for users and groups.
- [Map Access \(Pg. 279\)](#) - control access for any user or group to any map through the web server or remote server.
- [Map Backup](#) - enable automatic map backups and create a schedule for backing them up.
- [Notifier List \(Pg. 282\)](#) - view, add, copy, edit, and remove notifiers.
- [SSL Certificate \(Pg. 283\)](#) - create new Certificate Signing Requests (CSR) and upload new certificates to the Intermapper server.
- [AWS EC2 Credentials \(Pg. 291\)](#) - add, edit, and delete existing Amazon AWS EC2 instances in the Server Settings.

For more information on configuring your servers, see [Server Access Control \(Pg. 252\)](#). This explains how to set a server port, discusses encryption and when to use it, and describes how to configure a server's built-in firewall's list of IP addresses.

Configuring a Firewall

For each built-in server, the Firewall list shows all addresses that are allowed or blocked.



- If an incoming address matches an Allow address (or range), the connection is allowed.
- If the incoming address matches a Deny address, the connection is denied.
- Firewall definitions are checked against the incoming address in the order in which they appear.

Changing Firewall Definition Order

Firewall definitions are applied in the order in which they appear. You can change the order of the definitions after you create them.

To move a firewall definition to a different position in the list:

Click and drag the firewall definition to the new position.

Entering Addresses and Ranges

You can enter addresses in the access control list or you can enter address ranges. For more information, see [Entering an IP Address Range](#).

Tip: To deny access to certain addresses, add them at the top of the list and set the **Access** attribute to **Deny**.

For a description of the Access Control process and the rules Intermapper uses to determine whether a user should be allowed to connect to an Intermapper server, see [Controlling Access to Your Server](#).

Controlling Access to Your Server

You can configure the firewalls of Intermapper's built-in servers to accept or deny connections from a client based on its IP address. You can also require a user name and password. After these are accepted, a connection is associated with the user name that determines which maps and permissions are available. For examples of typical access control setups, see [Access Control Examples \(Pg. 277\)](#).

NOTE:

- You can also control access through the [Intermapper Authentication Server \(Pg. 613\)](#), which connects to an external authentication server such as Radius, LDAP, or ActiveDirectory to authenticate a user. For more information, see [Authentication Server \(Pg. 613\)](#).
- Any firewall that is protecting the machine that is running Intermapper must be configured to allow access to the ports specified for remote access. This includes the port specified for use by the web server.

Access Control

When a user attempts to connect to one of the Intermapper servers, the request goes through the following steps:

1. **The client's IP address is checked against the list of firewall definitions.** If the address matches a DENY address in the firewall list, or if the address fails to match an ALLOW address, the connection is dropped with a not allowed response.
2. **The client's IP address is checked against the list of Automatic Login addresses.** If the client's IP address matches an Automatic Login address, the connection is accepted and is assigned the user name associated with that Automatic Login.
3. If the client's IP address does not match an Automatic Login address, the connection is accepted and authentication by a username and password begins, as follows:
 - a. **Web server** - issues a 401 Unauthorized response, which forces the web browser to request a username/password from the user.
 - b. **Telnet server** - prompts for a username and password.
 - c. **Remote server** - proceeds after the Intermapper RemoteAccess client requests and supplies a username and password.
4. **The username and password are verified against Intermapper's built-in authentication database.** If they match, the connection is assigned the user name. Otherwise, the connection is dropped with a not allowed response. When using the Remote and Telnet servers, an error message is displayed, saying that the user name

is not allowed. When using the Web server, a web page is displayed, saying that the user is not allowed access.

5. **The users are checked for membership in a Special Group.** The following special groups provide broader access:

- **Administrators Group**

If the user is a member of the Administrators group, the connection is granted full (read/write) access to every map and setting.

- **FullWebAccess Group**

If you created a group named FullWebAccess, all members of that group are granted full access to all maps through the web server. As with all web access rights, this is a read-only view. This membership also overrides any individual map access settings. FullWebAccess members can also acknowledge down devices.

- **FullTelnetAccess Group**

If you created a group named FullTelnetAccess, all members of that group are granted full access to the Telnet server.

- **FullLogAccess Group**

If you created a group named FullLogAccess, all members of that group are granted full access to all log files.

6. **The user is granted access to maps.** After a connection has a user name associated with it, Intermapper checks to see which information is available for that user. Access to individual maps can be granted using the Map Access server setting (see [Map Access \(Pg. 279\)](#)).

If a user is not in the Administrators, FullWebAccess, or FullTelnetAccess group and has no access to an individual map, the connection is dropped with a not allowed response.

Remote Server

Intermapper's remote server allows you to configure and edit maps on an Intermapper installation from a remote computer. To allow these changes, the remote server accepts connections from the Intermapper or Intermapper RemoteAccess application, running on a different computer.

Intermapper always listens for remote connections on its localhost interface (127.0.0.1). This allows you to run a copy of the Intermapper RemoteAccess application on the machine that is running Intermapper. For security, Intermapper refuses all remote server connections from non-localhost addresses by default to prevent unauthorized configuration.

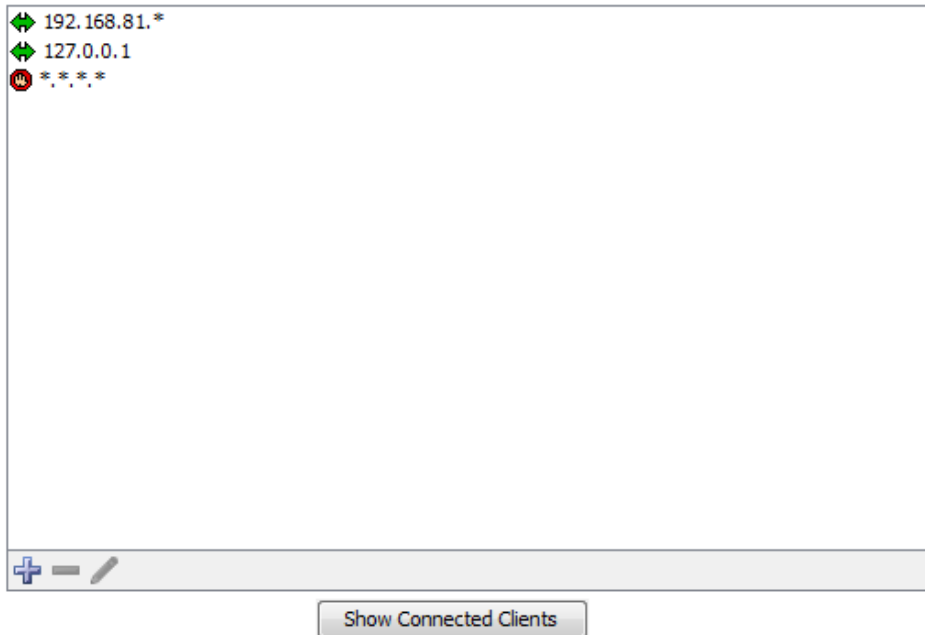
You can configure Intermapper to accept connections from remote computers, providing varying degrees of access by IP address or by username and password.

Unlike the Telnet and web servers, you cannot start or stop the remote server. You configure the remote server using the Remote Server settings panel of the Server Configuration section, found in the Server Settings window.

Remote Server Listening On Port 8181 [Secure]

Listen for connections on TCP port:

Access Control List to Remote Server based on IP Address:



192.168.81.*

127.0.0.1

..*.*

+ - ✎

Show Connected Clients

Send log file entries to:

To configure the Remote Server:

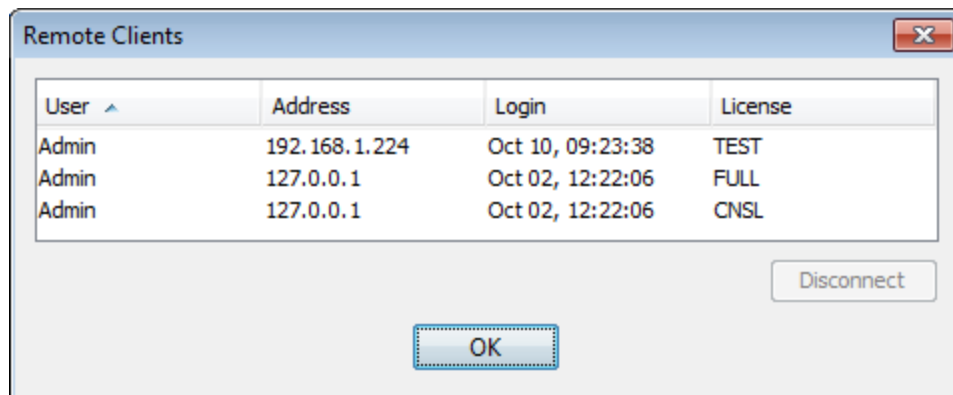
1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
2. From the **Server Configuration** section, click **Remote Server**. The Remote Server panel is displayed.
3. From the Remote Server panel, do the following:
 - Enter a TCP port number, or use the default value.
 - To configure access to the remote server, click the plus sign (+) to add addresses to the remote server firewall.
 - To remove an entry, click the entry and click the minus sign (-).
 - To edit an entry, click then entry and click the encil tool.
 - To see a list of clients connected to the server, click **Show Connected Clients**.

- To send entries from this server to a different log file, select a log file from the **Send log file entries to** menu. For more information on log files, see [Log Files \(Pg. 231\)](#).

NOTE: The Server Settings window is available only to users who have administrator privileges.

Showing Connected Clients

Click Show Connected Clients to view a list of Intermapper clients connected to the server. The Remote Clients window is displayed, showing the connected user's name, IP address, time of login, and type of license.



Additional Information

For more information on configuring your remote server, see [Server Access Control \(Pg. 252\)](#). It describes how to set your remote server's port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses.

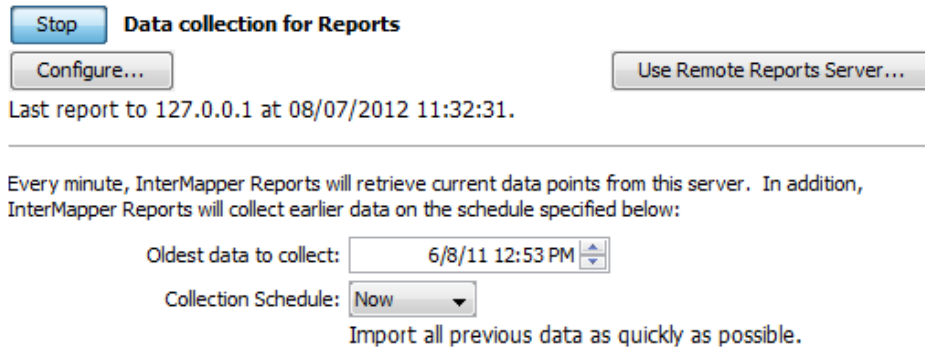
For more information on configuring your built-in servers' firewalls, see [Configuring a Firewall \(Pg. 250\)](#).

For more information on users and groups, see [Users and Groups \(Pg. 272\)](#). It describes how to set up users and groups and how to specify who may use the remote server. It also discusses administrator access to the remote server.

For more information on setting permissions for a particular map, see [Controlling Access to a Map \(Pg. 279\)](#). It describes how to set up unique access controls (by username) for an individual map.

Reports Server

The reports server stores data in a database for use in reports. Use the Reports Server panel, available from the Server Configuration section of the Server Settings panel, to specify the amount of data you want to store in the database.



Stop **Data collection for Reports**

Configure... **Use Remote Reports Server...**

Last report to 127.0.0.1 at 08/07/2012 11:32:31.

Every minute, InterMapper Reports will retrieve current data points from this server. In addition, InterMapper Reports will collect earlier data on the schedule specified below:

Oldest data to collect: 6/8/11 12:53 PM

Collection Schedule: Now

Import all previous data as quickly as possible.

Setting up the Reports Server

If InterMapper DataCenter is running on the same host machine as InterMapper server, the reports server is automatically configured and you can start collecting data as soon as you start it.

If InterMapper DataCenter is installed on another host machine, you need to configure InterMapper to use that server.

To open InterMapper DataCenter and configure the reports server:

Click **Configure**. For more about configuring the reports server, see [Configuring InterMapper DataCenter](#) for more information.

Starting Data Collection

You can start and stop data collection on the reports server.

To start or stop collecting InterMapper data:

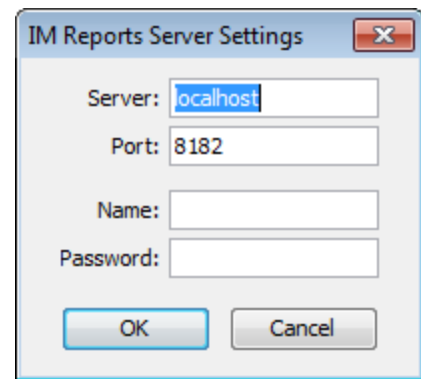
- Click **Start (Data collection for Reports)**.
- Click **Stop**.

Specifying an InterMapper Reports Server Connection

If Intermapper DataCenter is running on a different host than the Intermapper server, you must specify the server, port, and an account login for the database you want Intermapper to use.

To configure the Intermapper Reports Server connection:

From the **Reports Server** panel of the **Server Settings** window, click **Use Remote Reports Server** and enter the information in the Intermapper Reports Server Settings window as shown.



Collecting Current Data

Every minute, the Intermapper reports server sends a request for a certain number of rows of current data to insert into the database. The request contains a start and end time, where the start time is the oldest data desired, and the end time is the newest (generally, the present time).

The response from Intermapper server contains the rows to insert into the database, as well as the time of the next row to request. Intermapper reports server uses this information to update its notion of the current time, and the subsequent requests use that time.

The number of rows in the request is automatically adjusted so that the insertion process uses approximately half of the (one minute) time interval. Typically, 500 rows are requested for events and 25,000 rows are requested for data points.

If the time of the next row in the response is less than the requested end time, Intermapper reports server can tell that there is more data available.

Collecting Pre-Existing Data

In parallel, the Intermapper reports server retrieves historical data by working backwards (from newest to oldest), requesting data from the Intermapper server. It does this by making requests for a set of data rows older than a particular time.

The Intermapper server responds with those rows and the Intermapper reports server inserts them and updates the time of the next (oldest) row. Subsequent requests start at this time and retrieve still older data rows.

Select one of the following in the Collection Profile menu to specify the rate at which Intermapper reports server requests the historical data:

- **Now** - attempts to retrieve the historical data as fast as possible. It uses most of the remainder of the one-minute time interval (the time left after retrieving the current data) to request historical data. The Intermapper reports server adjusts the number

of rows in its request so that it finishes inserting in time to start the next current data request.

- **Gradually** - retrieves historical data between every other polls for current data.
- **Nightly** - only retrieves historical data between the hours of 01:00 and 03:00. During this time period, it uses the Now profile.
- **Weekend** - retrieves historical data between the hours of 01:00 and 23:00 on Saturday and Sunday. During this time period, it uses the Now profile.
- **Never** - never retrieves historical data.

What Data is Collected?

Certain variables for probes are recorded automatically when data is collected from a device by Intermapper reports server. You can also specify other variables you want to record when data for a device is stored.

For all probes, the following data is recorded:

- response time (in msec)
- long-term packet loss (%)
- input byte rates for all visible interfaces.
- output byte rates for all visible interfaces.

For built-in probes, Fortra selected default values that make sense to record for each probe.

For custom probes, you can specify which variables is recorded. The syntax for this is described in Recording Probe Data in the Developer Guide.

Web Server

Intermapper can act as a web server, publishing most of the information available from the Intermapper application.

NOTE: Before Intermapper allows web connections, you must configure the web preferences as described in [Configuring a Firewall](#). You must also make sure that any other firewall protecting the Intermapper machine allow traffic to the port specified below.

You start, stop, and configure the web server from the Web Server panel in the Server Configuration section of the Server Settings window.

Web Server Listening On Port 443 [Secure]
Default Refresh: 1 Minute ▼

URL: <https://10.4.1.120:443>

Listen for connections on TCP port:

☒ Use a secure protocol (SSLv3/TLS)

Access Control List to Web Server based on IP Address:

↔ 10.4.1.*
↔ 10.4.3.*

+ - ✎

Send log file entries to:

NOTE: When configuring the Intermapper web server on a machine where IIS is also installed, do not use the default port 80. IIS uses port 80 by default and this prevents the Intermapper web server from starting.

To start, stop, or configure the web server:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
2. From the **Server Configuration** section, click **Web Server**. The Web Server panel is displayed.
 - Click **Start** to start the web server.
 - Click **Stop** to stop the web server when it is running.
 - Enter a TCP port number or use the default value.
 - Select the **Use a secure protocol (SSLv3/TLS)** check box to use a secure protocol.
 - Click **Add** to add addresses to the web server firewall. For more information on configuring firewalls, see [Configuring a Firewall \(Pg. 250\)](#).
 - From the **Send log file entries to** menu, select a log file to which you want to send log entries.

NOTE: The Server Settings window is available only to users who have administrator privileges.

For more information on configuring your web server, see [Server Access Control \(Pg. 252\)](#). It describes how to set your web server port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses.

For more information on users and groups, see [Users and Groups \(Pg. 272\)](#). It describes how to set up users and groups and how you specify who may use the web server. It also discusses administrator access to the web server.

For more information on setting permissions for a particular map, see [Controlling Access to a Map \(Pg. 279\)](#). It describes how to set up unique access controls (by username) for an individual map.

Connecting to the Web Server

After you start the web server, a URL is displayed below the Stop button. Click the URL or enter the URL in a web browser. If the web server is configured correctly, the Intermapper Web Server's home page is displayed in your browser window.

Setting the Default Refresh Interval

You can use the Default Refresh menu, located in the upper-right corner of the Web Server Settings pane to set the refresh rate that a web page uses by default.

- When you change the value on a web page, the new value is remembered for that page.
- Each web page has its own value.
- The value is remembered for the page even if you navigate to it with a link.
- The value is remembered for the page if a link opens it in a new tab or window.

Telnet Server

Intermapper provides a Telnet service that provides basic information about monitored devices as well as detailed information about the Intermapper server itself. Before Intermapper accepts Telnet connections, you must configure the Telnet server firewall preferences as described in [Configuring a Firewall \(Pg. 250\)](#).

You start, stop, and configure the firewall for the Telnet server from the Telnet Server settings panel in the Server Configuration section of the Server Settings window.

Telnet Server Off

URL: *inactive*

Listen for connections on TCP port:

Access Control List to Telnet Server based on IP Address:

➡
192.168.1.*

⛔
,,*

+
-
✎

To start, stop, or configure the Telnet server:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
2. From the **Server Configuration** section, click **Telnet Server**. The Telnet Server panel is displayed.
 - Click **Start** to start the Telnet server.
 - Click **Stop** to stop the Telnet server when it is running.
 - Enter a TCP port number or use the default value.
 - Click **Add** to add addresses to the Telnet server firewall.

NOTE: The Server Settings window is available only to users with administrator privileges.

For more information on configuring your Telnet server, see [Server Access Control \(Pg. 252\)](#). It describes how to set your Telnet server port, discusses encryption and when to use it, and describes how to configure the built-in firewall's list of IP addresses. You can also see a variety of options for specifying IP address in [Entering an IP Address Range](#).

For more information on users and groups, see [Users and Groups \(Pg. 272\)](#). It describes how to set up users and groups and how you specify who can use the Telnet server. It also discusses administrator access to the Telnet server.

AutoMate

You can use the AutoMate pane of the Server Settings window to enable and configure a connection to a local version of the AutoMate application.

AutoMate System

Version:

Name: ☒ Enabled

Host: Port:

Password:

Polling Interval:

Server System Tasks

	Event	Task	
<input type="checkbox"/>	Server startup		⬆
<input type="checkbox"/>	Log file rotation		
<input type="checkbox"/>	Map backup comp...		⬇

To enable and configure a connection to a local version of the AutoMate application:

Specify the following:

- **Version** - the version of the selected AutoMate server.
- **Name** -the name of the selected AutoMate server.
- **Enabled** - allowd Intermapper to request execution of AutoMate tasks on behalf of Intermapper's AutoMate notifiers to trigger AutoMate and Server System tasks.
- **Host** - the host of the AutoMate server. The AutoMate server must be running on the same machine as Intermapper server.
- **Port** - the port to use to connect to the AutoMate server.

- **Password** - the default task password, if one is not supplied during task selection.
- **Polling Interval** - the number of seconds to use when polling the AutoMate server to check the status of a task. When set to 0, the polling interval increases over the length of time the task has been running.
- **Server System Tasks** - server system events you want to run as AutoMate tasks. These include Intermappers system startup, completion of a scheduled map backup, and log file rotation.

Using Layer 2

You can use the Layer 2 panel to enable and configure Layer 2 scanning.

NOTE: The Layer 2 features are experimental.

Use Layer 2 scanning to collect information about how your Ethernet switches are connected. Intermapper uses this information to produce more complete and accurate maps. This feature is experimental. It may not work for some switches.

☒ Enable Layer 2 scanning on this server

Layer 2 Settings

Maps with Layer 2 Scanning Enabled: 4

Select Maps for Layer 2 Scan

☒ Enable Layer 2 Scan on ALL new maps.

Depending on the number of maps and the number of devices on your network, this option could overwhelm the Intermapper server.

☒ **Collect all device information**

Use switch forwarding tables along with CDP, LLDP, and other SNMP information to find connections between switches. On large networks, this may cause high CPU utilization on your switches and routers while a Layer 2 scan is in process. Use this option sparingly until you have determined how your devices respond.

☐ **Collect device information using only CDP and LLDP**

Use CDP and LLDP to determine the connections between switches. This may result in maps that don't include switches where CDP or LLDP is not enabled. This option only discovers switches and their connections.

Collect detailed information from SNMP devices on specific maps and use the information to calculate the Layer 2 topology of the network:

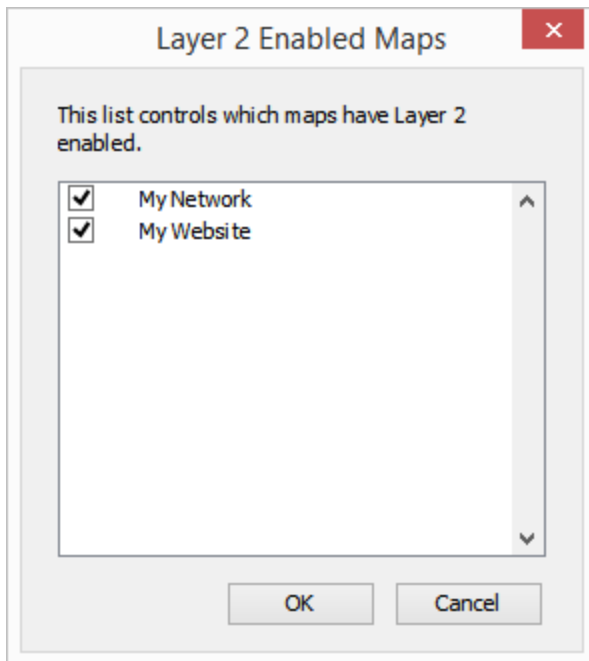
Once a Day Scan Not running - last updated: Never

Every day at 00:00

To enable and configure Layer 2 scanning using the Layer 2 panel:

Specify the following:

- **Enable Layer 2 scanning on this server** - makes Layer 2 scanning available.
- **Maps with Layer 2 Scan Enabled** - the number of maps enabled for Layer 2 scanning.
- **Select Maps for Layer 2 Scan** - the maps for which Layer 2 is enabled. The Layer 2-Enabled Maps window is displayed.



NOTE: After you enable Layer 2 on a map, use the [Map Settings window](#) to configure scanning for each enabled map.

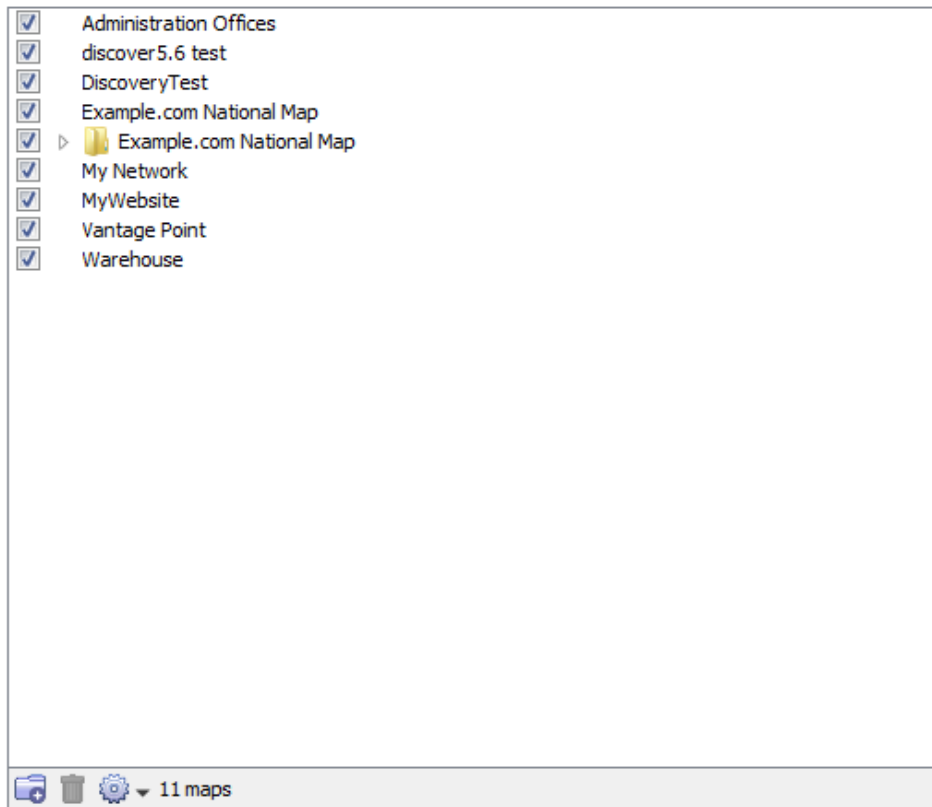
- **Enable Layer 2 Scan on ALL new maps** - select this option to automatically enable new maps for Layer 2 scanning.
- **Collect all device information** - select this option to collect detailed information from SNMP devices. This can add a significant CPU load on your switches and routers during scanning.
- **Collect information using only CDP and LLDP** - select this option to request only CDP and LLDP information from Layer 2 devices. This option reduces the CPU load on your switches during scanning. Collection is limited only to switches, but results might not include switches for which CDP or LLDP is not enabled.
- **Schedule scan** - specifies how often to start a scan. Select **Manually** to collect Layer 2 information only when you choose.
- **Scan** - immediately performs a Layer 2 scan.

Enabled Maps

You can use the Enabled Maps panel of the Server Settings window to enable and disable maps, to remove maps, to organize maps into folders, and to import and export them.

Select a check box to enable a map; clear the box to disable it.

Use the tools below to create folders, or to delete or perform other operations on selected maps. Drag maps into or out of folders.



- **Checked maps** - active maps. Intermapper actively polls everything on the map.
- **Unchecked maps** - inactive maps. Intermapper does not poll the devices on those maps.

The Enabled Maps panel lists available maps and shows which maps are enabled. From the Enabled Maps panel, you can do the following:

- **Enable or Disable a map.** Select the check box to the left of a map in the list to enable or disable it.
- **Import a map.** Click **Import** to import data into Intermapper.
- **Export a map.** Click **Export** to save the current map as an Intermapper map file on your local machine.
- **Duplicate a map.** Select a map and click **Duplicate** to create a copy of it.
- **Remove a map.** Select a map and click **Remove**. A confirmation window appears.

NOTE: When you remove a map, it is placed in the Maps (Deleted) folder.

- **Create a new Folder.** Click a map at the level you want to create the folder and click **New Folder**.

Organizing Maps into Folders

From the Enabled Maps panel, you can create folders and use them to organize your maps. This organization is displayed in the Map List window.

To organize maps into folders:

1. To create a folder, do one of the following:
 - Click any map at the top level and click **New Folder** to create a folder in the top level of the map list. A folder is created and named Untitled.
 - Click the folder where you want to create a new folder to create a folder within a folder.
2. Type a name for the new folder and press **Enter** on your keyboard. The folder name changes to the specified name it moves to the correct alphabetic location in the list.
3. Drag maps into the folder.

NOTE: When you create a folder with the same name as a map at the same hierarchical level, a folder is displayed. After the folder is created, you can open the map by double-clicking the associated folder in the Map List window.

Map File Locations

Maps are stored in the following locations:

- Enabled maps are stored in the InterMapper Settings/Maps/<version>/Enabled folder.
- Disabled maps are stored in the InterMapper Settings/Maps/<version>/Disabled folder.
- When you delete a map, it is not discarded. Instead, it is placed in the InterMapper Settings/Maps/Deleted folder.

NOTE: Even though you can place maps in the Maps folder using the file system, this is not recommended. If the server is running when you place the files in the folder, the maps are ignored and an error is logged when you go to the Server Configuration > Enabled Maps panel of the Server Settings window. Use the Enabled Maps panel's Import Map button to add maps to the Maps folder.

Users and Groups

You can use the Users panel of the Server Settings window to [add \(Pg. 268\)](#) and [edit \(Pg. 270\)](#) users and [groups \(Pg. 270\)](#), to [assign users to groups \(Pg. 270\)](#), and to assign privileges and access to maps.

NOTE: The Server Settings window is available only for users with administration privileges.

Users Panel

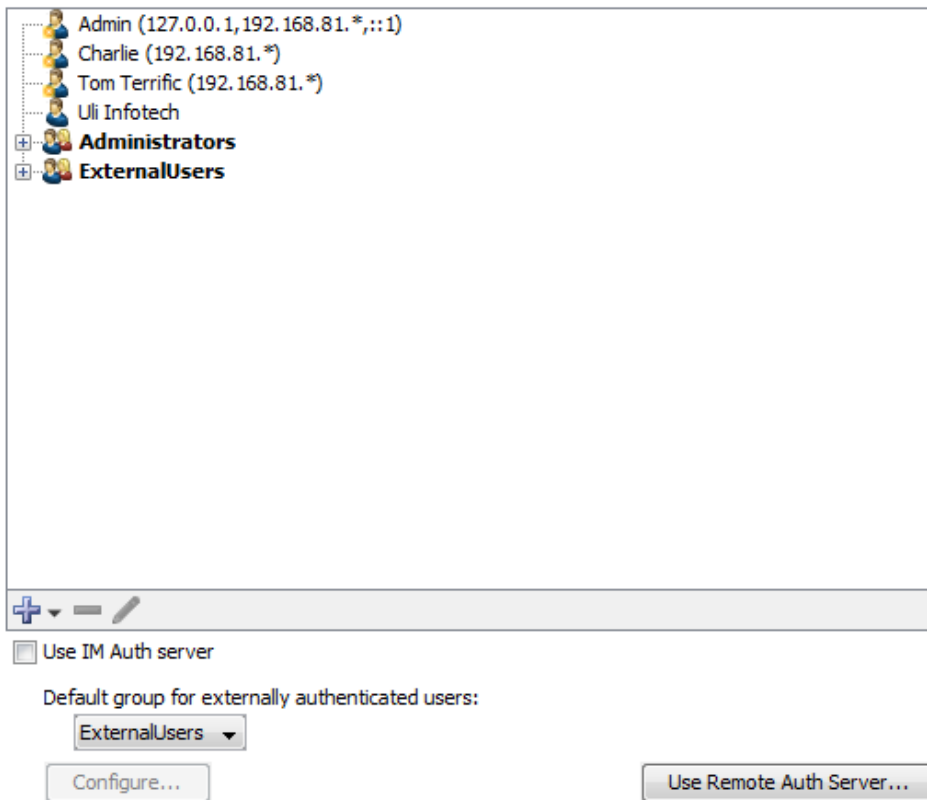
To maintain the list of users and groups allowed to access the various servers:

Do any of the following:

- Click **New User** to add a user.
- Click **New Group** to add a group.
- Select the user or group and click **Remove** to remove a user or group.
- Select the user or group and click **Edit** to edit a user or group's information.
- Select the **Use IMAuth Server** check box to use the [Intermapper Authentication server](#).
- Click **Configure** to open the [Intermapper DataCenter](#) to set up the IMAuth Server.
- Click **Use Remote Auth Server** to use an Authentication Server on another computer.
- Select a **Default group for externally authenticated users** from the menu.

The following example shows a typical user and group configuration in the Users panel of the Server Settings window:

This list shows the users and groups on the server.
Drag a user to a group to add it.



The screenshot shows a window titled "Server Settings" with a tab labeled "Users". Inside, there is a list of users and groups on the left side of a large empty box. The list includes:

- Admin (127.0.0.1, 192.168.81.*, ::1)
- Charlie (192.168.81.*)
- Tom Terrific (192.168.81.*)
- Uli Infotech
- Administrators**
- ExternalUsers**

Below the list is a toolbar with a plus sign (+), a minus sign (-), and an eraser icon. Underneath the toolbar is a checkbox labeled "Use IM Auth server". Below that is a label "Default group for externally authenticated users:" followed by a dropdown menu currently showing "ExternalUsers". At the bottom left is a "Configure..." button, and at the bottom right is a "Use Remote Auth Server..." button.

What Are Users and Groups?

- **User**

An individual identified by a user name and password or identified automatically from a client IP address or range.

- **Group**

A collection of users. Groups can be granted permissions to access certain servers or maps and can be granted different levels of access for a server or map.

Creating a New User

To create a new user:

1. Click the plus sign **+** and select **Add User**. The User Information dialog is displayed.
2. In the **Name** and **Password** text boxes, do one of the following:

- Type the name and password for the new user.
- In the **Automatic Login** text box, omit the password and enter an IP address range.
- Select the **Use External Authentication** check box and type the username used by the external authentication server. No password is necessary; authentication is performed by the external authentication server.


How Automatic Login Works


- If a connection arrives from an address that matches an Automatic Login address, the person is automatically logged in as the specified user.
- If you supply both the password and automatic login address, the person is logged in automatically from the specified address, but must supply a password when connecting from other addresses.
- Automatic login addresses should be unique between users. The resulting login name is not guaranteed if two automatic-login addresses are the same.
- For more information see [Controlling Access To Your Server \(Pg. 252\)](#).

Edit User

Name:

☒ Change password (current password required)

New Password: 
Enter new password

Current Password: 
Enter current password

☐ Use External Authentication

Automatic Login:
Clients from this IP address range will be automatically identified as this user without checking their password:

Users in Intermapper need to have passwords that meet the following requirements:

- The passwords are at least 12 characters in length (after multiple spaces are combined).
- The passwords can not be longer than 128 characters.
- The passwords can be changed. If the user has a password already, the current password is required to change the password.
- Spaces can not be at the beginning or end of the password.
- By clicking the lock icon, the user can choose to either temporarily display the password as plain text or masked text.

Editing User Information

To edit the information about a user:

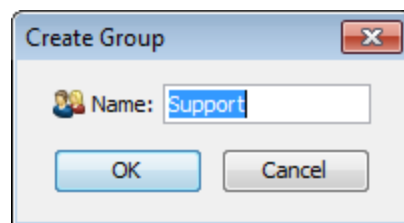
1. From the user list, select the user you want to edit.
2. Click **Edit** or double-click the user. The User Information dialog is displayed, containing information about the selected user.

Managing Users and Groups

A group is a collection of users, all of whom have the same set of permissions.

To create a new group:

1. Click the plus sign **+** and select **Add Group**. The Group Information dialog is displayed.
2. In the **Name** text box, type the name of the new group.
3. Click **OK**. The new group is displayed in the User list.



Adding and Removing Group Members

To view the users in a group:

Click the plus sign (+) to the left of the group to expand it.

To add a user to a group:

Click and drag the user's entry to the group entry. The user is displayed in the list of users for that group.

To remove a user from a group:

1. Expand the group list to view the users in the group.
2. Click the user you want to remove and click **Remove**. A confirmation dialog is displayed.
3. Click **OK**. The user is removed from the group.

NOTE: When you remove a user from a group, the user definition is removed only from the group, not from the user list. For information on removing a user completely from the list and all groups, see [Removing Users and Groups \(Pg. 271\)](#).

Removing Users and Groups

To delete a user or group completely:

1. Select the user you want to remove.
2. Click **Remove**. A confirmation dialog is displayed.
3. Click **OK** to confirm. The user or group entry is removed from the list.

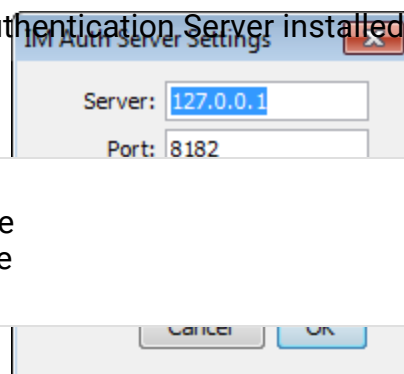
NOTE:

- The **Administrators** group is always present and cannot be removed.
- The **FullWebAccess** group is defined by you. If present, its members can view all web pages and can acknowledge devices through the web server.
- The **FullLogAccess** group is defined by you. If present, its members can view all log files.
- The **FullTelnetAccess** group is defined by you. If present, its members have full access to the Telnet server.

Configuring the Intermapper Authentication Server

Click **Use Remote Auth Server** to connect to an Intermapper Authentication Server installed on a different machine from Intermapper. For more information, see [Authentication Server \(Pg. 613\)](#).

NOTE: If the Intermapper Authentication Server is installed on the same machine as Intermapper, you need only to select the Use IM Auth Server check box. The default server and port are used and there is no need to enter a name or password.



Importing Users and Groups

Click Import to upload a file containing data for users and groups. For information on importing data, see [Importing Data \(Pg. 631\)](#). For information on the user and group data structure, see [User Attributes \(Pg. 672\)](#).

Users and Groups

You can use the Users panel of the Server Settings window to [add \(Pg. 273\)](#) and [edit \(Pg. 275\)](#) users and [groups \(Pg. 275\)](#), to [assign users to groups \(Pg. 275\)](#), and to assign privileges and access to maps.

NOTE: The Server Settings window is available only for users with administration privileges.

Users Panel

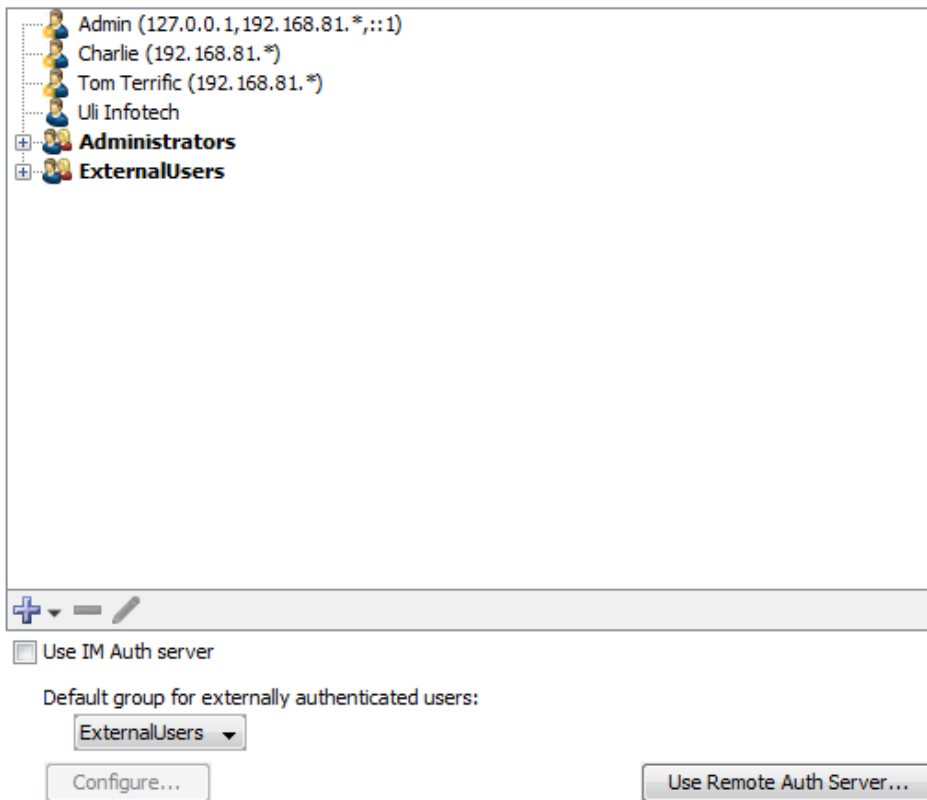
To maintain the list of users and groups allowed to access the various servers:

Do any of the following:

- Click **New User** to add a user.
- Click **New Group** to add a group.
- Select the user or group and click **Remove** to remove a user or group.
- Select the user or group and click **Edit** to edit a user or group's information.
- Select the **Use IMAuth Server** check box to use the [Intermapper Authentication server](#).
- Click **Configure** to open the [Intermapper DataCenter](#) to set up the IMAuth Server.
- Click **Use Remote Auth Server** to use an Authentication Server on another computer.
- Select a **Default group for externally authenticated users** from the menu.

The following example shows a typical user and group configuration in the Users panel of the Server Settings window:

This list shows the users and groups on the server.
Drag a user to a group to add it.



The screenshot shows a window titled "Server Settings" with a tab labeled "Users". Inside the window, there is a list of users and groups on the left side, each preceded by a small icon of a person. The list includes:

- Admin (127.0.0.1, 192.168.81.*;::1)
- Charlie (192.168.81.*)
- Tom Terrific (192.168.81.*)
- Uli Infotech
- Administrators**
- ExternalUsers**

Below the list, there is a toolbar with a plus sign (+), a minus sign (-), and an eraser icon. Underneath the toolbar, there is a checkbox labeled "Use IM Auth server". Below that, there is a label "Default group for externally authenticated users:" followed by a dropdown menu currently showing "ExternalUsers". To the right of the dropdown is a "Configure..." button. At the bottom right of the window is a button labeled "Use Remote Auth Server...".

What Are Users and Groups?

- **User**

An individual identified by a user name and password or identified automatically from a client IP address or range.

- **Group**

A collection of users. Groups can be granted permissions to access certain servers or maps and can be granted different levels of access for a server or map.

Creating a New User

To create a new user:

1. Click the plus sign **+** and select **Add User**. The User Information dialog is displayed.
2. In the **Name** and **Password** text boxes, do one of the following:

- Type the name and password for the new user.
- In the **Automatic Login** text box, omit the password and enter an IP address range.
- Select the **Use External Authentication** check box and type the username used by the external authentication server. No password is necessary; authentication is performed by the external authentication server.

How Automatic Login Works

- If a connection arrives from an address that matches an Automatic Login address, the person is automatically logged in as the specified user.
- If you supply both the password and automatic login address, the person is logged in automatically from the specified address, but must supply a password when connecting from other addresses.
- Automatic login addresses should be unique between users. The resulting login name is not guaranteed if two automatic-login addresses are the same.
- For more information see [Controlling Access To Your Server \(Pg. 252\)](#).

Edit User

Name:

☒ Change password (current password required)

New Password:

Enter new password

Current Password:

Enter current password

☐ Use External Authentication

Automatic Login:

Clients from this IP address range will be automatically identified as this user without checking their password:

OK Cancel

Users in Intermapper need to have passwords that meet the following requirements:

- The passwords are at least 12 characters in length (after multiple spaces are combined).
- The passwords can not be longer than 128 characters.
- The passwords can be changed. If the user has a password already, the current password is required to change the password.
- Spaces can not be at the beginning or end of the password.
- By clicking the lock icon, the user can choose to either temporarily display the password as plain text or masked text.

Editing User Information

To edit the information about a user:

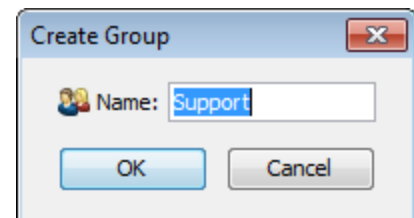
1. From the user list, select the user you want to edit.
2. Click **Edit** or double-click the user. The User Information dialog is displayed, containing information about the selected user.

Managing Users and Groups

A group is a collection of users, all of whom have the same set of permissions.

To create a new group:

1. Click the plus sign **+** and select **Add Group**. The Group Information dialog is displayed.
2. In the **Name** text box, type the name of the new group.
3. Click **OK**. The new group is displayed in the User list.



Adding and Removing Group Members

To view the users in a group:

Click the plus sign (+) to the left of the group to expand it.

To add a user to a group:

Click and drag the user's entry to the group entry. The user is displayed in the list of users for that group.

To remove a user from a group:

1. Expand the group list to view the users in the group.
2. Click the user you want to remove and click **Remove**. A confirmation dialog is displayed.
3. Click **OK**. The user is removed from the group.

NOTE: When you remove a user from a group, the user definition is removed only from the group, not from the user list. For information on removing a user completely from the list and all groups, see [Removing Users and Groups \(Pg. 276\)](#).

Removing Users and Groups

To delete a user or group completely:

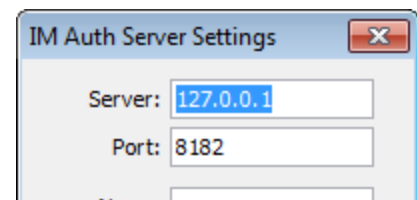
1. Select the user you want to remove.
2. Click **Remove**. A confirmation dialog is displayed.
3. Click **OK** to confirm. The user or group entry is removed from the list.

NOTE:

- The **Administrators** group is always present and cannot be removed.
- The **FullWebAccess** group is defined by you. If present, its members can view all web pages and can acknowledge devices through the web server.
- The **FullLogAccess** group is defined by you. If present, its members can view all log files.
- The **FullTelnetAccess** group is defined by you. If present, its members have full access to the Telnet server.

Configuring the Intermapper Authentication Server

Click **Use Remote Auth Server** to connect to an Intermapper Authentication Server installed on a different machine from Intermapper. For more information, see [Authentication Server \(Pg. 613\)](#).



NOTE: If the Intermapper Authentication Server is installed on the same machine as Intermapper, you need only to select the Use IM Auth Server check box. The default server and port are used and there is no need to enter a name or password.

Importing Users and Groups

Click Import to upload a file containing data for users and groups. For information on importing data, see [Importing Data \(Pg. 631\)](#). For information on the user and group data structure, see [User Attributes \(Pg. 672\)](#).

Access Control Examples

The following are typical access control configurations that might be used in different settings:

To allow connections from anywhere (no authentication):

1. From the **Server Settings** window, click a server (Remote Server, Web Server, or Telnet Server). A list of firewall entries is displayed in the right pane.
2. Add a firewall definition and set it to Allow *.*.*.*.
3. From the [Users panel \(Pg. 272\)](#), create a guest account with an Automatic Login address of *.*.*.*.

NOTE:

- This is a very open setting. Be sure that you actually intend to allow anyone to connect. This configuration might be reasonable if Intermapper is running behind a firewall and thus not visible outside your organization.
- The IP wildcard example above works with 32-bit IPv4 address. Intermapper now supports 128-bit IPv6 addresses. Wildcard characters are not currently supported for IPv6 addresses.

To allow connections from anywhere, but with authentication:

1. Define your user names and passwords as described in [Users and Groups \(Pg. 272\)](#).
2. From the Server Settings window, click **Remote Server**. A list of firewall entries appears in the right pane.
3. Add a firewall definition and set it to "Allow *.*.*.*."

Anyone that connects is required to provide a username/password.

To allow web connections to see all maps:

1. Define a group named **FullWebAccess**.
2. Add users to that group.

The users in the group can view all web pages, and can acknowledge down devices.

To allow people from known addresses to connect without entering a password:**This is called an automatic-login user.**

1. Create a new user with the desired name.
2. Leave the **Password** box empty.
3. In the **Automatic Login** box, type an IP address.

All connections from that IP address or range are automatically connected, and are assigned the specified user name.

To allow a non-administrator user to see the log files:

1. Define a group named FullLogAccess.
2. Add users to that group.

The users in the group can view all the log files.

To allow an automatic-login user name to connect from elsewhere by entering a password:

Create an [automatic-login user \(Pg. 278\)](#) as described above, but enter a password.

When connecting from an IP address within the range specified for automatic login, the user is automatically connected and assigned the specified user name.

When connecting from an IP address outside the range specified for automatic login, the user is prompted for a user name and password.

To deny all connections from certain addresses or sites:

You can prohibit connections from certain sites.

1. From the **Server Settings** window, click **Remote Server**. A list of firewall entries is displayed in the right pane.
2. Click **Add**. The Firewall Definition dialog is displayed.
3. In the **IP Address** text box, type an IP address or [IP address range \(Pg. 251\)](#).
4. From the **Access** menu, select **Deny**.
5. Click **OK**.

All connections from the specified IP address or range are denied.

To grant a single user access to a specific map:

1. From the **Users** tab, [create a new user \(Pg. 250\)](#).
2. From the **Maps** tab, set the user permissions for the Web and Remote servers.

These permissions are tested only if the user fails to match the global IP address test and/or username and password

Controlling Map Access

You can use the Map Access panel of the Server Settings window to authorize access to a map to one or more users or groups.

NOTE: All individuals in the Administrators group have access to all maps.

The Map Access Panel

Intermapper allows you control the access rights to each map in the following ways:

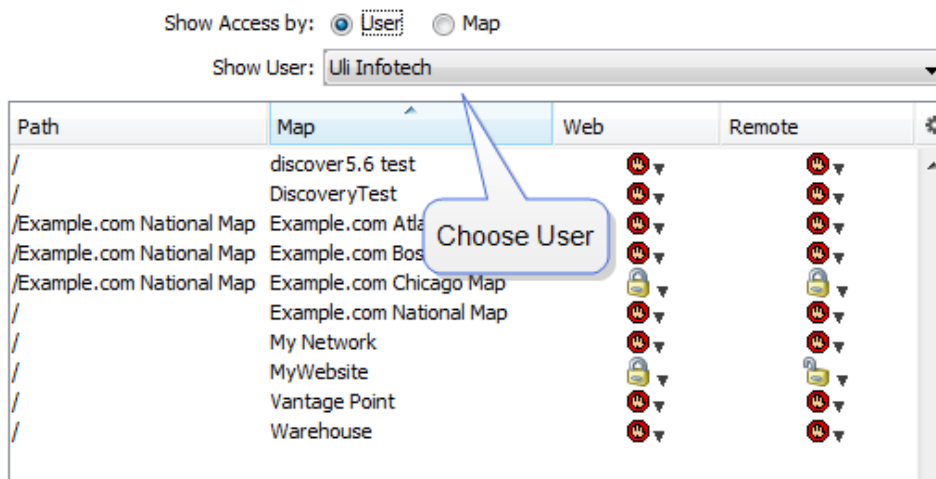
- **Control access by user** - view each user's rights to a particular map.
- **Control access by map** - view each map's access rights for a particular user.

The first example shows the list sorted per-user. It shows the rights that Crabby Appleton has for each of the maps. The second example shows the list sorted per-map. It shows what access each user has to the Current Wireless Probes map.

Controlling Map Access by User

To control map access by user:

1. Select **Show Access by: User** to control access to each map by a specific user through the web and remote servers.



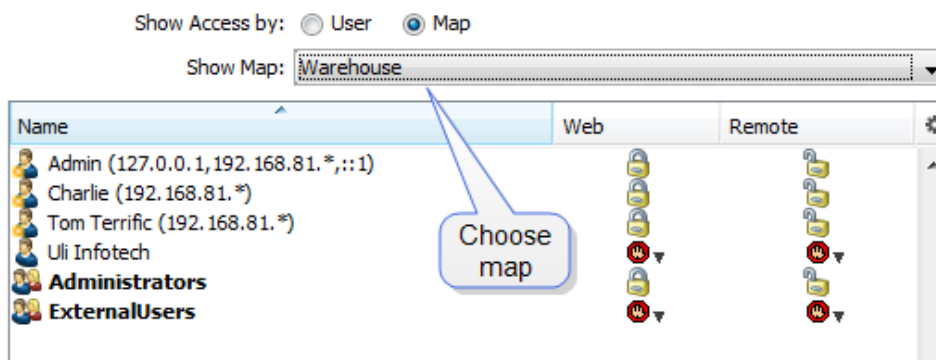
2. Do any of the following:

- Select the user from the **Show User** menu to **set a user's access for any open map**.
- Click the icon in the **Web** column for the user or group whose access permissions you want to set for the selected map through the web server, then select a permission level.
- Click the icon in the **Remote** column for the user or group whose access permissions you want to set for the selected map through the remote server, then select a permission level.
- Alt-click or Cmd-click (Mac) the web or remote menu for any map in the window to set access for all maps at once. When you select from the menu, the value in the selected column is set to the same value for all maps.

Controlling User Access by Map

To control user access by map:

1. Select **Show Access by: Map** to control each user's access to a specific map through the web and remote servers.






2. Do any of the following:

- Select a map from the **Map Name** menu to set access control parameters for any open map.
- Click the icon in the **Web** column for the user or group whose access permissions you want to set for the selected map through the web server, then select a permission level.
- Click the icon in the **Remote** column for the user or group whose access permissions you want to set for the selected map through the remote server, then select a permission level.
- Alt-click or Cmd-click (Mac) the web or remote menu to set access to the selected map for all users at once. When you choose from the menu, the value in the selected column is set to the same value for all users.

Map Access Permission Levels

Select a map's web and remote server access permission levels for each user or group as follows:

	No Access	Denies access to this map.
	Read-Only Access	Allows the user to view the map, but does not allow the user to make changes. (Access to the web server is always read-only.)
	Read-Write Access	Allows the user to view and edit the map.

Map Backup

You can use the Map Backup panel of the Server Settings window to configure scheduled backups of your maps.

Define a schedule for automatic backup of all enabled maps.

☒ Enable scheduled backups

Days:

- ☐ All
- ☐ Sunday
- ☒ Monday
- ☐ Tuesday
- ☒ Wednesday
- ☐ Thursday
- ☒ Friday
- ☐ Saturday

Start time: 09:30

Maximum backups: 2

To schedule map backups:

1. Select the **Enable scheduled backups** check box.
2. Select the **Days** on which you want to schedule backups.
3. Set a **Start time** for the backup.
4. Specify a number of **Maximum backups**.

Scheduled backups are displayed in the Backup and Restore windows as Scheduled. For more information, see [Backup](#) section of the File Menu reference topic.

Notifier List

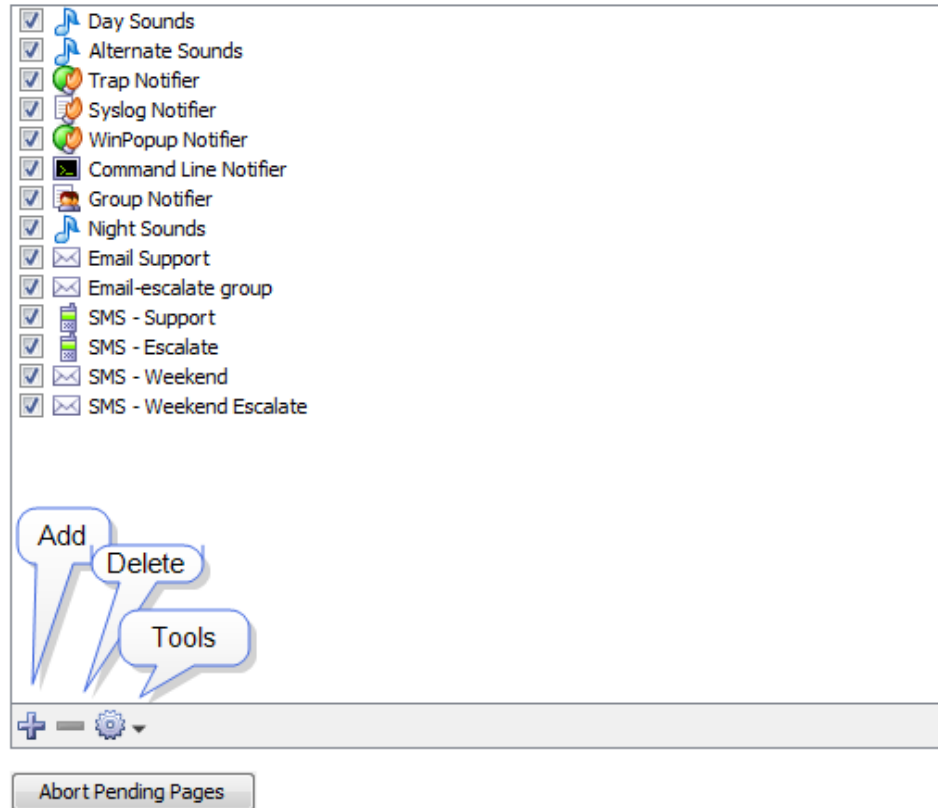
Use the Notifier List section of the Server Settings window to add, edit, copy, and delete notifiers. For more information, see [Using Notifiers \(Pg. 108\)](#).

To view and edit the Notifier List:

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed, showing three sections on the left, each containing a list of available settings. On the right is a panel in which the selected settings are displayed.
2. Click **Notifier List**. A list of notifiers is displayed in the right panel of the Server Settings window.

A notifier sends an alert when the notifier is triggered by an attached device.

Uncheck a notifier to deactivate it for all devices (e.g., during vacation periods).



3. Do any of the following:

- **Add a notifier.** Click **+** The Configure Notifier window is displayed. For more information on configuring notifiers see [Configuring a Notifier \(Pg. 108\)](#).
- **Edit an existing notifier.** Select the notifier you want to edit and select **Edit** from the **Tools** menu. The Configure Notifier window is displayed, showing the current settings for the selected notifier.
- Duplicate a notifier. Select the notifier you want to duplicate and select **Duplicate** from the **Tools** menu. The Configure Notifier window is displayed, showing the current settings of the selected notifier, but with the **name** **<selected notifier > Copy**.
- Delete a notifier. Select a notifier and click the minus sign (-). A confirmation window is displayed.
- **Abort Pending Pages.** All messages sent to pagers still in process are terminated as soon possible and pages waiting to be sent are deleted. This affects only pages sent to Dialup Pagers; it has no affect on SNPP pages or other notifiers.

SSL Certificates

Intermapper's web and remote servers can employ a certificate to encrypt the data going between the server and clients. This assures that the client connected to the actual server and not another server acting as an impostor.

Intermapper ships with a certificate signed by Fortra. The data is encrypted, but does not use a strong encryption (it is easily broken) and web browsers using HTTPS connections give a warning that there is a problem with the certificate and that data might be intercepted in transit.

Creating a Signed SSL Certificate

To create SSL Certificates:

Do one of the following:

- Create a certificate signed by a Trusted Authority. This is the recommended method for production servers.
- Create a self-signed certificate.

WARNING: Self-signed certificates are not appropriate for use on public-facing servers. The only time they should be used is on a local intranet or on a development server when developing or testing an application.

Creating a Certificate From a Trusted Authority

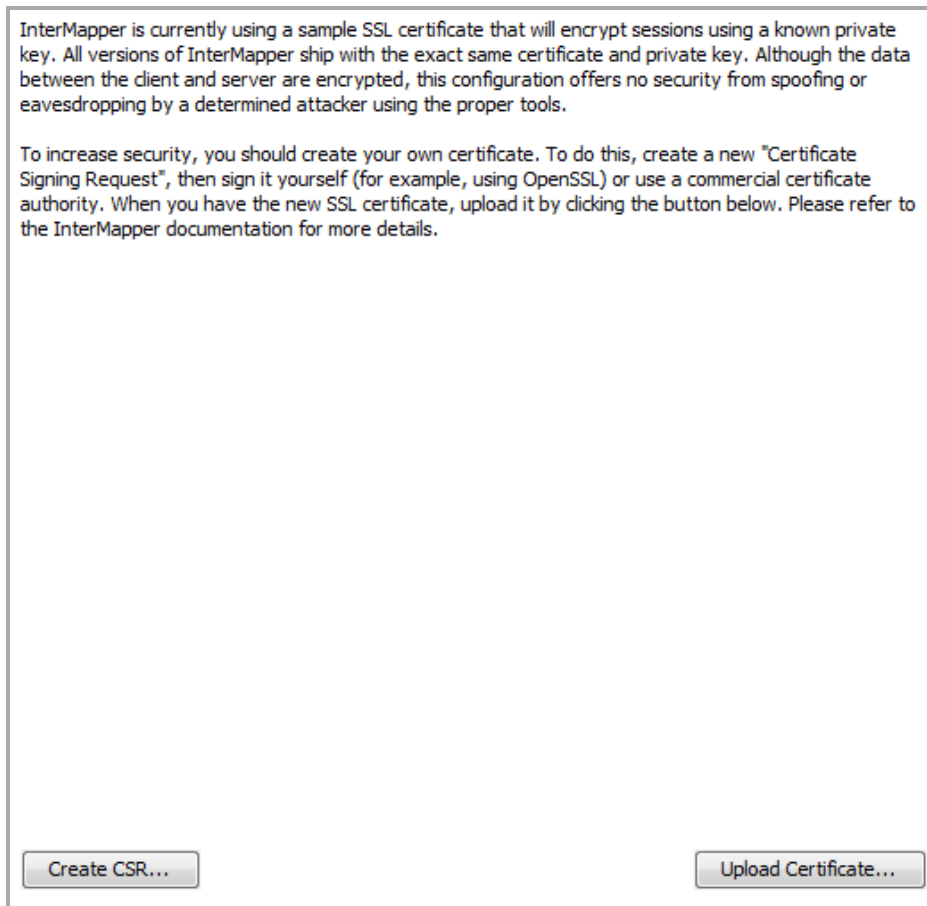
To achieve stronger encryption and verification that the server is authentic, you can create and install your own SSL certificate.

To create and install your own SSL certificate:

1. Create a **Certificate Signing Request** (CSR). The CSR contains all the information needed to identify the computer. Intermapper includes a built-in function for collecting this information and building the certificate.
2. Sign the CSR. Signing is a process where an authority verifies the information in the certificate.
3. Upload the signed certificate into Intermapper to make it operational.

In either case, you must first create a Certificate Signing Request (CSR), which is a file that you can create using Intermapper. Then you need to sign the CSR yourself or send it to a commercial Certificate Authority to sign.

Use the SSL Certificate panel, available from the Server Configuration section of the Server Settings window, to create a Certificate Signing Request and to upload a signed certificate to the InterMapper server.



Step 1: Create a Certificate Signing Request

1. From the **Edit** menu, select **Server Settings**. The Server Settings window is displayed.
2. From the **Server Configuration** section, click **SSL Certificate**. The SSL Certificate panel is displayed.
3. Click **Create new CSR**. The Certificate Signing Request window is displayed.
4. Enter the required information as described below, and click **OK**. A 1,024-bit private key is generated for your system and the information is used to create the Certificate Signing Request. The key and a copy of the CSR are saved in the InterMapper Settings:Certificates folder and a standard Save File dialog is displayed.

You are asked to save a copy of the CSR (with a filename of the FullyQualifiedDomainName.csr) on your disk. Fortra recommends that you save this on the desktop so you can find it when you create a signed certificate. After you

request a signed certificate, you can discard this file.

5. Click **Save**. The new certificate is saved in the specified location.

Enter the following information for your Certificate Signing Request:

- **Common Name**

The full DNS name or IP address of your server. If possible, it should include your domain name.

- **Organization**

The name of your organization.

- **Organizational Unit**

If applicable, the name of an organizational unit within your organization, such as a department or division name.

- **Country**

The two-letter abbreviation for your country

- **State or Province**

The state or province name or abbreviation

- **City or Locality**

The descriptive location of the server.

- **Make new private key**

The first time you generate a CSR, this box is dimmed. On subsequent uses, select this check box to create a new private key. Leave it unchecked to use the same private key.

- **Key Size**

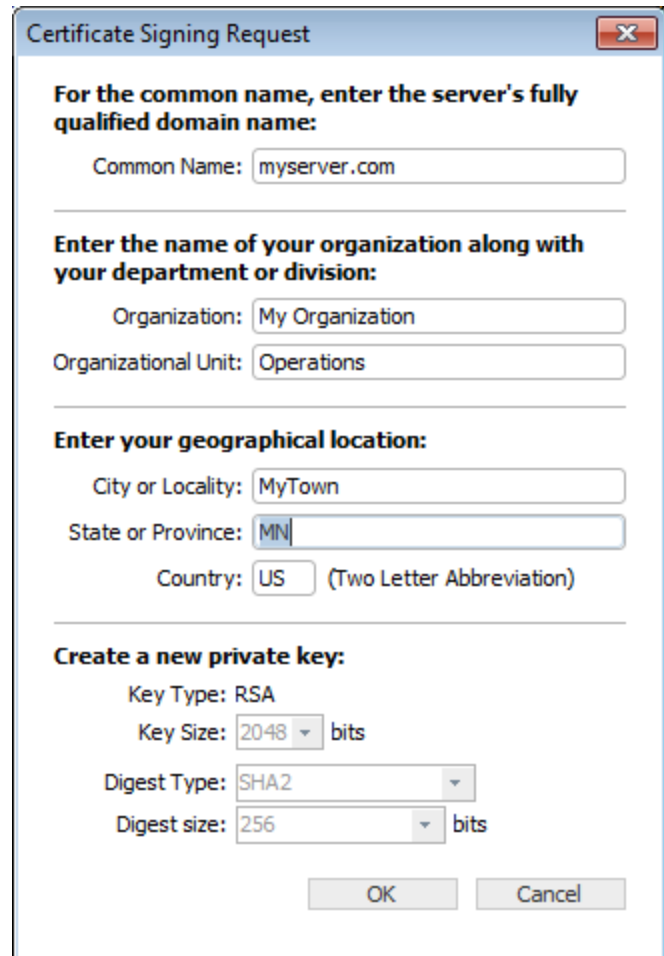
1024 or 2048 bits.

- **Digest Type**

SHA1 or SHA2. SHA1 is the default value.

- **Digest Size**

If you select SHA2, select 256 or 512 bits.



The screenshot shows a 'Certificate Signing Request' dialog box with the following fields and options:

- For the common name, enter the server's fully qualified domain name:**
 - Common Name:
- Enter the name of your organization along with your department or division:**
 - Organization:
 - Organizational Unit:
- Enter your geographical location:**
 - City or Locality:
 - State or Province:
 - Country: (Two Letter Abbreviation)
- Create a new private key:**
 - Key Type: RSA
 - Key Size: bits
 - Digest Type:
 - Digest size: bits

At the bottom right are 'OK' and 'Cancel' buttons.

When you click OK, InterMapper generates a private key for your system and uses the information entered above to create the Certificate Signing Request. InterMapper saves following files in the InterMapper Settings\Certificates folder:

- **SSLCertificateKeyFile** - contains your private key
- **Pending.csr** - the Certificate Signing Request (CSR) file

You are also asked to save another copy of the CSR (with a filename of the FullyQualifiedDomainName.csr) on your disk. Fortra recommends that you save this on the desktop so you can find it when you are ready to create a signed certificate. You can discard this file after you request a signed certificate.

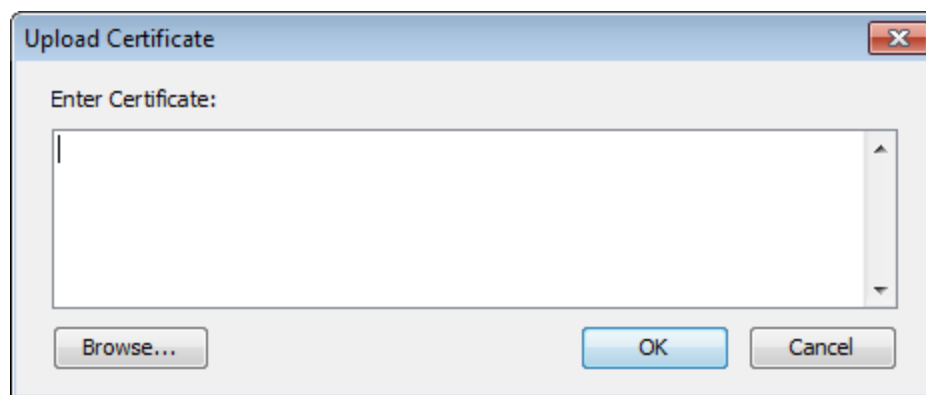
Step 2: Sign the Certificate

After you have a CSR file, you must have it signed. The file can be signed in one of the following ways:

- Use the OpenSSL software (available from <http://www.openssl.org>) or the Windows CA to sign the CSR. This creates a self-signed certificate that you can easily use within your own organization.
- Send the CSR to any of several commercial certificate authorities, such as InstantSSL (<http://www.instantssl.com>), Verisign (<http://www.verisign.com/products/site/index.html>), or Thawte (<http://www.thawte.com>). These companies return a signed certificate that is globally-recognizable as authentic.

Step 3: Uploading the Signed Certificate

After the certificate is signed, click **Upload new Certificate**. Either copy and paste the text of the certificate into this window, or click **Browse** and locate the certificate file on your hard drive.



At the conclusion of this, the Intermapper Settings\Certificates folder contains the following files:

- **SSLCertificateKeyFile** - contains your private key.
- **SSLCertificateFile** - contains your signed certificate (the file from Verisign, InstantSSL, or OpenSSL). Remove any suffix (such as .pem) from the file name.
- **SSLCACertificateFile** - contains the public certificate chain of the signing CAs (in order).

Stop and restart the affected server from the Server Settings window. These certificates are used for HTTPS and Intermapper Remote client connections if the SSL/TLS boxes are selected in the respective server settings.

Using an Externally Generated CSR and Private Key

If you use a different application than Intermapper to create your Certificate Signing Request (CSR), Intermapper does not have access to the private key used to create the CSR. To upload your certificate with the private key, create a text file containing the signed certificate, the private key, and the CA's public certificate chain (if included). Click **Upload new certificate** to upload this combined file.

Creating a Self-Signed Certificate

You can create your own self-signed certificate in order to use an encrypted connection. This is only recommended for intranets and development servers. You should never use a self-signed certificate for a production server.

To create and use a simple self-signed certificate with Intermapper:

1. Create the certificate and its private key.
2. Create a version of the key and certificate suitable for use in Microsoft Windows.
3. Import the certificate and key into Intermapper.
4. Import the certificate and key into Microsoft Windows.

Configuring SSL Protocols, Cipher Selections, and Options

After you set up your OpenSSL certificate, you can configure the operation of the OpenSSL-based services provided by the Intermapper server to conform to your local security policy. For information on how to configure the operation, see the description of the `ssl.conf` file in [Intermapper Server Settings Folder](#).

Technical Notes

The design for this scheme is based on the SSL section of the Apache Mod-SSL httpd.conf file.

- For InstantSSL, the SSLCertificateFile is the same as the ca-bundle file, described in http://www.instantssl.com/ssl-certificate-support/cert_installation/.
- If there is no SSLCertificateKeyFile, InterMapper looks for the private key in SSLCertificateFile.
- InterMapper always loads additional CA certificates, if they exist, from SSLCertificateFile first, then it checks to see if SSLCACertificateFile exists.
- You can set up the configuration so one file, named SSLCertificateFile, contains everything. The file must contain a key, certification, and trust chain in that order, or the certificate is not imported properly.
- InterMapper converts CRs to LFs in the file data before loading it. There is no need to worry about CR-LF translation issues.

Configuring New Device Detection

You can use the New Device Detection panel to enable and configure new device detection.

New Device Detection through InterMapper Flows Server

New Device Detection can be done through InterMapper Flows server with no Flows license.

Flows server is not running. New Device Detection will take effect when Flows server starts.

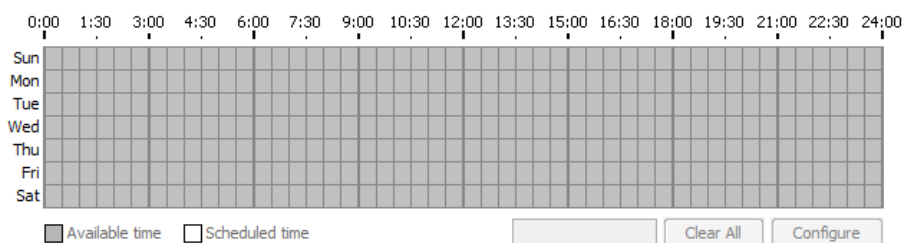
☐ Run New Device Detection with Flows server

☐ Turn off Flows data collection

New Device Detection through Scheduled Auto-Discovery

New Device Detection can be also done through Scheduled Auto-Discovery.

☐ Run New Device Detection with Scheduled Auto-Discovery



To enable and configure new device detection from the New Device Detection panel:

Do one of the following:

- **Run New Device Detection with Flows server** - select this check box to use the Flows server for new device detection.
- **Turn off Flows data collection** - select this check box to disable Flows data collection.
- **Run New Device Detection with Scheduled Auto-Discovery** - select this check box to use the Flows server for new device detection.

Methods of New Device Detection

The following methods are available for detecting new devices:

- Use the Intermapper Flows server to query a Flows exporter to find new devices.
- Use Scheduled Auto-Discovery to have the Intermapper server perform Auto-Discovery as scheduled, searching only for new devices.

Which Method Should You Use?

The two methods described above are not mutually exclusive. You can use both methods at the same time. Each has its advantages and disadvantages.

Using the Flows Server for Detecting New Devices

- When enabled, new device detection runs continuously. (It cannot be scheduled.)
- A Flows license is not required, but you must set up [a Flows exporter](#) to use this feature.
- This method detects devices that actively generate network traffic and can discover devices that might otherwise be missed by Auto-Discovery.

Using the Scheduled Auto-Discovery for Detecting New Devices

- When enabled, uses the same methods as regular Auto-Discovery, but queries only IP addresses that are not already in the device list.
- Use this method to schedule discovery of new devices to run as often as every half hour. This method can put additional load on the Intermapper server, so consider scheduling discovery for off-peak periods, such as nights and weekends.
- This method actively probes devices and discovers devices that are not generating network traffic and thus are not discovered using the Flows server.

Detection Map

As soon as you enable either method, a new map is displayed in the map list, named DetectionMap. All new devices (ones are not currently in the Device List) are displayed on the map. After they are discovered, you can move these devices to other maps. For more information, see [Using The Detection Map](#).

Entering AWS EC2 Instance Credentials Through Server Settings

There is an AWS EC2 panel in Server Settings to allow you to add, edit, and delete AWS EC2 instances. You can access this information from your Amazon AWS account. You can select an EC2 instance to use when you add an AWS EC2 probe.

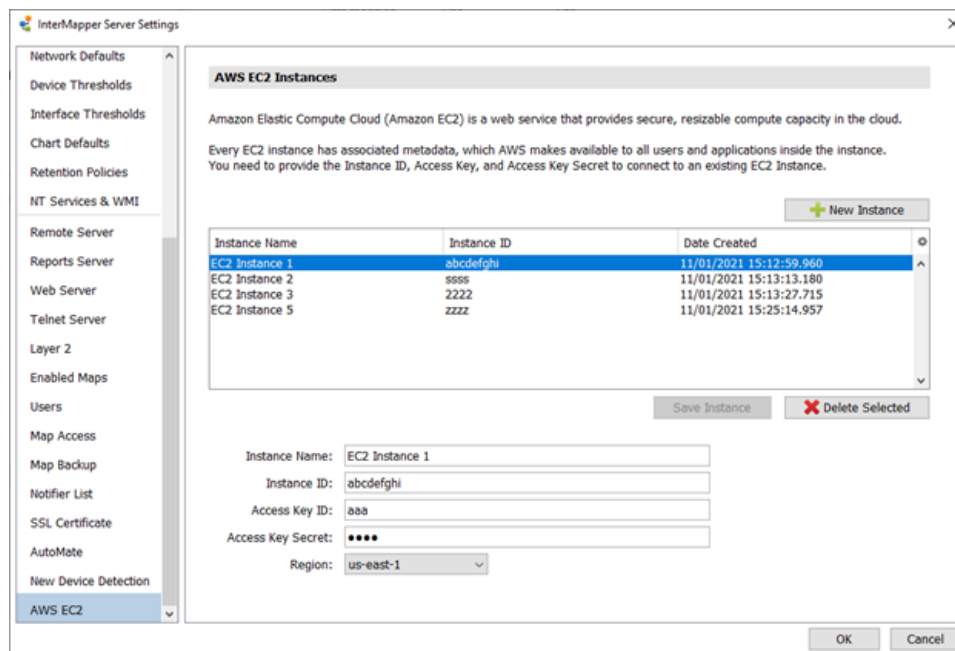
The Access Secrets of the AWS EC2 instances are reversibly encrypted using AES256. A random encryption key, which is generated on-demand-generated on first use are stored in the Intermapper server's host file system protected by OS file system security. This file is readable only by Intermapper and root users on UNIX hosts and only by a user with local administrator privilege on Microsoft Windows systems.

NOTE:

User information for EC2 instances is created in AWS. (The information is used by Intermapper but is not created in Intermapper.)

NOTE:

An EC2 instance must have a valid Instance ID in order for it to be saved.



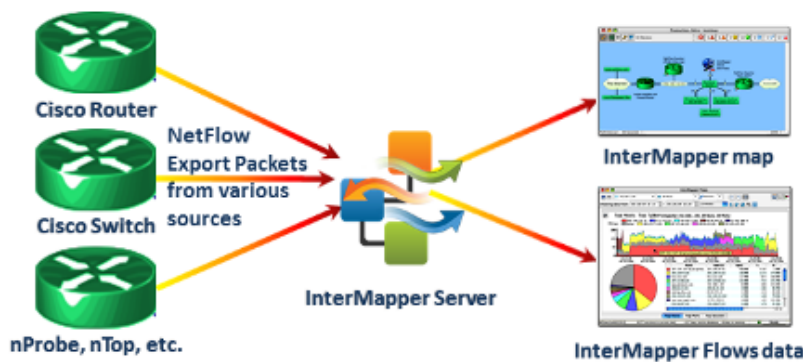
Intermapper Flows™ Overview

Intermapper has always made it easy to see heavy traffic at a glance. Its charts show when traffic peaks, but not what it is used for.

Intermapper Flows™ is a feature of Intermapper that allows you to obtain deeper insight into the traffic on your network. It is a Flows analyzer that works with NetFlow, sFlow, JFlow, and cFlow and can display the following:

- Top talkers and listeners
- Top protocols in use
- Top conversations and sessions
- Detailed session information to identify particular machines

How Intermapper Flows Works With Intermapper



Intermapper Flows collects and stores Flows data from any device that supports its collection (Flows Exporter). For information on supported devices, see [Supported Exporters](#). You can select the available exporters from which you want to collect data. For more information, see [Flows Settings - Exporters Tab](#).

Intermapper Flows™ Overview

Intermapper has always made it easy to see heavy traffic at a glance. Its charts show when traffic peaks, but not what it is used for.

Intermapper Flows™ is a feature of Intermapper that allows you to obtain deeper insight into the traffic on your network. It is a Flows analyzer that works with NetFlow, sFlow, JFlow, and cFlow and can display the following:

- Top talkers and listeners
- Top protocols in use
- Top conversations and sessions
- Detailed session information to identify particular machines

How Intermapper Flows Works With Intermapper



Intermapper Flows collects and stores Flows data from any device that supports its collection (Flows Exporter). For information on supported devices, see [Supported Exporters](#). You can select the available exporters from which you want to collect data. For more information, see [Flows Settings - Exporters Tab](#).

Installing Intermapper Flows

Consider the following before installing Intermapper Flows:

- Intermapper Flows is installed automatically with Intermapper. For more information, see [Installing and Launching Intermapper](#).
- If you are running a trial version, Intermapper Flows is fully operational. After your trial expires, an Intermapper Flows license is required.
- Remove any firewalls on the selected UDP ports for NetFlow. The default port is 2055.

NOTE: The Intermapper Flows service/daemon might not start if another program is using port 2055 (or whatever port you have designated for netflow packets). Stop or uninstall other netflow packages on the system.

- Configure one or more Flows exporters to send data to the Intermapper Flows server. Intermapper Flows automatically detects the exporters and begins data collection. Many switches and routers can be configured to export Flows data.

Flows Window

You can use the Flows window to view and analyze traffic at a very detailed level. Intermapper Flows acts as a NetFlow/sFlow collector. The Flows window provides a view of Flows data collected from supported hardware and software exporters.



To open the Flows window:

- **See all Flows data** - from the **Map List** window, **right-click** or **Ctrl-click** a server and select **Flows Window**. This is an unfiltered view of your Flows data and no filters are set.
- **See Flows data for a specific exporter's interface** - **right-click** or **Ctrl-click** a link on a device that shows an exporter device badge and select **Show In > Flows Window**. The Exporters filter is set to the selected exporter.

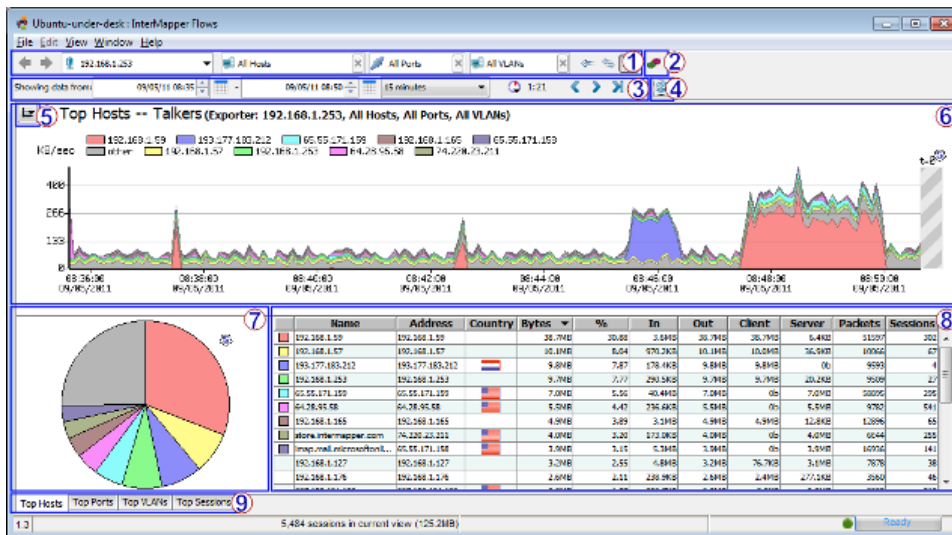
NOTE: The Exporter badge is displayed for any device that is in the list of Flows exporters. For more information, see [Flows Settings - Exporters Tab](#).

- **See all Flows data for a device** - **right-click** or **Ctrl-click** a device and select **Show In > Flows Window**. The Device filter is set to the selected device. If the device has the same IP address as an exporter, that exporter is selected in the Exporters filter and only data for that exporter is displayed.

For more information on filters, see [Filter Tools](#) below.

Understanding the Flows Window

You can use the Flows window to view Flows data.



When you first open the Flows window, the Hosts tab is selected. From the Hosts tab, do the following:

- **1: Filter tools** - select the subset of Flows data to view.
- **2: Intermapper Flows Settings** - view and edit Intermapper Flows settings.
- **3: Time Range Selection tools** - select and navigate Flows data over a specified period.
- **4: Refresh button** - click to refresh the current view of Flows data.
- **5: Set Graph Scale** - select a scale to use for viewing data in the stack chart.
- **6: Stack Chart** - view current host, port, or VLAN data in a stack chart.
- **7: Hosts, Ports, or VLANs pie chart** - view current host, port, or VLAN data as a percentage of total data flow in a pie chart.
- **8: Hosts, Ports, or VLANs list table** - view details about a specific host, port, or VLAN.
- **9: Page Selection tabs** - Click a tab to select a Flows window page.




Click a tab to select one of the following Flows window pages:

- **Top Hosts tab** - view a list of top talkers, listeners, or both, with stack and pie charts showing the relative activity of each.
- **Top Ports tab** - view a list of ports with the highest activity, with stack and pie charts showing the relative activity of each.
- **Top VLANs tab** - view a list of VLANs with the highest activity, with stack and pie charts showing the relative activity of each.

- **Top Sessions tab** - view a list of sessions, with start and end IP addresses and the start and end time of each session.




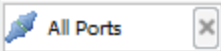
Flow Type Icons



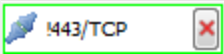
When collecting data from NetFlow and sFlow exporters, you can see what kind of exporter the data is coming from.

	NetFlow Data	This icon is shown when viewing data from a NetFlow exporter. Depending on the version, the icon shows a 1, 5, 7, or 9.
	sFlow Data	This icon is displayed when viewing data from an sFlow exporter.
	J-Flow, CFlow	These exporters implement a Flows format that is identical to NetFlow v5, so they appear as NetFlow v5 in the Flows window.

Filter Tools

You can use the filter tools to view a subset of the data, selecting from available exporters, talkers, listeners, ports, or sessions collected by Intermapper Flows.

	Previous/Next view	Click the left arrow to view the current tab with a previous set of filters. If you clicked a previous set of filters, click the right arrow to view the current tab with the next set of filters in the view history.
	Exporter	Select a different exporter from the menu to view traffic from that exporter. You can also select a specific interface on an exporter from the menu.
	Host	Enter an IP address or subnet (x.x.x.x/#) to view traffic from that host or subnet or select from the menu. Type an exclamation point (!) to exclude the specified host.
	Port	Enter a port from the menu to view traffic from that port or choose from the menu. Type an exclamation point (!) to exclude the specified port.

	VLAN	Enter a VLAN number in the box to show Flows activity for only that VLAN. Type an exclamation point (!) to exclude the specified VLAN.
	Talkers/ Both/ Listeners	Click the left arrow to view Top Listeners (receivers) only, the right arrow to view Top Talkers (senders) only, and the button with both arrows to view Top Hosts by the total traffic sent and received by each host.
	Context Menu	Right-click or Ctrl-click an area of host activity in the Stack chart, Pie chart, or list and choose from the context menu. The menu changes depending on which area of the window you right-click. Get more detail in the Top Hosts , Top Ports , or Top Sessions tab.
	Exclude Host/Port/VLAN	Type an exclamation point (!) to negate a filter, or right-click (Ctrl-click) a host, port, or VLAN in the pie chart or graph and select Exclude. Negated filters are shown with green border.

Time Range Selection







You can use the time range selection controls to view and select a range of time for which you want to view.




To select a time range:

- Select by dragging across an area of the stack chart.
- For precise control, enter times in the Showing data from Start and End time fields.
- Click the calendar icon to set a Start or End date.
- Use the menu to select a preset time range. When you change this value, the current End time is preserved.

- Use the time navigation controls shown below to jump back or forward by the amount shown in the time range menu or jump to now.

	Back in Time	Click the left arrow to view the previous page of data. The amount of data shown is determined by the current setting of the time range menu.
	Forward in Time	Click the right arrow to view the next page of data. The amount of data shown is determined by the current setting of the time range menu.
	Forward to Now	Click Now to view the latest data. The amount of data shown is determined by the current setting of the time range menu.
	Zoom Out	Click Zoom Out to reset the time range to the most recent setting in the Time Range menu.
	Refresh	Click Refresh to view the most recent data, based on the setting of the time range menu.
	Auto-refresh Interval	Select a refresh interval from the Auto-refresh menu.
	Time until refresh	The time to the right of the Auto-refresh Interval button indicates the time until the next refresh of the window.

Reports and Settings

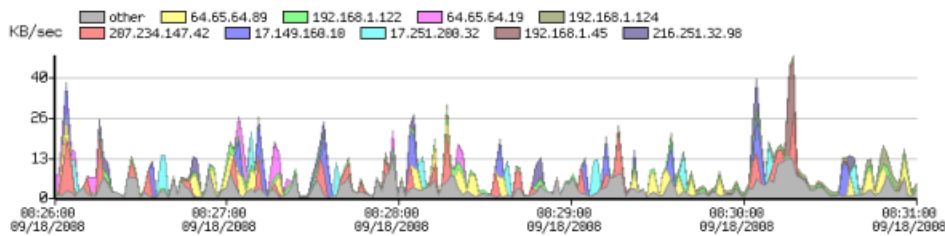
	Save...	Select this command from the File menu to save a PDF report to disk. A standard file dialog is displayed. The report contains the Top Hosts, Top Ports, and Top Sessions tabs.
	Print...	Select this command from the File menu to print a report using the current time range and filter settings. A standard print dialog is displayed.
	Open Settings Dialog	Click this button to open the Intermapper Flows Settings dialog. For more information, see the Intermapper Flows Settings topic.

Top Hosts Tab

Click the **Top Hosts** tab (or type **Ctrl-1**) to view a list of top talkers, listeners, or both, with stack and pie charts showing the relative activity of each.

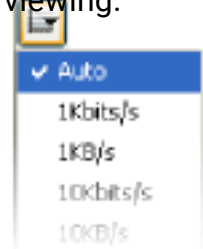
Stack Chart

You can use the Stack chart in the Top Hosts tab to view the relative activity of different hosts over time. Each host's activity is stacked with the others, with the top host on the bottom of the stack. Here's a typical stack chart:



The legend above the chart shows the top hosts for the data you are currently viewing.

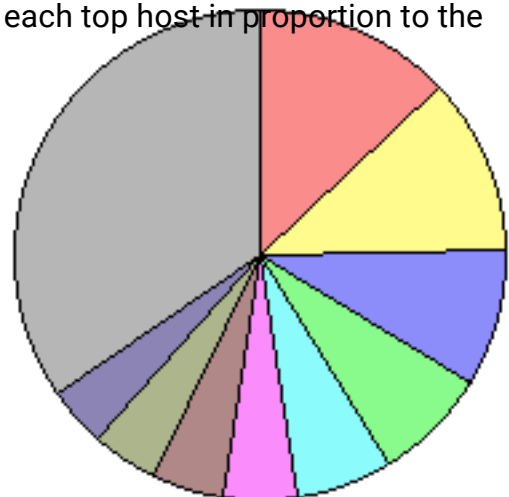
- Click a legend (above the stack chart) to select the corresponding line in the Host list.
- Mouse over an area of the stack chart to view the host address for that activity.
- Click an area of the stack chart to select the corresponding line in the Host list.
- Click and drag a region of the chart to reset the time range to that area of the stack chart.
- Click **Set Graph Scale** to set the vertical scale for the stack chart. Select **Auto** to normalize the scale to the displayed data, or select a scale between 1Kbits/second and 10GBytes/second.
- Right-click an area of the stack chart and select from the context menu as described below.



Pie Chart

You can use the Pie chart to view the relative activity of each top host in proportion to the others.




- Click a pie segment to select the corresponding line in the Host list.
- Mouse over a pie segment to view the host address for that segment.
- Right-click an area of the Pie chart and select from the context menu as described below.




Host List

You can use the Host List to view detailed statistics about a particular host. Below is a typical host list, which shows the top 25 hosts.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Ctrl-click a row to select or de-select it.
- Right-click a line or IP address from the Host list and select from the context menu as described below.

Legend	Hostname	Address	Country	Bytes	%	In	Out	Client	Server
	207-234-147-42.ptr.example.com	207.234.147.42		385.5 KB	13.03	41.7K B	385.5 K	3.9KB	381.6 KB
	example.net	64.65.64.89		343.3 K	11.61	35.2K B	343.3 KB	0b	343.3 KB
	nwk-www.example.com	17.149.160.10		267.7 KB	9.05	12.9K B	267.7 KB	0b	267.7 KB
	dhcp-122.dartware.com	192.168.1.122		223.0 KB	7.54	1.1M B	223.0 KB	217.5 KB	5.5KB
	cup-www.example.com	17.251.200.32		189.9 KB	6.42	8.1KB	189.9 KB	0b	189.9 K
	vws.example.net	64.65.64.19		142.3 K	4.81	17.2K B	142.3 KB	0b	142.3 KB
	nitro.dartware.com	192.168.1.45		141.1 KB	4.77	670.4 KB	141.1 KB	74.2K B	66.9K B
	dhcp-124.dartware.com	192.168.1.124		125.1 KB	4.23	76.6K B	125.1 KB	83.9K B	41.2K B
	hosting.example.com	216.251.32.98		115.8 KB	3.91	8.5KB	115.8 KB	0b	115.8 KB
	eclair.example.net	64.65.64.64		98.1K B	3.32	18.8K B	98.1K B	0b	98.1K B

outgoing02.example.net	64.65.64.125		69.2K B	2.3 4	26.0K B	69.2K B	0b	69.2K B
192.168.1.12	192.168.1.12		63.3K B	2.1 4	67.8K B	63.3K B	25.5K B	37.8K B
<up to 25 rows>								
Other	Other		396.5 KB	13. 40	555.8 KB	396.5 KB	118.5 KB	278.0 KB

- **Legend** - The top 10 hosts are indicated with color legends. The report shows the top 25 hosts or ports, but places the Other category at the bottom of the list, as it shows total traffic for the remaining hosts or ports not shown in the previous 24 rows.
- **Hostname** - the host name of the talker or listener.
- **Address** - the IP address of the talker or listener.
- **Country** - a flag indicating the country in which the host name or IP address originates.
- **Bytes** - the volume of traffic (in bytes/kbytes/mbytes) for a particular row in the specified time interval.
- **%** - the percentage of traffic attributed to this host during the specified time interval.
- **In** - the number of bytes received by the host's IP address.
- **Out** - the number of bytes sent from the host IP address.
- **Client** - the number of bytes transmitted when the host acted as a client (for example, sending a request to another server.)
- **Server** - the number of bytes transmitted when the host acted as a server (for instance, when responding to a request from a client).

NOTE: Intermapper Flows uses the following heuristic rules to determine which host is operating as a client or server:

- It has a built-in list of common server ports. If the port matches an entry in the list, it is treated as a server.
- If there is no match with a common host port, the lower-numbered port is treated as a server.

- **Packets** - the number of packets sent or received by this host.
- **Sessions** - the number of sessions including this host.

Context Menu - Top Hosts tab

Right-click or Ctrl-click (macOS) on the Stack chart, Pie chart, or Host list, and select from the Context menu as follows:

Stack chart

- **Select On [host]** - includes only traffic from the selected host.
- **Exclude [host]** - excludes traffic from the selected host.
- **Center on this** - centers the stack chart on the selected point in the timeline.

Pie chart

- **Select On [host]** - includes only traffic from the selected host.
- **Exclude [host]** - excludes traffic from the selected host.

Hosts List

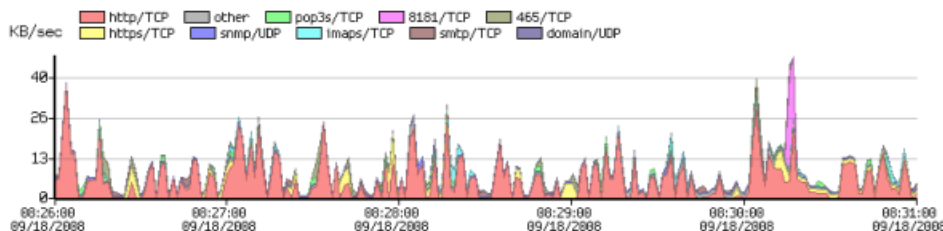
- **Select All** - selects all rows of the table
- **Filter on selected host** - includes only traffic to or from the selected host.
- **Exclude selected host** - excludes traffic from the selected host.
- **Copy selected rows** - copies the fields from the selected table rows to the clipboard.
- **Copy IP address** - copies only the IP address from the selected row to the clipboard.
- **Whois Lookup** - see the Whois description for the selected host.

Top Ports Tab

Click the **Top Ports** tab (or type **Ctrl-2**) to view a list of ports with the highest activity, with stack and pie charts showing the relative activity of each.

Stack Chart

You can use the Top Ports tab's Stack chart to view the relative activity of different ports over time. Each port's activity is stacked with the others, with the top port on the bottom of the graph. For example,



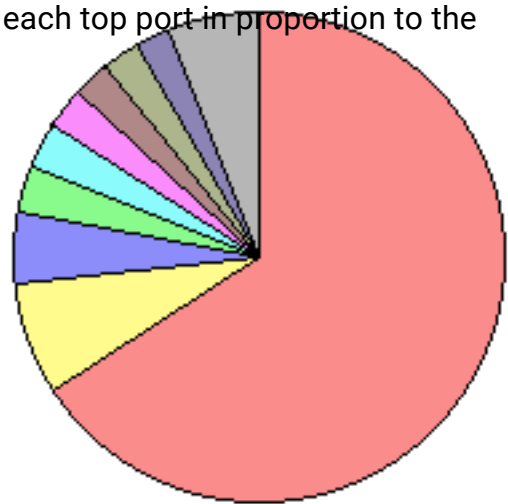
The legend above the chart shows the top hosts for the data you are currently viewing.

- Click a legend above the Stack chart to select the corresponding line in the Port list.
- Mouse over an area of the Stack chart to view port information for that activity.
- Click an area of the stack chart to select the corresponding line in the Port list.
- Click and drag a region of the chart to reset the time range to that area of the Stack chart.
- Click the **Set Graph Scale** button to set the vertical scale for the Stack chart. Select **Auto** to normalize the scale to the displayed data, or select a scale between 1Kbits/second and 10GBytes/second.
- Right-click an area of the Stack chart and select from the context menu as described below.

Pie Chart

You can use the Pie chart to view the relative activity of each top port in proportion to the others.

- Click a pie segment to select the corresponding line in the Ports list.
- Mouse over a pie segment to view the port corresponding to that segment.
- Double-click a segment of the pie chart to set a filter allowing you to view data only for the selected port.
- Right-click or Ctrl-click a point in the timeline and select **Center on This** from the context menu to bring a particular point in the Stack chart to the center of the timeline.
- Double-click a pie segment or right-click or Ctrl-click a segment and select **Select on Port/Protocol [Service or Port number]** from the context menu to set a filter for that port.
- Right-click an area of the Stack chart and select from the context menu as described below.



Ports List

You can use the Ports List to view detailed data about the top 25 ports.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Control-click a row to select or de-select it.
- Right-click or Ctrl-click a row and select **Select All** to select all rows.
- Right-click a selected row and select **Copy Selected Rows** to copy the currently selected set of rows to the clipboard in tab-delimited format.

Legend	Service	Protocol	Port	Bytes	%
	HTTP	TCP	80	1.9MB	65.76
	HTTPS	TCP	443	223.8KB	7.57
	SNMP	UDP	161	134.8KB	4.56
	SNMP	UDP	161	134.8KB	4.56
	SNMP	UDP	161	134.8KB	4.56
	8181	TCP	8181	78.3KB	2.65
	SMTP	TCP	25	74.0KB	2.50
	465	TCP	465	72.2KB	2.44
	1278	UDP	1278	41.6KB	1.40
	ICMP	ICMP		22.7KB	0.77
	1220/TCP	TCP	1220	17.1KB	0.58
	1220/TCP	TCP	1220	17.1KB	0.58
	106/TCP	TCP	106	11.6KB	0.39
	< up to 25 rows >				
	OTHER	IP		13.4KB	0.45

- **Legend** - the top 10 ports are indicated with colored legends. The report shows the top 25 ports, but places the Other category at the bottom of the list, as it shows total traffic for the remaining ports not shown in the previous 24 rows.
- **Service** - the name of the server associated with the port.
- **Protocol** - the protocol (TCP/UDP/GRE/ICMP) associated with the port.
- **Port** - the port number
- **Bytes** - the volume of traffic (in bytes, kbytes, or mbytes) for a particular row in the

specified time interval.

- % - the percentage of traffic for the specified port in the specified time interval.

Context Menu - Top Ports Tab

You can right-click or Ctrl-click (macOS) on the Stack chart, Pie chart, or Ports list and select from the Context menu as follows:

Stack chart

- **Select On [port]** - includes only traffic from the selected port.
- **Exclude [port]** - excludes traffic from the selected port.
- **Center on this** - centers the stack chart on the selected point in the timeline.

Pie chart

- **Select On [port]** - includes only traffic from the selected port.
- **Exclude [port]** - excludes traffic from the selected port.

Ports List

- **Select All** - selects all rows of the table.
- **Filter on selected port** - includes only traffic to or from the selected port.
- **Exclude selected port** - excludes traffic from the selected row.
- **Copy selected rows** - copies the fields from the selected table rows to the clipboard.
- **Copy IP address** - copies only the IP address from the selected row to the clipboard.
- **Whois Lookup** - see the Whois description for the selected port.

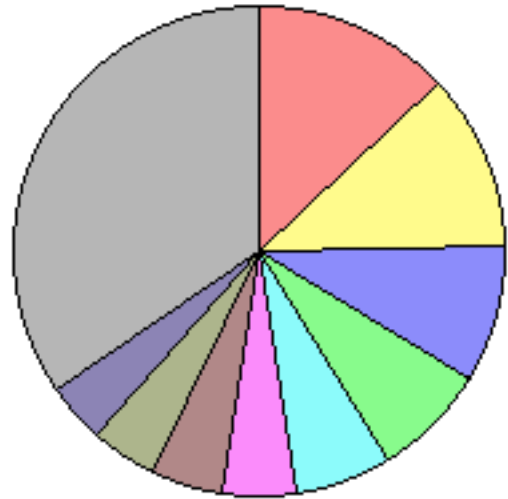
Top VLANs Tab

Click the **Top VLANs** tab (or type **Ctrl-3**) to view a list of VLANs with the highest activity, with stack and pie charts showing the relative activity of each.

Pie Chart

You can use the Pie chart to view the relative activity of each top VLAN in proportion to the others.

- Click a pie segment to select the corresponding line in the VLAN list.
- Mouse over a pie segment to view the percentage of traffic for that VLAN.
- Right-click an area of the Pie chart and choose from the context menu as described below.



VLAN List

You can use the VLAN List to view detailed statistics about a particular VLAN.

- Click a column heading to sort by that column. Click again to reverse the sort.
- Click an unselected row to select it.
- Shift-click an unselected row to select all rows between that row and the currently selected row.
- Control-click a row to select or de-select it.
- Right-click a line in the VLAN list and select from the context menu as described below.

Legend	VLAN	Bytes	%
	0	385.5K	13.03
	1	343.3K	11.61
	2	267.7K	9.05
	3	223.0K	7.54
	4	189.9K	6.42
	5	142.3K	4.81
	6	141.1K	4.77
	7	125.1K	4.23
	8	115.8K	3.91
	9	98.1K	3.32
	10	69.2K	2.34

	11	63.3K	2.14
	<up to 25 rows>		
	Other	396.5KB	13.40

- **Legend** - the top 10 VLANs are indicated with color legends. The report shows the top 25 VLANs but places the Other category at the bottom of the list, as it shows total traffic for the remaining VLANs not shown in the previous 24 rows.
- **VLAN** - the number of the VLAN.
- **Bytes** - the volume of traffic (in bytes, kbytes, or mbytes) for a particular row in the specified time interval.
- **%** - the percentage of traffic attributed to this VLAN during the specified time interval.

Context Menu - Top Hosts tab

Right-click or Ctrl-click (macOS) the Stack chart, Pie chart, or Host list and select from the Context menu as follows:

Stack chart

- **Select On VLAN [NN]** - includes only traffic from the selected host.
- **Exclude VLAN [NN]** - excludes traffic from the selected host.
- **Center On This** - centers the stack chart on the selected point in the timeline.

Pie chart

- **Select On VLAN [NN]** - includes only traffic from the selected host.
- **Exclude VLAN [NN]** - excludes traffic from the selected host.

VLANs List

- **Filter on selected VLAN** - includes only traffic to or from the selected VLAN.
- **Exclude selected VLAN** - excludes traffic from the selected row.
- **Select All** - selects all rows of the table.
- **Copy selected rows** - copies the fields from the selected table rows to the clipboard.

Top Sessions Tab

Click the **Top Sessions** tab (or type **Ctrl-4**) to view a list of sessions, with client and server IP addresses and the start and end time of each session.

You can use the Top Sessions tab to view detailed data about sessions with the greatest amount of traffic.

- **Client** - the IP address or host name of client in the session.
- **Server** - the IP address or host name of the server to which the session is connected.
- **Service** - the service used during the session.
- **Total Bytes** - the total number of bytes sent and received during the session.
- **Client Port** - the port number used by the session's client.
- **Server Port** - the port number used by the session's server.
- **Protocol** - the protocol (TCP, UDP, GER, or ICMP) used during the session.
- **Client Packets** - the total number of packets sent by the client during the session.
- **Client Bytes** - the total number of bytes sent by the client during the session.
- **Server Packets** - the total number of packets sent by the server during the session.
- **Server Bytes** - the total number of bytes sent by the server during the session.
- **Start Time** - the session's start time. If the session started before the start of the time range currently being viewed, the start time is shown in a different color.
- **Last Update** - the time when the last packet is sent or received during the session. If the session ended before the start of the time range currently being viewed, the Last Update time is shown in a different color.
- **Exporter** - the IP address of the exporter that recorded the session.
- **In** - the index of the device interface through which the client packets entered.
- **Out** - the index of the device interface through which the server packets entered.
- **VLAN In** - the number of the VLAN used for incoming packets.
- **VLAN Out** - The number of the VLAN used for outgoing packets.

Sorting the Sessions List

You can sort the Sessions list by any column.

To sort the Sessions list:

Do one of the following:

- Click a column heading to sort by that column.
- Click again to reverse the sort.

Supported Exporters

NetFlow: Intermapper Flows handles NetFlow v1, v5, v7, and v9 exports from routers and switches from Cisco and other NetFlow-compatible vendors as well as a number of software exporters.

sFlow: Intermapper Flows handles sFlow versions 2, 4, and 5, including MIB Enterprise numbers 4300 and 14706 from equipment from HP, Extreme, Foundry, Force10, and others.

J-Flow, CFlow: Identical to NetFlow v5, implemented by different vendors. The NetVlow v5 icon is displayed when using these exporters

Using Intermapper Flows with sFlow

sFlow provides information about the traffic through the network, including the sender and recipient of the traffic flows and the protocols used.

To configure Intermapper Flows to receive the sFlow data, you must first enable sFlow export on the router or switch. Most modern gear uses SNMP to enable or disable sFlow export, as described in the [sFlow specification](#).

Intermapper Flows allows you to specify the exporter(s) that should send data.

To add an sFlow exporter:

1. Open the **Flows Settings** window.
2. Click the **Exporters** tab.
3. Set the sFlow port (default is 6343) at the bottom of the window.
4. Click **Add sFlow exporter**. The Enter sFlow Information window is displayed.
5. Enter the IP address of the exporter, the SNMP read/write community string, select the IP address for the collector, select a sampling rate, and click **OK**. Intermapper Flows configures the selected exporter (using SNMP) to send sFlow records to the specified collector. The exporter is displayed in the Exporters list.

Intermapper Flows Settings

You can use the Flows Settings window to view and edit settings for Intermapper Flows.

To open the Flows Settings window:

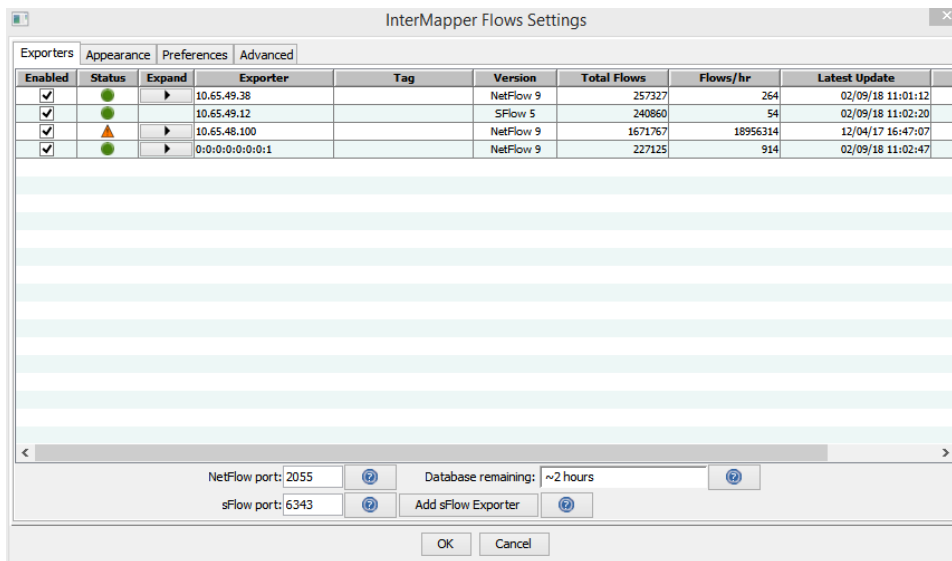
Click the **Settings** icon in the top-right corner of the **Flows** window.

The following tabs are available in the Settings window:

- **Exporters** - to select which exporters you want to collect from.
- **Appearance** - to select a coloring theme for protocols and hosts.
- **Preferences** - to set parameters that control behavior of Intermapper Flows.
- **Advanced** - to set performance-related parameters, the path to your database, and a database size.

Exporters tab

You can use the Exporters tab to select the exporters from which you want to collect data.



Selecting and Adding Exporters

The Exporters tab lists all available exporters.

To select exporters:

- Select or clear the **Enabled** check box to enable or disable collection and analysis of data from an exporter.

NOTE: NetFlow exporters are displayed in the list automatically if they are properly configured. The exporter must be configured to send data to Intermapper Flows.

- Click **Add sFlow Exporter** to add an sFlow exporter. The Enter sFlow Information window appears as shown below. Enter information about the exporter, then click OK. Intermapper Flows sends SNMP commands to the exporter to turn on sFlow.

Enter sFlow Information

InterMapper Flows can add itself as a destination for your sFlow-capable device. It needs the following SNMPv2 information:

sFlow Exporter/Switch Address: 192.168.100.100

SNMP Read/Write Community String: public

sFlow Destination: 192.168.1.127

Desired Flow Rate (1 per N packets): 512

OK Cancel

Do the following:

- **sFlow Exporter/Switch Address** - enter the address of an SNMPv2-capable sFlow exporter.
- **SNMP Read/Write Community String** - enter the community string for the exporter.
- **sFlow Destination** - the address of the Intermapper Flows collector. Your server might have multiple network devices, each with its own IP address. Intermapper Flows makes its best determination as to which IP address should be listed as your sFlow collector, but it can guess incorrectly. If the exporter is not registered correctly, try a different IP address.
- **Desired Flow Rate (1 per N packets)** - ask the exporter to send an sFlow update every **N** packets. The exporter may not be able to honor this request, so Intermapper Flows keeps track of the actual update rate as well.

Additional Columns

- **Expand** - click the right arrow to expand an exporter to view information for all available interfaces. Click the down arrow to collapse the exporter's interface lines.
- **Tag** - double-click to edit the tag for any exporter or interface. Tags are displayed in the Exporter/Interface menu in the Flows window. Intermapper Flows fills in these tags, if available, from every device.
- **Version** - the NetFlow or sFlow version used by the exporter.
- **Total Flows** - the total number of Flow records exported.
- **Flows/hr** - the average flows-per-hour from this exporter.
- **Latest Update** - the date and time of the last update from this exporter.
- **First Report** - the date and time of the first report from this exporter.

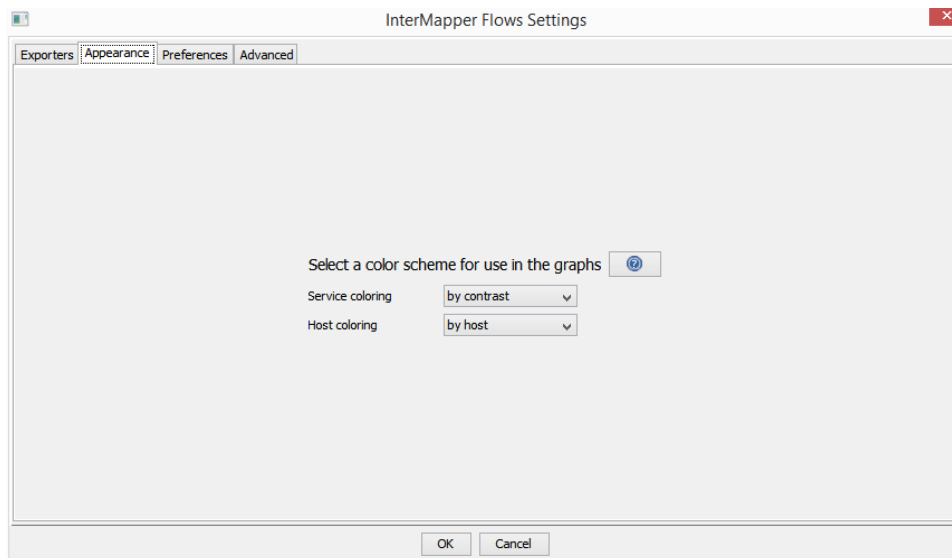
Additional Boxes

- **NetFlow port** - Intermapper Flows listens for NetFlow v1, v5, v7, and v9 on this port. 2055 is the default port, but ports 9555 and 9995 are sometimes used.

- **Database remaining** - each exporter has an estimated flow rate, updated the last time it reported. The combined rate is used to calculate an estimated database capacity.
- **sFlow port** - InterMapper Flows listens for sFlow on this port. The default port is 6343. This must be different from the NetFlow port. Make sure that this port is not firewalled from any of your exporters.
- **Add sFlow Exporter button** - click this button to add an sFlow exporter. The Enter sFlow Information window appears.

Appearance Tab

You can use the Appearance tab to select a coloring scheme for charts in the Flows window.



To select a color scheme:

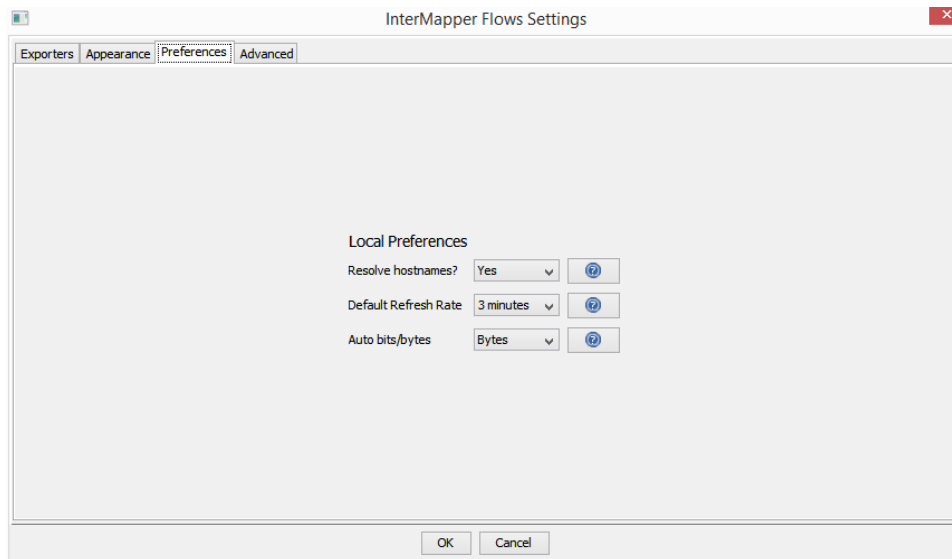
- **Service coloring** - select a scheme to use for Services.
- **Host coloring** - select a scheme to use for Hosts.

The following color scheme strategies are used for charts and graphs:

- **By port or host** - colors are fixed for each port or host. This means the color for a port or host is the same in every chart when that port or host is displayed. Because of the limited number of colors, it is possible for two adjacent hosts in a chart to have the same color.
- **By contrast** - chart colors are assigned in the same order for each chart. This provides greater contrast, but a single host or port might be colored differently in each chart or in the same chart at different times.

Preferences Tab

You can use the Preferences Tab to set local preferences for Intermapper Flows.

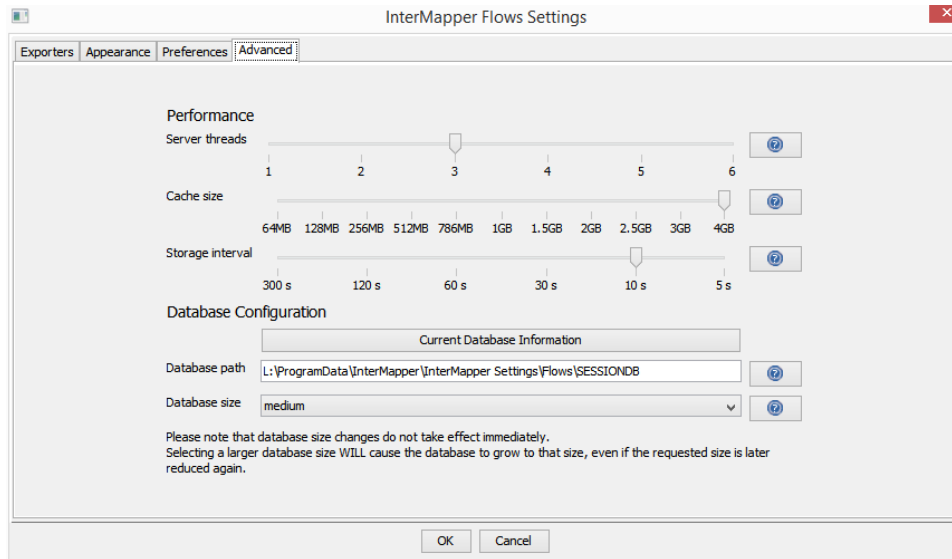


Local Preferences

- **Resolve hostnames?** - click **Yes** to resolve IP addresses to show host names. Click **No** to display only IP addresses. This can improve performance and security.
- **Default Refresh Rate** - select a default refresh rate for a new Flows window. To override this setting in any Flows window, select a different refresh rate from the Auto-update menu.
- **Auto bits/bytes** - select a default display setting of **Bits** or **Bytes** for any new Flows window. To override this setting, select a different setting from the Graph Scale menu in the upper left of the Stack Chart.

Advanced tab

You can use the Advanced tab to set performance- and database-related parameters.



Performance Settings

- **Server threads** - the number of available query threads to start. In practice, this number can be small. It is the number of concurrent requests that InterMapper Flows handles without queuing requests. A good rule of thumb for this value is the number of processors in the server, plus 1. For example, a quad-core server might use 5 threads.
- **Cache size** - the size of the memory session cache. Session records are written to disk regularly, but to speed up queries (for graphs and tables), some are cached in memory. It is safe to set this close to the memory capacity of the server.

NOTE: - Larger values for the session cache increases server startup and restart times as records are loaded from disk. A cache larger than 1.5Gb requires a 64-bit processor.

- **Storage interval** - the number of seconds between disk commits. Committing more often can decrease performance by using physical media more often. Committing less often requires more session cache to avoid losing data.

Database Configuration Settings

- **Database path** - the path to an existing directory. The server must have read and write access to this directory.

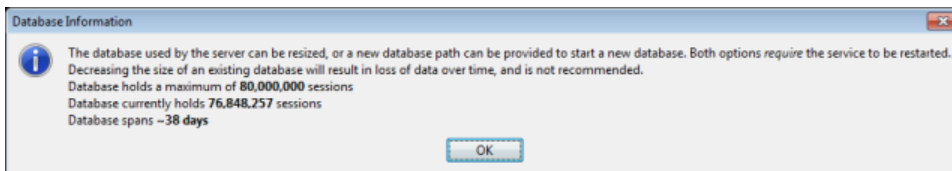
NOTE: If you change the database path, the existing database is not copied to the new location, however, you can do this manually while the service is not running. The old database is not deleted.

- **Database size** - available sizes as shown below (calculated from the current flow rate):

Size	# Session Records	Size on disk
tiny	3000	~400 KB
small	~8 million	~1000 MB
medium	80 million	~10 GB
large	800 million	~100 GB
very large	2 billion	~256 GB

NOTE: Resizing a database can be a gradual process. Growing a database allocates more space for session records, while shrinking a database takes longer, as records are cropped over time.

- **Current Database Information** - shows the maximum size of the database, the number of records in the database, and the number of days when those records are collected.



Using the Layer 2 View

Overview

You can use the Layer 2 view of the Device List window to view information about your switches and what is connected to them. With the Layer 2 view, you can answer the following questions:

- What switch port is this computer connected to?
- What computers are connected to that switch port?
- How are these two switches connected?

NOTE: Layer 2 features are experimental.

What Layer 2 Processing Does

Intermapper periodically scans all switches on maps where Layer 2 is enabled (see the [Layer 2 pane](#) of the Map Settings window). It collects information on which devices are attached to which ports, what other switches are present, and places the resulting information into the Endpoints pane.

Intermapper Layer 2 uses device MAC addresses to identify devices. It looks through the forwarding databases of the switches to identify the ports where devices connect. The Layer 2 process also looks through ARP tables and other sources of data to map the MAC addresses to IP addresses, to collect DNS names, VLANs, and other information, locating each device as precisely as it can.

When Layer 2 passes the connection information back to the map, automatically showing the connection of each device on the map to the proper port on the switch.

To use Intermapper's Layer 2 scanning:

1. In the **Server Settings** window, enable [Layer 2 scanning](#).
2. Enable [Layer 2](#) in the [Map Settings window](#) or in the [Layer 2-Enabled Maps window](#) (available in the **Server Settings** > **Layer 2** pane for any map containing switches you want to include during Layer 2 scanning).

To use the Layer 2 connection information to make connections on the map automatically, select **Enable Layer 2 scan for this map** from the Layer 2 pane of the Map Settings window.



NOTE: The Layer 2 View is disabled when the following occurs:

- Layer 2 scanning not enabled in the Server Settings > Layer 2 window.
- The scanning is enabled, but the user is not an administrator.
- The scanning is enabled, but the user is not an administrator and not a member of the **FullLayer2Access** group. (A member of this group can access the Layer 2 View without having other administrator privileges. The group is not created automatically; you must create it and add users to it.)

Viewing Layer 2 Information

Layer 2 information is shown in a sub-view of the global Device List Window, available from the Window menu.

To open the Layer 2 view:

1. From the **Window** menu, select **Device List**. The Device List window is displayed. 
2. From the **Device List** window, click . The Layer 2 window is displayed.

Alternatively, do the following:

- Right-click a device on a map and click **Show in > Layer 2** from the **Context** menu.
- Select a device on a map and click **Show in > Layer 2** from the **Monitor** menu.

NOTE: The Show in > Layer 2 command is available only when Layer 2 scanning is enabled for the map.

Using the Layer 2 View

Overview

You can use the Layer 2 view of the Device List window to view information about your switches and what is connected to them. With the Layer 2 view, you can answer the following questions:

- What switch port is this computer connected to?
- What computers are connected to that switch port?
- How are these two switches connected?

NOTE: Layer 2 features are experimental.

What Layer 2 Processing Does

Intermapper periodically scans all switches on maps where Layer 2 is enabled (see the [Layer 2 pane](#) of the Map Settings window). It collects information on which devices are attached to which ports, what other switches are present, and places the resulting information into the Endpoints pane.

Intermapper Layer 2 uses device MAC addresses to identify devices. It looks through the forwarding databases of the switches to identify the ports where devices connect. The Layer 2 process also looks through ARP tables and other sources of data to map the MAC addresses to IP addresses, to collect DNS names, VLANs, and other information, locating each device as precisely as it can.

When Layer 2 passes the connection information back to the map, automatically showing the connection of each device on the map to the proper port on the switch.

To use Intermapper's Layer 2 scanning:

1. In the **Server Settings** window, enable [Layer 2 scanning](#).
2. Enable [Layer 2](#) in the [Map Settings window](#) or in the [Layer 2-Enabled Maps window](#) (available in the **Server Settings** > **Layer 2** pane for any map containing switches you want to include during Layer 2 scanning).

To use the Layer 2 connection information to make connections on the map automatically, select **Enable Layer 2 scan for this map** from the Layer 2 pane of the Map Settings window.


NOTE: The Layer 2 View is disabled when the following occurs:

- Layer 2 scanning not enabled in the Server Settings > Layer 2 window.
- The scanning is enabled, but the user is not an administrator.
- The scanning is enabled, but the user is not an administrator and not a member of the **FullLayer2Access** group. (A member of this group can access the Layer 2 View without having other administrator privileges. The group is not created automatically; you must create it and add users to it.)

Viewing Layer 2 Information

Layer 2 information is shown in a sub-view of the global Device List Window, available from the Window menu.

To open the Layer 2 view:

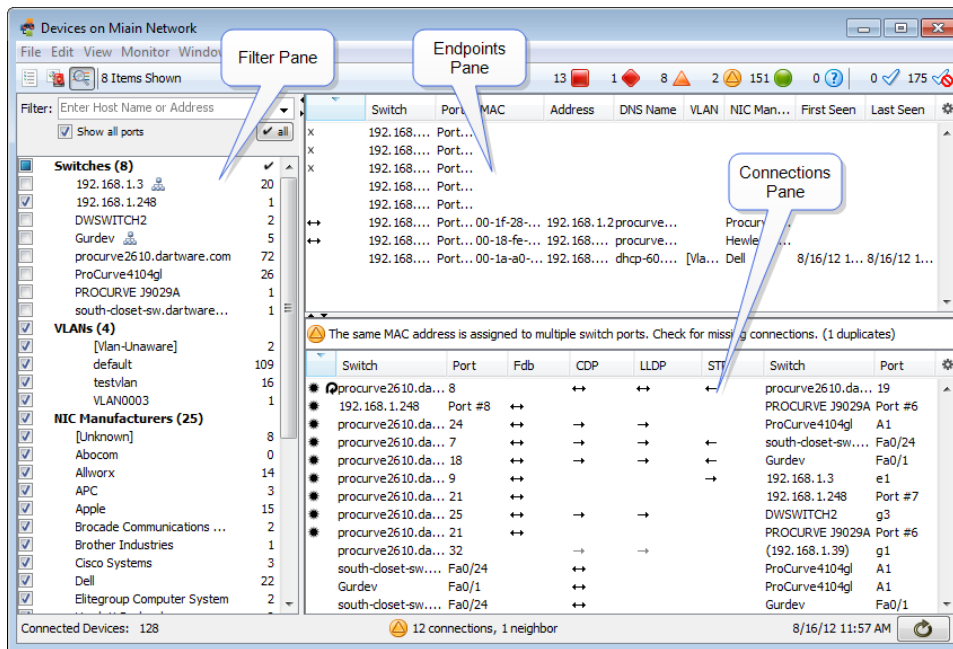
1. From the **Window** menu, select **Device List**. The Device List window is displayed.
2. From the **Device List** window, click . The Layer 2 window is displayed.

Alternatively, do the following:

- Right-click a device on a map and click **Show in > Layer 2** from the **Context** menu.
- Select a device on a map and click **Show in > Layer 2** from the **Monitor** menu.

NOTE: The Show in > Layer 2 command is available only when Layer 2 scanning is enabled for the map.

Layer 2 View



The Layer 2 View contains the following panes:

- **Endpoints pane** - the upper-right pane lists all switch ports and the devices connected to them. It contains only those ports and devices that match the filter criteria in the Filter pane.
- **Filter pane** - the left pane provides criteria for showing or hiding endpoints based on their presence on a particular switch, VLAN, or the endpoint's manufacturer. It also lists available switches, the VLANs in which they appear, and manufacturers of network interface cards of the devices connected to them. Use the check boxes to select or hide endpoints in the Endpoints pane and type additional criteria to help select the endpoints to view.
- **Connections pane** - the lower-right pane provides details about switch-to-switch connections.

Filter Pane

You can use the Filter pane to limit the endpoints you want to view in the Endpoints pane. Select a combination of switch, VLAN, and NIC Manufacturer to select the devices you want to view.

The **Switches** section lists each switch by name, and shows the number of endpoints attached to that switch.

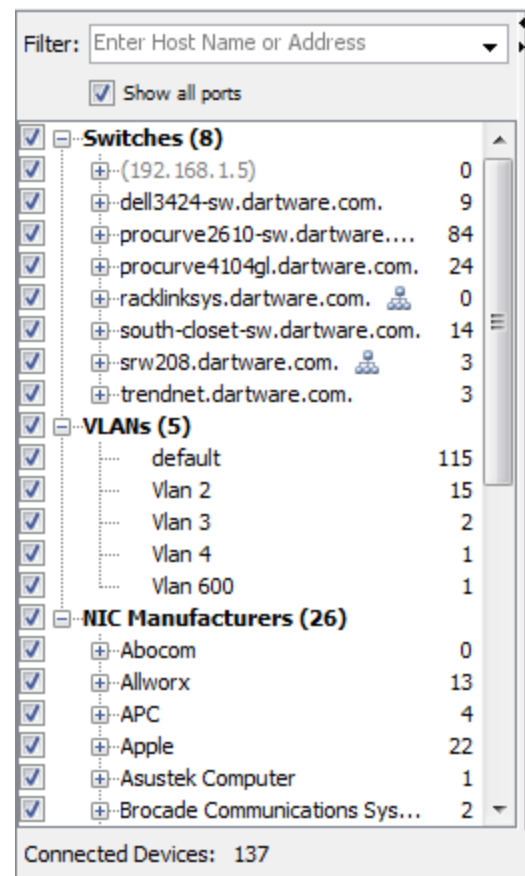
The **VLANs** section lists all VLANs and the number of endpoints on each.

The **NIC Manufacturers** section lists all unique NIC Manufacturers connected to devices.

The right column of the Filter Pane shows a count of endpoints present for each of the criteria. See [Understanding Endpoint Counts](#) for more information.

You can use the following methods to control the filter criteria:

- By default, all check boxes are selected.
- Select or clear check boxes to get the combination of switch, VLAN, and NIC Manufacturer that matches the devices you want to view.
- Double-click a check box to select it and clear all other check boxes in the section.
- Expand the Switch tree to view and select switch ports.
- Right-click a switch and select **Remove switch from Layer 2 database** to prevent the switch from being polled for Layer 2 information. This is equivalent to the **Poll this address for Layer 2 information** check box, available in the [Set Behavior window](#).
- Expand the VLANs tree to view and select VLANs.
- Expand the NIC Manufacturer tree to view and select NIC models from those available.
- Select or clear the **Show all ports** check box to show or hide the ports in the Endpoints pane to which nothing is connected.
- Use the Filter Control (see below) for additional control of the set of rows that are displayed in the Endpoints pane.
- The Filter box provides significant additional filtering capability. In the **Filter box**, enter a hostname or address to limit the devices shown in the Endpoints pane. For more information on the options, see [Using the Filter Box](#).






- Certain flags are displayed next to entries. For more information, see [Understanding Layer 2 Flags](#).
- A switch that appears in grey and in parentheses indicates that the switch was previously detected, but is no longer on a Layer 2-enabled map.

Endpoint Counts

The right column of the Filter pane shows the number of Endpoint devices (specifically, the number of distinct MAC addresses) for each of the filter criteria.

- An SNMP-enabled managed switch or hub is displayed as zero endpoints since it is not considered an endpoint.
- A single endpoint (host, workstation, server, router, and so on) shows as one endpoint.
- If an unmanaged hub or switch is present, or if the switch is not present on a Layer 2-enabled map, the endpoint count reflects the number of endpoints detected that are out of that port. In some cases, this can be a very large number of endpoints.

The number of endpoints indicated in the Filters panel often exceeds the number of entries in the Endpoints pane. This discrepancy occurs because the Endpoints panel often displays multiple entries for the same MAC address. Multiple entries are displayed in the following cases:

- **Multi-homed devices** - devices with multiple IP addresses that use a single MAC address. 
- **Interior devices** - devices attached to an unmanaged switch or hub that are placed between two managed switches. Intermapper's Layer 2 algorithm cannot show the correct switch port (because it is unmanaged), so it indicates the device as an interior device, meaning the device is between two managed switches. Interior devices are indicated with left or right arrows as shown at right.  

When you select the **Show All Ports** check box, the Endpoints pane also shows the following:

- All ports, whether a device is connected or not.
- Ports that are connected to other switches. (Normally these are hidden because switches are not considered endpoints.)
- Fuzzy devices (any device whose connection point cannot be completely determined).

For more information, see [Understanding Layer 2 Flags](#).

Using the Filter Box

You can use the Filter box, located at the top of the Device Filter pane, to limit the devices you see in the Endpoints pane.

- Enter a host name or address to view only devices connected to that domain or address.
- From the Filter menu, select or clear the **Endpoints Only** check box to include or exclude entries for ports with switches, unknown devices, and devices identified as fuzzy. For more information, see [Understanding Fuzzy Devices](#).
- From the Map or List view, select a device, and click **in Layer 2** from the **Show** submenu, available from the **Monitor** menu and the **Context** menu, to view that device's connections in the Layer 2 View.
- If the value is in double quotation marks (""), list all endpoints where the value is part of the NIC Manufacturer. For example, App matches Apple, Appliance, and so on.
- If the value is an IPv4 CIDR block, list all endpoints with IP addresses in that CIDR block. (For example, enter 192.168.1.1/24.)
- If the value is decimal digits separated by periods, or just digits, treat it as an IPv4 address. For example,
 - **192.168** matches any IP address that begins with 192.168.
 - **.1** matches any IP address that ends with .1.
 - **10** matches any IP address that begins with 10. (no period necessary).
- If the value is hexadecimal and separated by dashes, treat it as a MAC address. Search for endpoints with the MAC address or MAC address substring. For example, 00-00-0c, 00-00-d7-00-10-ab, and so on.
- If the value starts with an alphabetic character, resolve the host name to an IPv4 address and filter on that IP address.
- If the value starts with a pound sign (#), process the specified debug command. For example, #help.

Endpoints Pane

The Layer 2 view's Endpoints pane lists all endpoint devices (servers, workstations, and routers) and the switch ports they are connected to. It does not include managed switches, which are not considered to be endpoints.

The following columns are available in the Endpoints pane:

- **Flags** - provides detailed information about the port or device. For more information, see [Layer 2 Flags](#).
- **Switch and Port** - describes a particular switch port
- **MAC and Address** - the MAC address and the IP Address of the device.
- **DNS** - the DNS name of the device (if known).
- **VLAN** - the VLAN(s) supported by this port.
- **NIC Manufacturer** - the manufacturer of the Network Interface Card (NIC), derived from the MAC address.
- **First Seen** - the time the device was first detected during a Layer 2 scan.
- **Last Seen** - the most recent time the device was detected during a Layer 2 scan.
- **Present** - two numbers, separated by a forward slash (/). The first is the number of times this device was visible during a scan, the second is the total number of scans.
- **ifAlias** - the ifAlias taken from the Switch and Port (if available).

	Switch ^	Port	MAC	Address	DNS Name	VLAN	NIC ...	First Seen	Last Seen	
↔	procurve4104gl.dartware.com.	A1	00-12-0e-...	192.168.1....	trendnet...		Abocom			
🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.63	dhcp-63.d...	Vlan 600	Apple	10/20/11 ...	10/20/11 ...	
🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.63	dhcp-63.d...	default	Apple	10/20/11 ...	10/20/11 ...	
🏠	procurve4104gl.dartware.com.	D9	00-50-56-...			default	VMware	7/25/11 6...	7/25/11 1...	
🏠	procurve4104gl.dartware.com.	B10	00-50-56-...	192.168.1....	dhcp-122...	default	VMware	10/19/11 ...	10/19/11 ...	
🔴🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.68	dhcp-68.d...	Vlan 600	Apple	10/20/11 ...	10/20/11 ...	
🔴🏠	procurve4104gl.dartware.com.	D1	00-25-4b-...	192.168.1.68	dhcp-68.d...	default	Apple	10/20/11 ...	10/20/11 ...	
	procurve4104gl.dartware.com.	D18	00-50-56-...	192.168.1....	dhcp-118...	default	VMware	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D7	00-50-56-...	192.168.1....	solaris.dar...	default	VMware	7/22/11 6...	10/20/11 ...	
	procurve4104gl.dartware.com.	D2	00-50-56-...	192.168.1....	aurorax-s...	default	VMware	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-17-f2-0...	192.168.1....	cswmac.d...	default	Apple	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-11-11-...	192.168.1....	cswvmwar...	default	Intel	6/24/11 2...	10/20/11 ...	
	procurve4104gl.dartware.com.	D1	00-0c-29-...	192.168.1....	csw2k8...	default	VMware	8/16/11 4...	10/20/11 ...	
	procurve4104gl.dartware.com.	B17	00-50-56-...	192.168.1....	supportw2...	default	VMware	7/22/11 6...	10/20/11 ...	
	procurve4104gl.dartware.com.	B14	00-0c-29-f...	192.168.1....	aurora-ms...	default	VMware	6/24/11 2...	10/20/11 ...	

Controlling What You See in the Endpoints Pane

- From the **Filter** pane, click various combinations of Switch, VLAN, and NIC Manufacture to control the rows that are in the **Endpoints** pane.
- From the **Endpoints** pane, click a column heading to sort by that column. Click again to reverse the sort.
- Click the sprocket at the right end of the **Endpoints** pane's column heading bar to add to or remove columns from the **Endpoints** pane.
- By default, the **Endpoints** pane shows endpoints only, meaning it hides ports connected to other switches, ports with no devices attached (regardless of whether they are up or down), or devices marked as fuzzy. Select the **Show All Ports** check box near the top of the [Filter pane](#) to show all ports.

Using Layer 2 Information to Update Map Connections

In addition to this tabular view, Intermapper can pass connection information back into the Map view, automatically showing the connection of each device on the map to the proper port on the switch. This simplifies the creation and arrangement of your maps; all you need to do is tidy up the map. You can enable this feature from the Layer 2 Features pane of the [Map Settings](#) window.

Connections Pane

The Layer 2 Connections pane lists all switches, the switches they are connected to, and the ports through which they are connected. This information is derived from the switch's forwarding tables, as well as information available through Cisco Delivery Protocol (CDP), Link Layer Delivery Protocol (LLDP), and Spanning Tree Protocol (STP).

Switch	Port	VLAN	Fdb	CDP	LLDP	STP	Switch	Port
* procurve2610-sw.dart...	7	default	↔	→	→	←	south-closet-sw.dar...	Fa0/24
* procurve2610-sw.dart...	8			↔	↔	←	procurve2610-sw.d...	19
* procurve2610-sw.dart...	9	default	↔			←	dell3424-sw.dartwar...	e1
procurve2610-sw.dart...	9			→	→		procurve4104gl.dart...	A1
procurve2610-sw.dart...	18			→	→		(192.168.1.35)	Fa0/1
* procurve2610-sw.dart...	28	default	↔				srw208.dartware.com.	e6
* dell3424-sw.dartware....	e4	default	↔				procurve4104gl.dart...	A1

Connections Pane Columns

- **Switch and Port** - each row displays two switches and two ports. These switches are known to be connected by the specified ports.
- **VLAN** - the VLAN(s) that are present on the connection between the switches.
- **Fdb** - (Forwarding database)
 - A **two-headed arrow** means that both switches' forwarding databases have entries for each other.
 - A **single-headed arrow** points toward the switch that is in the other switch's Fdb. There is no corresponding entry in the reverse direction.
- **CDP and LLDP** - (Cisco Discovery Protocol and Link Layer Discovery Protocol)
 - A **two-headed arrow** indicates that both switches hear the other's protocol advertisements.
 - A **single-headed arrow** points to the switch that receives the protocol advertisements from the other.

NOTE: Some CDP/LLDP-aware switches can turn off advertisements on certain ports. This affects the arrows.

- **STP** - (Spanning Tree Protocol)
 - A **single-headed arrow** points away from the root of the spanning tree.
 - A **two-headed arrow** indicates that the path for some spanning trees (such as certain VLANs) goes one way, while the path for other spanning trees goes the other way. If there are loops between these two switches, the port closest to the root may be in a blocking state.

Using the Connections Pane











- Click a column heading to sort by that column. Click again to reverse the sort.
- Click the sprocket icon to the right of the column heading bar to select which the columns are displayed in the list.







Layer 2 Flags

The meanings of flags in the Layer 2 view depend the pane in which they appear.

Flags in Device Filter and Endpoints Panes









In the Filter and Endpoints panes, flags indicate the following:

	Switch-to-Switch connection - connected to another switch
 or 	Interior device - the device is attached to a hub or switch that is connected between ports of two managed switches. The left or right arrow points away from the spanning tree root.
	Down - this port is not operating.
	Multi-homed device - a single MAC address has multiple IP addresses. Each IP addresses is shown as a separate row in the Endpoints pane.
	Ghost - indicates that the port is not active, and the endpoint (device with this MAC address) has not been seen elsewhere in the network. It was last seen on the indicated switch port.
	Not present on Map - indicates that the port is connected to a managed switch, but that switch is not present on a Layer 2-enabled map.
 or  or 	Fuzzy - the Layer 2 process cannot determine the exact port where the device is attached. See Understanding Fuzzy Devices below.



	Duplicate MAC address detected - the Layer 2 process has found the same MAC address on two separate switch ports.
	IP conflict - the Layer 2 process has found the same IP address on two separate switch ports.
	Spanning tree root - this switch is the root of the spanning tree.
	Loop - a port is connected to another port on the same switch.
	Wireless (assigned manually) - a port or VLAN is tagged as Wireless. The Wireless flag is displayed next to the port in the Filters and Endpoints panes. For more information, see Manual Tagging .
	Virtual machine (assigned manually) - all NICs from this manufacturer with this OUI (organizationally unique identifier) are virtual machines. The Virtual Machine flag is displayed next to the OUI and any endpoints that use NICs with that OUI. For more information, see Manual Tagging .

Flags in the Connections Pane

The following flags might be present in the Flags column of the Connections pane:

	Confirmed connection - specifies that a connection is confirmed and will be exported to a map.
	Not present on Map - specifies that the port is connected to a device that is not present on a Layer 2-enabled map.
	Loop - specifies that a direct port-to-port connection on this switch.
	specifies that both ends see each other's CDP/LLDP advertisements.
	the left end of the connection sees the right end's CDP/LLDP advertisements.
	the right end of the connection sees the left end's CDP/LLDP advertisements.
	connected to a device that is not present on any map.
	confirmed connection specifies that a connection is confirmed and will be exported to a map.

STP column: In the STP column of the Connections Pane, arrows indicate the direction of travel of STP bridge information.

	Right switch is the left switch's path to root for one or more of the left switch's spanning trees. (Right switch's port might be in blocking state, if there are loops.)
	Left switch is the right switch's path to root for one or more of the right switches' spanning trees. (Left switch's port might be in blocking state, if there are loops.)



Right switch is left switch's path to root for one or more spanning trees and left switch is right switch's path to root for other spanning trees. (Either switch's port may be in blocking state for one or more spanning trees, if there are loops.)

Fuzzy Devices

A device with a MAC address whose location in the Layer 2 topology cannot be completely determined is considered to be a fuzzy device by Intermapper.

Fuzzy devices are quite common and can occur for a number of reasons. The Layer 2 engine attempts to collect information from all the switches nearly simultaneously. However, some time can elapse between the times that two switches finishes collecting Layer 2 information. During this time period, a MAC address collected from one switch can age out of another switch. Alternatively, a device can connect to the network during Layer 2 collection, so its MAC address is reported in one switch's forwarding tables, but not in the edge switch (due to the difference in scan times for the two switches).



Devices can also be classified as fuzzy due to bugs in certain switch models. For example, Fortra has a small managed desktop switch that doesn't report its complete forwarding table via SNMP. The extra un-reported devices are displayed as fuzzy, because the upstream switch reports the MAC address, but the downstream switch never reports them (even though the switch is otherwise perfectly functional).

Fuzzy devices are distinct from Interior devices. A fuzzy device appears to be in the middle of the network (between two switches) because Intermapper does not have complete information. An interior device appears to be in the middle of the network because there is actually another switch or hub located there, but it is not part of the Layer 2 information.

Manual Tagging

For certain kinds of connections, you can tag a port or endpoint device so you can see easily what kind of device it is.

The following tagging options are available:

	<p>Wireless (assigned manually) - right-click a switch port or VLAN in the Filters pane and select as Wireless from the Tag submenu. The Wireless icon is displayed next to the port or VLAN.</p>
	<p>Virtual machine (assigned manually) - right-click a port in the NIC manufacturer's section of the Filters pane (one that is associated with a virtual machine) and select as Virtual Machine from the Tag submenu. The Virtual Machine icon is displayed next to the OUI and any endpoints that use NICs with that OUI.</p>

Mapping with Layer 2

You can use Layer 2 to create maps that accurately reflect your network's topology.

Converting an Existing Map to Use Layer 2

For maps with a relatively small number of devices, you can convert the map directly so that it uses Layer 2 to configure the map. You can also create a new map and use Layer 2 information to add the switches and devices.

To convert an existing map to Layer 2:

1. Open the map you want to convert and make it editable.
2. From the **Map Settings** window's **Layer 2** pane, select the **Enable Layer 2 scan for this map** check box.
3. From the **Window** menu, click **Device List** and select **Layer 2** from the **View** menu or click the **Layer 2 View** icon. The Layer 2 window is displayed, showing your available Layer 2 devices.
4. From the **Layer 2** view, click **Scan** at the lower right corner of the window.
5. From the **Map Settings** window's **Layer 2** pane, click **Change Now**. Any Layer 2 connections are broken and reconnected using Layer 2 information.
6. Select all devices and click **Organic** from the **Format** menu's **Arrange** submenu. The map now uses Layer 2 information to connect the devices on the map.

To create a new map using Layer 2 information:

1. Create a new empty map and make it editable.
2. From the **Window** menu, click **Device List** and select **Layer 2** from the **View** menu or click the **Layer 2 View** icon. The Layer 2 window is displayed, showing your available Layer 2 devices.
3. From the **Layer 2** view, click **Scan** at the lower right corner of the window.
4. From the **Connections** pane, select the lines for the switches you want to map and select **Copy** from the **Edit** menu.
5. Paste into your new map. The switches are displayed on your map.
6. From the **Map Settings** window's **Layer 2** pane, select the **Enable Layer 2 scan for this map** check box.
7. Click **Change Now**. The switches on the map are connected as defined by Layer 2 information. This represents your network's switch backbone.
8. From the **Layer 2** window's **Endpoints** pane, select all endpoints, copy them, and paste them into your map.
9. From the **Map Settings** window's **Layer 2** pane, click **Change Now**. The devices are connected as defined by Layer 2 information.

10. Although optional, you might find it helpful to select all devices and select **Organic** from the **Format** menu's **Arrange** submenu.

NOTE: Layer 2 mapping can display only information returned from a Layer 2 scan. For example, if a switch's `dot1dTpFdbTable` (BRIDGE-MIB) is missing or sparsely populated, the Layer 2 scan can fail to return the connections, so they cannot be shown.

Intermapper Reports

You can use the Intermapper Reports server to create, view, print and save reports that use data collected from Intermapper servers.

Intermapper Reports is a module of [Intermapper DataCenter](#). Use your favorite browser to use Intermapper Reports to create your reports.

NOTE:

Before you can use it, you must start the Intermapper Reports server. This allows Intermapper to send data to the Reports server where it is collected in a database.

To start collecting data:

1. From the **Server Settings** window, select **Reports Server**. The Reports Server pane is displayed.
2. From the **Reports Server** pane, click **Start**. The Configure button becomes active.

To view the Reports Server interface:

From any Intermapper map, right-click a device and select **Reports** from the **Show in** submenu. A browser page launches and the Intermapper Reports window is displayed.

Intermapper Reports

You can use the Intermapper Reports server to create, view, print and save reports that use data collected from Intermapper servers.

Intermapper Reports is a module of [Intermapper DataCenter](#). Use your favorite browser to use Intermapper Reports to create your reports.

NOTE:

Before you can use it, you must start the Intermapper Reports server. This allows Intermapper to send data to the Reports server where it is collected in a database.

To start collecting data:

1. From the **Server Settings** window, select **Reports Server**. The Reports Server pane is displayed.
2. From the **Reports Server** pane, click **Start**. The Configure button becomes active.

To view the Reports Server interface:

From any Intermapper map, right-click a device and select **Reports** from the **Show in** submenu. A browser page launches and the Intermapper Reports window is displayed.

Creating a Report

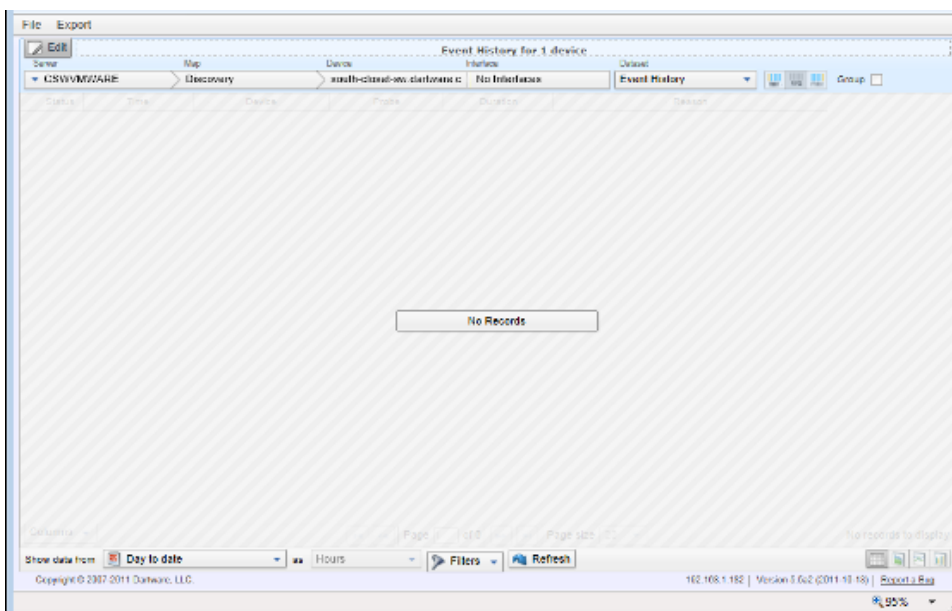
You can use the Reports server web UI to create, save, load, link, or print a report.

You can open the Intermapper Reports window from an Intermapper map.

Opening the Reports Window

To open the Intermapper Reports window:

1. Select a device from an Intermapper map window.
2. Right-click the device and from the **Context** menu and click **Reports**. The Intermapper Reports window is displayed in a new browser window.



You can also open the Reports window by doing one of the following:

- Use the following URL:

`https://[Intermapper Server address]:8182/~imreports/`

- From the **Server Settings** window, view the **Reports Server** pane, click **Configure**, log into the Intermapper DataCenter, and click **View Reports** in the Intermapper **Reports** box.

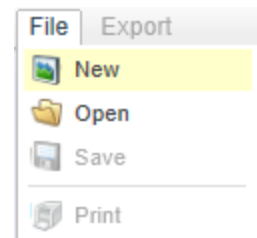
Creating a New Report

You can create a new report in one of the following ways:

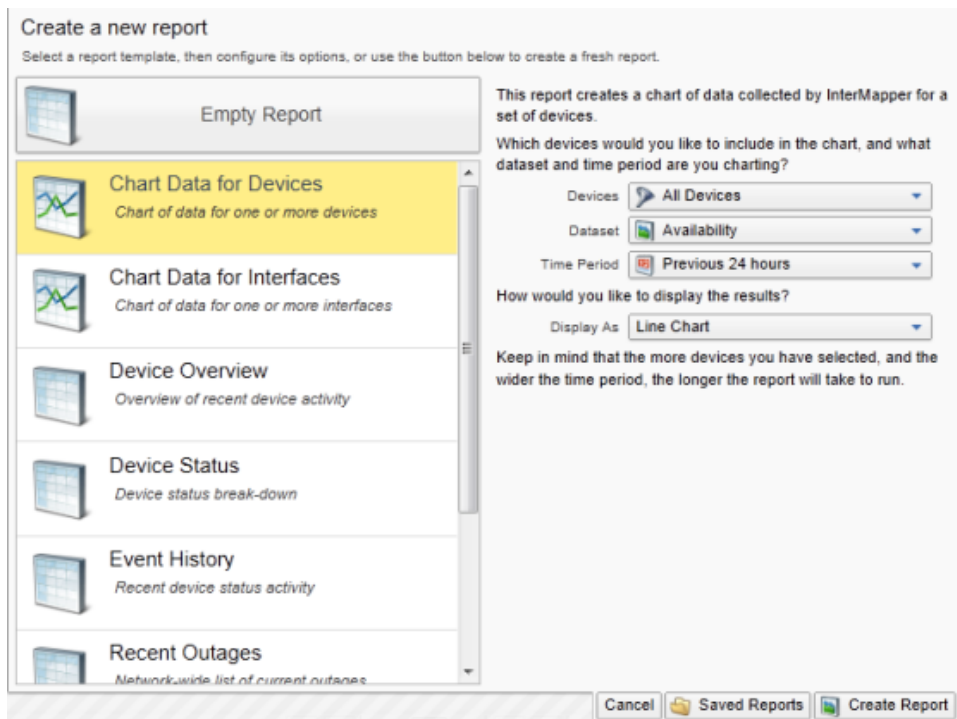
- **From the Map Window** - opens the Reports window after selecting one or more devices or interfaces.
- **From a template** - a number of pre-configured templates are available.
- **From scratch** - using an empty template, select your own devices or interfaces, the data you want to show from each, any calculations you want to apply, a report period and interval, and specify how data is shown.

To create a new report from a template:

1. If you have not stored any reports, you can start with a template.
2. From the **Report** window's **File** menu, select **New**. The Templates list is displayed.
3. Select a template from the left side of the list. A set of parameters for that template is displayed on the right. You can also click **Saved Reports** to view a list of saved reports.
4. Select the template's available parameters.



5. Click **Create Report**. The report loads with the selected parameters.



Report Types

Report templates fall into two general categories:



Graph - can be used with datasets that contain only numeric data. The following display options are available in a Graph report:

- **Area** - a line chart with the area below the line filled
- **Line** - a line chart with a dot at each data point
- **Bar** - a bar chart



Table - a tabular report, containing columns and rows.

To create a new report from the Empty Report template:

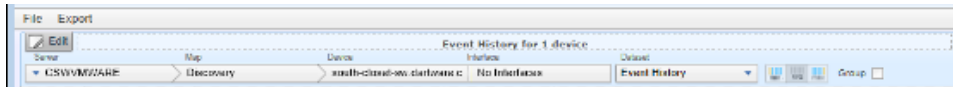
1. If you select the **Empty Report** template, you can create a report from scratch. You can also recall an existing report to use as a starting point.



2. Click **Edit**, located just below the **File** and **Export** menus. The Reports window changes to Edit mode. (The Edit button toggles the report in and out of Edit mode.)

Editing a Report

The following image shows the controls you can use to fine-tune your report definition.



After you enter the Edit mode, you need to answer some or all of the following questions, depending on your requirements for this report:

- **Which devices?** Select the devices (**Servers**, **Maps** and **Devices**) you want to include in the report. If network interface data is available for any of the selected devices, select one or more interfaces.
- **Which data?** Select the datasets. A number of datasets, including Details and Event History, are standard for all devices; other datasets are based on data available from your device selection.

NOTE:

Currently, only one dataset can be included in a report.

- **Calculations?** If you select a Dataset other than Details and Event History (such as Response Time), you can select one of the following basic calculation options:
 - **Min** - shows the only lowest values for the dataset.
 - **Avg** - averages the results (most commonly used).
 - **Max** - shows only the highest values in the dataset.

The Group checkbox allows you to group devices in your selection as one dataset in the results.
- **Period of time?** Select a start date or date range. (Not active when Detail dataset is selected.) For other datasets, common date selections are available. When specifying a date range, the calendar indicates whether data is available from the selected date range (grayed for no data, black for data).
- **Interval?** Specifies data interval, which controls the density of the data over time.

NOTE:

Event History and Details datasets do not use Interval.

- **Report Type?** Specifies how the dataset results are displayed. By default, a Tabular report (list) is shown. When the selected dataset contains numeric values, you can

also select Area, Line, or Bar chart. For Event History and Details, only a tabular view is available.

Additional Report-Editing Features

The following controls are also available to customize your report further:

- Click the **title** to edit it.
- For tabular reports, click a column heading to sort by that column; click again to reverse the sort. The sort order is saved with the report.
- To change the order of tabular report columns, drag a column heading to move the column to the right or left.
- To save the report, click **Save** from the **Report** window's **File** menu, type a report name, and click **Save Report**.

Opening a Saved Report

You can save reports, then open, view, or print them at a later time. For more information, see [Managing and Printing Your Reports](#).

Selecting Source Data

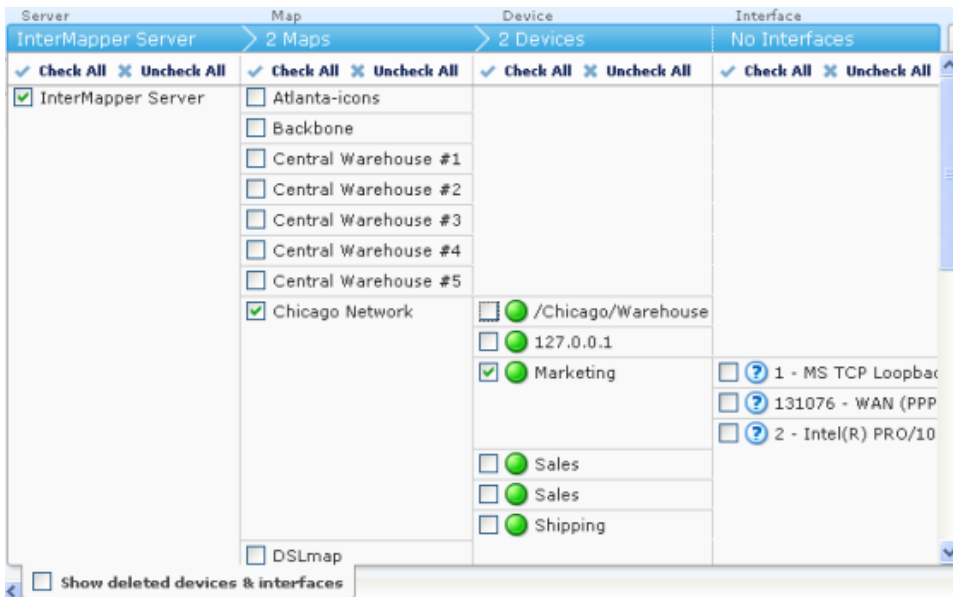
When creating a report, you first need to specify which device or interface data to include in the report.

You can use the data source selection bar to select the devices or interfaces for your report.

Server	Map	Device	Interface
InterMapper Server	scan test	192.168.81.1	No Interfaces

To select data sources:

- Click anywhere in the data source selection bar (shown above). A selection tree is displayed.



- Select or clear the check boxes for the devices or interfaces whose source data you want to include in the report.
- Select the **Show deleted devices & interfaces** check box to include devices or interfaces that have been deleted.
- Click **Select All** or **Unselect All** to select or unselect all devices or interfaces in a column.
- Click the source selection bar. The selection tree is removed and the selected data is displayed.

NOTE:

If you select a large amount of data over a large time range, it can take a few moments or longer for the data to appear. This depends on a number of variables such as the speed of reports server CPU, the amount of data, the time units selected.

Selecting a Dataset

To create graphs, you need to select a dataset that contains numeric values. The datasets available depend on which devices are selected, the probes used to monitor those devices, what datasets are recorded through those probes, and whether those datasets are being exported to the Reports Server database.

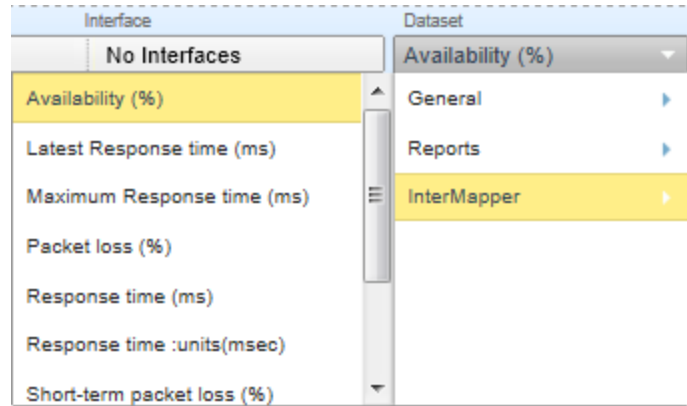
A dataset is available when retention policy for the selected device is not set to **None** and one of the following is true:

- For devices, response time or short-term packet loss are always stored.
- For interfaces, incoming or outgoing bytes/second are always stored.

- If the dataset is specified in the probe to be 'autorecord' .
- If a chart was created from the dataset by clicking it in the Status window or dragging it from the Status window to an existing chart.

To select a dataset:

From the Dataset dropdown menu, near the right of the device selection controls, choose a dataset. Assuming you are still in Table view, a list of values appears.



Selecting Data Grouping



Grouping by Time

In most cases, the selected time scale causes each data point to represent a group of raw samples. Use the data grouping buttons to specify how you want the group of samples represented by a graph data point.

To select data grouping for each time period:

Do one of the following:

- Click **Min** to display the minimum value from the group of samples during a data point's time period.
- Click **Avg** to take the average value from the group of samples during a data point's time period.
- Click **Max** to display the maximum value from the group of samples during a data point's time period.

Grouping by Device or Interface

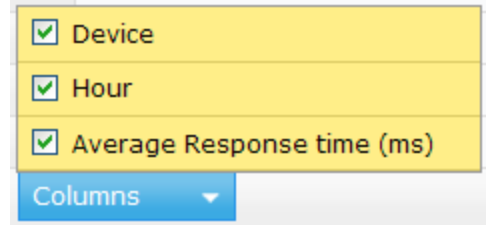
When multiple devices or interfaces are selected, each device or interface's dataset appears as a line or bar on the graph. The Group check box allows you to group the datasets from multiple devices or interfaces into a single dataset that shows the minimum, average or maximum value for all devices in the group over the selected time period.

To view devices or interfaces as one dataset:

Select the **Group** check box.

Selecting Columns (Table view)

In Table view, regardless of the selected dataset, use the Columns selector to select which columns are displayed in the report.



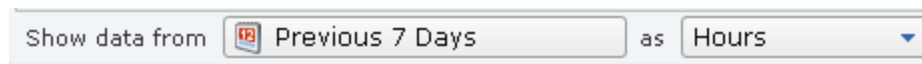
Using the Page Controls



To select the page of data you want to view:

- Click the left and right arrow buttons to move to the start or end of the report or to move to the previous or next page.
- Type a page number to move to that page.
- Use the menu to specify the number of results are shown on a page.

Selecting a Data Range

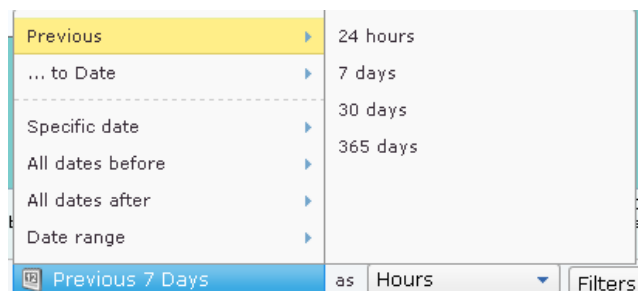


You can limit the amount of data from the dataset that is displayed in the report. Using the **Show Data From** controls at the bottom of the window, select a data range, you select data over a time range and control the density of that data over the specified range. Select a range of data by date and specify the units (hours, days, weeks, months, and so on). For more information, see Data Range Options.

Data Range Options

Previous

Select data from a range of time previous to today.



to Date

Select all data from beginning of the most recent day, week, month, or year.

Time units vary with your selection.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

Day

Week

Month

Year

Previous 7 Days

as

Hours

Filters

Specific date

Select data for a specific date.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

December 2010

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Previous 7 Days

as

Hours

Filter

All dates before

Select all data before the specified date.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

December 2010

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Previous 7 Days

as

Hours

Filter

All dates after

Select all data after the specified date.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

December 2010

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Previous 7 Days

as

Hours

Filter

Date Range

Select data from the specified range of dates.

Previous

... to Date

Specific date

All dates before

All dates after

Date range

December 2010

December 2010

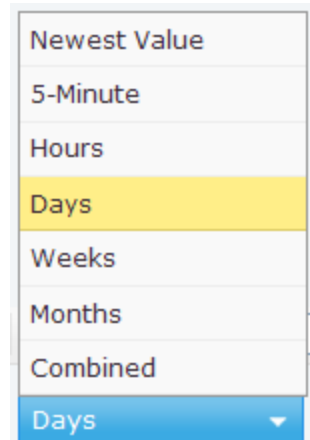
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Previous 7 Days

Specifying Time Units

In addition to selecting a range of data over time, you can specify the units used to display the data.

Selected data units affect the time it takes to display the report. (Displaying data every 5 minutes over a year, for example, represents a large amount of data.)



Creating and Using Data Filters

You can limit the amount of data, or select specific subsets within a dataset, using Filters.

To create a filter:

Click **Filters**. A new filter control is displayed.

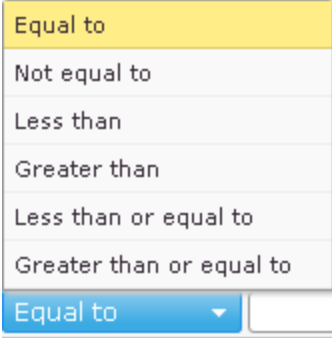
Filter Options

Filters generally have the following parts:

- **Data field** - the default value is Any Field.
- **Comparison operator** - the default value is Matches.
- **Comparison value** - no default value

The available values for comparison operators depend on the type of data field selected. For example,

<p>Data field options</p> <p>Lists all available fields in the dataset.</p>	
<p>Comparison operators (non-numeric fields)</p> <p>When comparing values in non-numeric fields, a Boolean comparison operator is available.</p>	



<p>Comparison operators (numeric fields)</p> <p>When comparing numeric values, a number of comparison operators are available.</p>	 <p>Equal to Not equal to Less than Greater than Less than or equal to Greater than or equal to Equal to</p>
---	--

Multi-Part Filters

You can create filters with more than one set of filter criteria.



The image shows a filter bar with two identical filter criteria. Each criterion consists of a dropdown menu set to 'Any Field', followed by a dropdown menu set to 'Matches', and a text input field. The two criteria are separated by a plus sign icon.

<p>To add a filter to an existing filter set:</p> <p>Click the plus sign.</p>	
<p>To remove a filter from an existing filter set:</p> <p>Click X.</p>	

Selecting a Report Style

The following report styles are available:

- **Table** - a list-style report with rows and columns.
- **Area** - a line chart with the area below the line filled.
- **Line** - a line chart.
- **Bar** - a standard bar chart.

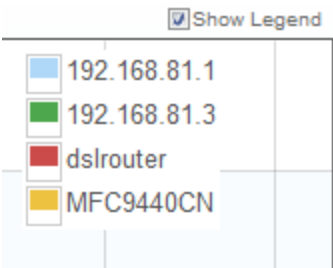
To select a report style:

Click one of the report style tabs in the lower right of the window.

NOTE:
Area, Line, and Bar styles are available only for datasets with numeric values.

Showing or Hiding the Legend

For Area, Line, and Bar styles, select or clear the Show Legend check box to show or hide the legend.



Viewing Data Point Values

In Area, Line, and Bar styles, mouse over a data point to see its value.

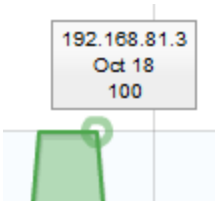


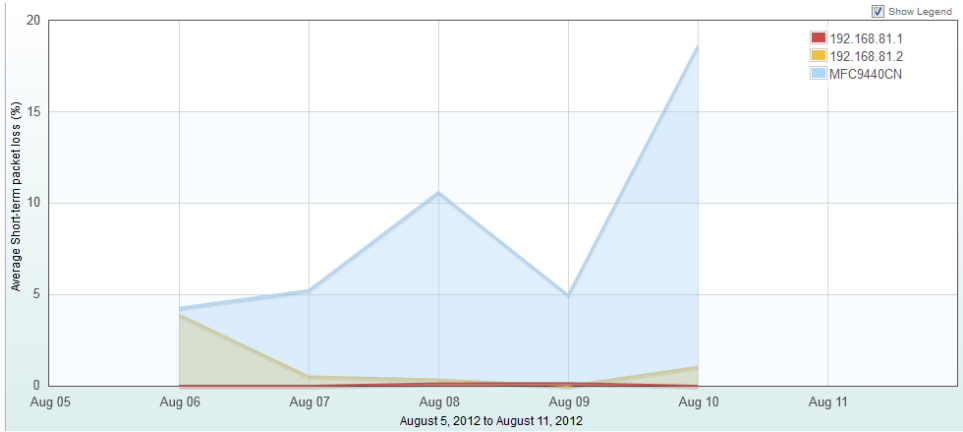
Table Report



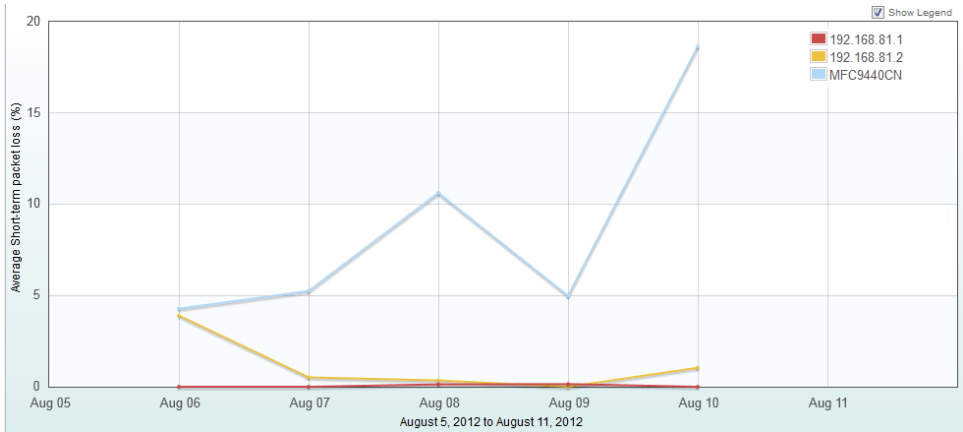
	Map	Device	Days	Average Short-term packet loss (%)
1	My Network	192.168.81.1	2012-08-06 00:00:00	0.00
2	My Network	192.168.81.1	2012-08-07 00:00:00	0.00
3	My Network	192.168.81.1	2012-08-08 00:00:00	0.13
4	My Network	192.168.81.1	2012-08-09 00:00:00	0.15
5	My Network	192.168.81.1	2012-08-10 00:00:00	0.00
6	My Network	192.168.81.2	2012-08-06 00:00:00	3.90
7	My Network	192.168.81.2	2012-08-07 00:00:00	0.52
8	My Network	192.168.81.2	2012-08-08 00:00:00	0.35
9	My Network	192.168.81.2	2012-08-09 00:00:00	0.00
10	My Network	192.168.81.2	2012-08-10 00:00:00	1.04
11	My Network	MFC9440CN	2012-08-06 00:00:00	4.28
12	My Network	MFC9440CN	2012-08-07 00:00:00	5.24
13	My Network	MFC9440CN	2012-08-08 00:00:00	10.62
14	My Network	MFC9440CN	2012-08-09 00:00:00	4.99
15	My Network	MFC9440CN	2012-08-10 00:00:00	18.63

Area Report



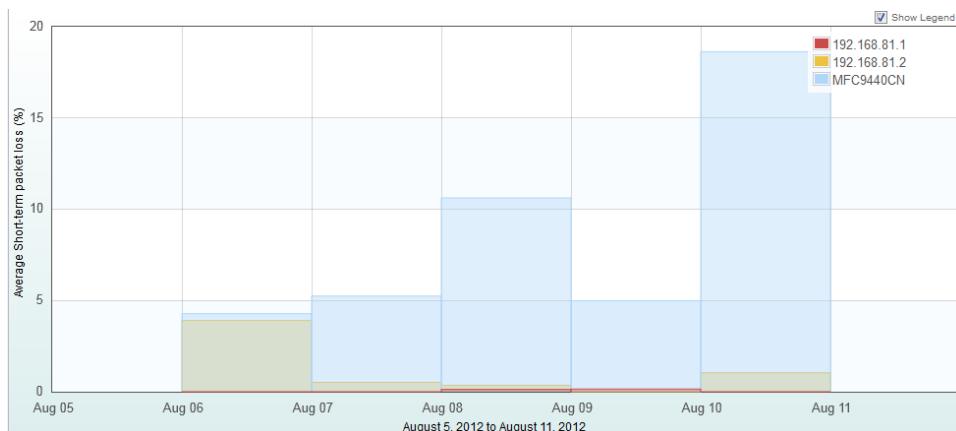


Line Report



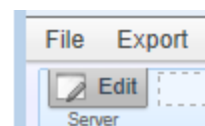
Column Report



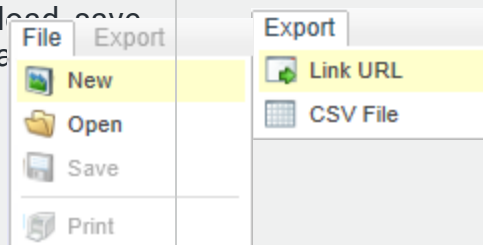


Managing and Printing Reports

Click Edit to switch between Edit and View modes.



Use the File and Export menus to create new reports, to load saved reports, to get a link URL for distribution, or to export a report to a CSV file.

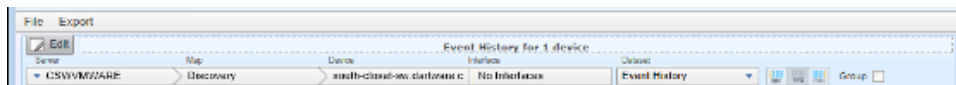


Switching to Edit Mode

To edit a report, you must be in Edit mode.

To switch to Edit mode:

Click **Edit**. The Edit controls are displayed. Click **Edit** again to switch back to View mode.

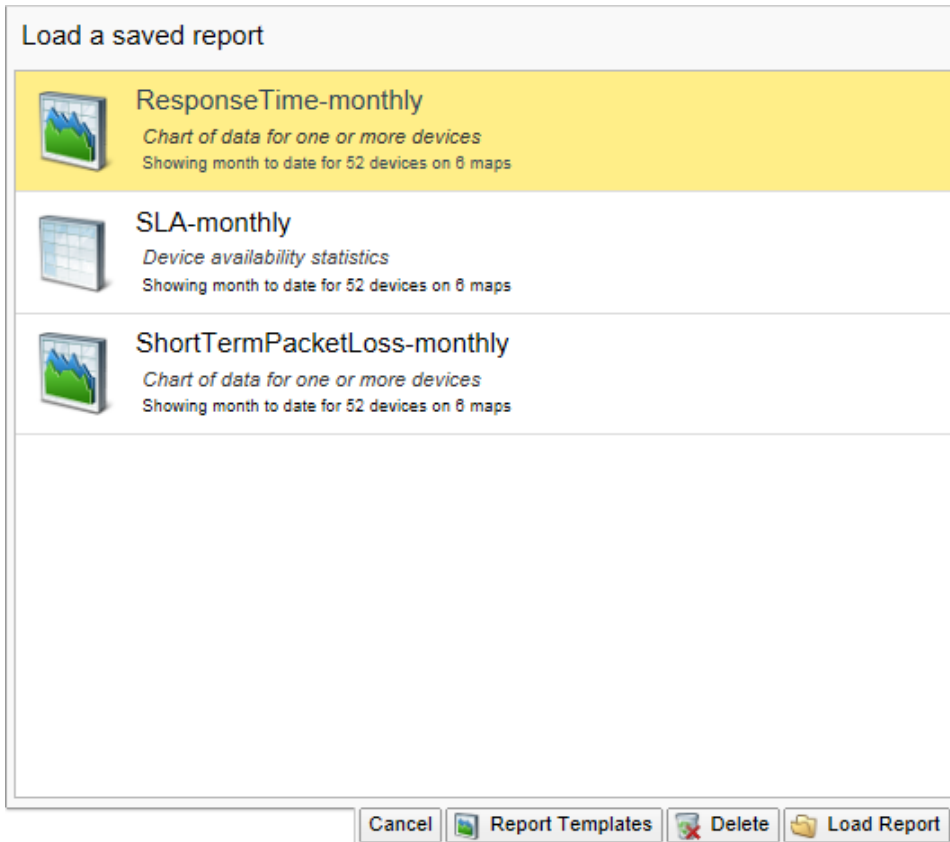


Loading a Saved Report

You can save any number of reports, then open, view or print them at a later time.

To open a saved report:

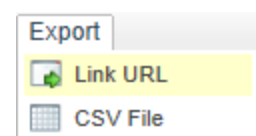
1. From the **Report** window's **File** menu, click **Open**. A list of saved reports is displayed. Each report shows a summary of selected parameters.
2. Click the report you want to load and click **Load Report**. To create a new report, click **Report Templates** to view available templates.

**Deleting a Saved Report**

You can delete a saved report from the Saved Reports list.

To delete a saved report:

1. From the **Report** window's **File** menu, select **Open**. A list of saved reports is displayed.
2. Click the report you want to delete and click **Delete**. A Confirm window is displayed.
3. Click **OK**. The selected report is removed from the list.

Exporting and Linking to a Report

You can use the Report window's Export menu to obtain a URL for distribution or to export the report data into a CSV file.

To get the URL to a report:

1. After viewing the report, select **Link URL** from the **Report** window's **Export** menu. The Link URL box is displayed.



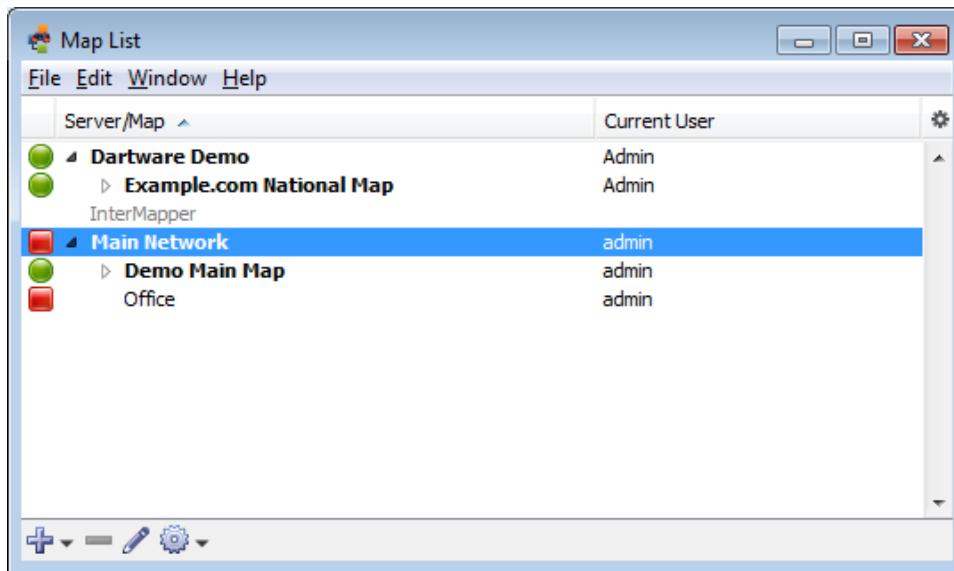
2. Copy the URL and paste it into an email, document, or other container you want to use to distribute it.
3. Click **Cancel** to close the **Link URL** box.
4. To protect the URL from being changed, select **Lock against changes**.

To export a CSV file:

1. After viewing the report, select **CSV File** from the **Report** window's **Export** menu. The result depends on your browser, but a file save action is initiated.
2. Specify a location for the file and click **Save** (the actual name depends on your browser.) A CSV file is saved to the specified location.

Using InterMapper Remote Access

InterMapper can make its maps available to people who are away from the server. They can use a program called [InterMapper Remote Access](#) to view and configure the server.



Intermapper Remote Access is capable of configuring every aspect of Intermapper. For more information on enabling the remote server and a description of how to set up access permissions per-map or by IP address, see [The Remote Server](#).

Intermapper RemoteAccess is also accessible through a [command-line interface](#).

Note to Microsoft Windows users: By default, Microsoft Windows has significant firewalling turned on. You need to create exceptions (poke holes) in the firewall in order to use the remote server, web server, telnet server, or DataCenter server as well as to monitor SNMP traps.

Intermapper Reference

Use the Intermapper Reference section to collect detailed information about Intermapper components. The following references are available:

- **Command/Menu Reference** - displays a list of menu items for each menu and the purpose of each.
- **Probe Reference** - displays an overview of the Set Probe window, a list of probes with a description of each, a number of topics about packet-based, SNMP, Command-Line, other specialized probes, and a topic on troubleshooting.
- **Using Intermapper Data Center** - explains how to configure and use the data center.
- **Files and Folders** - displays information about the default locations of various files and folders for different platforms and how to control locations.

Command and Menu Reference

This chapter describes each menu command in detail. The following commands are available from each menu:

- [File Menu \(Pg. 349\)](#)
Used to execute commands for opening, closing, and saving maps, for printing windows, and for quitting Intermapper. You can also import and export maps from the File menu.
- [Edit Menu \(Pg. 355\)](#)
Used to execute commands for copying and pasting data and selecting and hiding items in maps.
- [View Menu \(Pg. 359\)](#)
Used to change how map are displayed. The View menu is available only from a map window.
- [Monitor Menu \(Pg. 362\)](#)
Used to re-probe one or more devices on a map, to edit information about one or more devices, and to open various windows related to map items. The Monitor menu is available only from a map window.
- [Insert Menu \(Pg. 378\)](#)
Used to insert devices, networks, links, text blocks or icons, and to group or un-group probes. You can also initiate the Auto-discovery process, scan a network, or set a

benchmark for use with geographic coordinates. The Insert menu is enabled only when the Map Editor is active and when you are viewing a map window.

- [Format Menu \(Pg. 385\)](#)

Used to format and arrange items on the map. The Format menu is enabled only when you are viewing a map window, the Map Editor is active, and you have one or more map items selected. The Format menu is available only from a map window.

- [Window Menu \(Pg. 397\)](#)

Used to execute commands for controlling the view of the current map, for viewing log files, and for bringing open windows to the front of your screen.

- [Help Menu \(Pg. 401\)](#)

Used to view the online help system, to view information about Intermapper, and to report bugs or send screenshots to Fortra.

- [Intermapper and IM Remote Access Menus \(Pg. 405\)](#)

macOS adds an Intermapper menu or IM Remote Access menu. These menus contain items that are normally displayed in other menus on other platforms.

- [Context Menus \(Pg. 406\)](#)

These menus are implemented through the Intermapper user interface. These menus allow you to select options that are available only for and related to specific objects in the window.

- [Keyboard Shortcuts \(Pg. 406\)](#)

Certain menu items have keyboard shortcuts. The topics listed above contain the keyboard shortcuts available in the listed menus. For more information on keyboard shortcuts and how they relate to different platforms, see [Keyboard Shortcuts \(Pg. 406\)](#).

Command and Menu Reference

This chapter describes each menu command in detail. The following commands are available from each menu:

- [File Menu \(Pg. 349\)](#)

Used to execute commands for opening, closing, and saving maps, for printing windows, and for quitting Intermapper. You can also import and export maps from the File menu.

- [Edit Menu \(Pg. 355\)](#)

Used to execute commands for copying and pasting data and selecting and hiding items in maps.

- [View Menu \(Pg. 359\)](#)

Used to change how map are displayed. The View menu is available only from a map window.

- [Monitor Menu \(Pg. 362\)](#)

Used to re-probe one or more devices on a map, to edit information about one or more devices, and to open various windows related to map items. The Monitor menu is available only from a map window.

- [Insert Menu \(Pg. 378\)](#)

Used to insert devices, networks, links, text blocks or icons, and to group or un-group probes. You can also initiate the Auto-discovery process, scan a network, or set a benchmark for use with geographic coordinates. The Insert menu is enabled only when the Map Editor is active and when you are viewing a map window.

- [Format Menu \(Pg. 385\)](#)

Used to format and arrange items on the map. The Format menu is enabled only when you are viewing a map window, the Map Editor is active, and you have one or more map items selected. The Format menu is available only from a map window.

- [Window Menu \(Pg. 397\)](#)

Used to execute commands for controlling the view of the current map, for viewing log files, and for bringing open windows to the front of your screen.

- [Help Menu \(Pg. 401\)](#)

Used to view the online help system, to view information about Intermapper, and to report bugs or send screenshots to Fortra.

- [Intermapper and IM Remote Access Menus \(Pg. 405\)](#)

macOS adds an Intermapper menu or IM Remote Access menu. These menus contain items that are normally displayed in other menus on other platforms.

- [Context Menus \(Pg. 406\)](#)

These menus are implemented through the Intermapper user interface. These menus allow you to select options that are available only for and related to specific objects in the window.

- [Keyboard Shortcuts \(Pg. 406\)](#)

Certain menu items have keyboard shortcuts. The topics listed above contain the keyboard shortcuts available in the listed menus. For more information on keyboard shortcuts and how they relate to different platforms, see [Keyboard Shortcuts \(Pg. 406\)](#).

File Menu

You can use the File menu to create new maps, open existing maps, save edited maps, import and export maps, configure maps, and print maps. The following table shows the

commands available from the File menu. It also shows which commands are available from the Map or Map List window.

NOTE: Use shortcuts with Ctrl key (Microsoft Windows) or Command key (macOS).

Command	Description
<u>New Map</u>	creates a new map.
<u>Save</u>	saves a PDF report to disk. (Flows)
<u>Open Recent (submenu)</u>	selects a recently-opened map from the submenu.
<u>Close</u>	closes the current window.
<u>Backup</u>	backs up the current map.
<u>Restore</u>	restores the current map from a backup.
<u>Rename</u>	renames the selected map.
<u>Duplicate</u>	creates a copy of the selected map.
<u>Disable</u>	If you have administrator privileges, use this command to disable the current map (Map Window) or the selected map (Map List window).
<u>Import (submenu)</u>	<p>Select one of the following submenu commands:</p> <ul style="list-style-type: none"> • Map - copies a map file saved on the Intermapper Remote Access machine to the Intermapper server and makes it available. (Use the Export... command to save the file on the Intermapper Remote Access machine.) • Data File - creates maps or updates devices from a tab-delimited import file. For more information, see Importing Data Into Maps. • Probe - imports custom probe files to your server. • MIB - imports an SNMP MIB file for a specific device or family of devices.

<u>Export (submenu)</u>	<p>Select one of the following submenu commands:</p> <ul style="list-style-type: none"> • Map - saves a copy of a server's map to the Intermapper client machine in Intermapper's native MAP format, or as a graphics file in PNG, SVG, or Visio (Microsoft Windows only) format. <div> <p>NOTE:</p> <p>To save a map in the Visio format, you must have the full version of Visio 2013 or higher installed.</p> </div> <ul style="list-style-type: none"> • Data... - saves a file containing selected data from a map in tab-delimited, XML, HTML, CSV, or JSON format. • Helper Apps... - saves an XML file containing a list of Helper Apps.
<u>Server (submenu)</u>	<p>Select one of the following submenu commands:</p> <ul style="list-style-type: none"> • Log In - logs into an Intermapper server. • Log Out - logs out of an Intermapper server. • Info - displays (IM) and changes (IMRA) server name, address, and port info.
<u>Page Setup</u>	opens the standard Page Setup dialog. (Map)
<u>Print</u>	<p>prints the current window on the currently selected printer. (Map)</p> <p>prints a report using the current time range and filter settings. (Flows)</p>
<u>Print Single Page</u>	prints a single page of a map in the current view. (Map)
<u>Exit/Quit</u>	<p>exits the application.</p> <div> <p>NOTE: On macOS, this command is available from the Intermapper or IM Remote Access menu.</p> </div>

New Map

Creates a new empty map. For more information on automatically creating a map, see [Autodiscovery](#).

Save

Saves a PDF report to disk. A standard file dialog is displayed. The report contains the Top Hosts, Top Ports, and Top Sessions tabs.

Open Recent (Submenu)

Selects a recently-opened map from a submenu.

Close

Closes the current window.

NOTE: Closing a map window does not stop the map's devices from being polled or from sending notifications. To prevent a map from being polled, disable the map from the Enabled Maps section of the [Server Settings window](#).

Backup

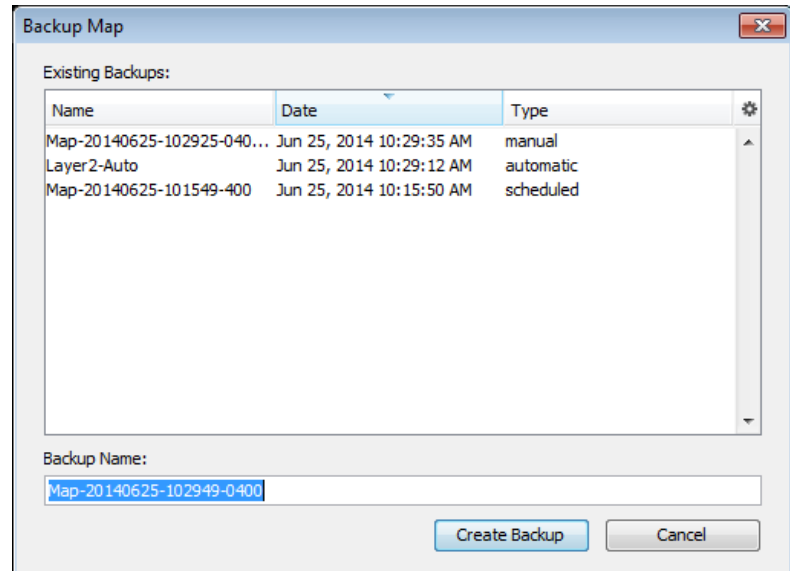
Makes a snapshot backup of the current map.

The Backup Map window shows a list of previous backups of the selected map. Enter a name for the backup or accept the default name, then click **OK**.

Backup Types

Intermapper creates the following backup types:

- **Manual** - the backup was created using the Backup command.
- **Automatic** - the backup was created automatically by enabling Layer 2 in a map and clicking **Change Now**.
- **Scheduled** - the backup was created automatically, based on a schedule defined in the Map Backup panel of the Server Settings window.



Restore

Restores from a previous backup of a map.

The Restore Map window shows a list of previous backups. Click the backup you want to restore and click **OK**.

See Backup (above) for information on backup types.

Rename

Renames the selected map.

Enter a new name for the selected map and click **OK**.

Duplicate

Creates a copy of the selected map.

Disable

If you have administrator privileges, you can use this command to disable the current map (Map Window) or the selected map (Map List window).

Import (submenu)

You can use the Import submenu to select one of the following Import commands:

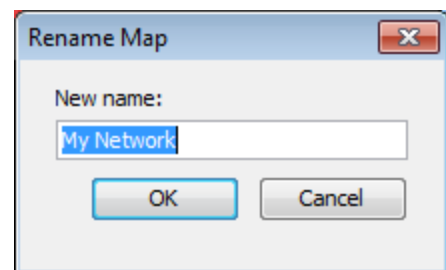
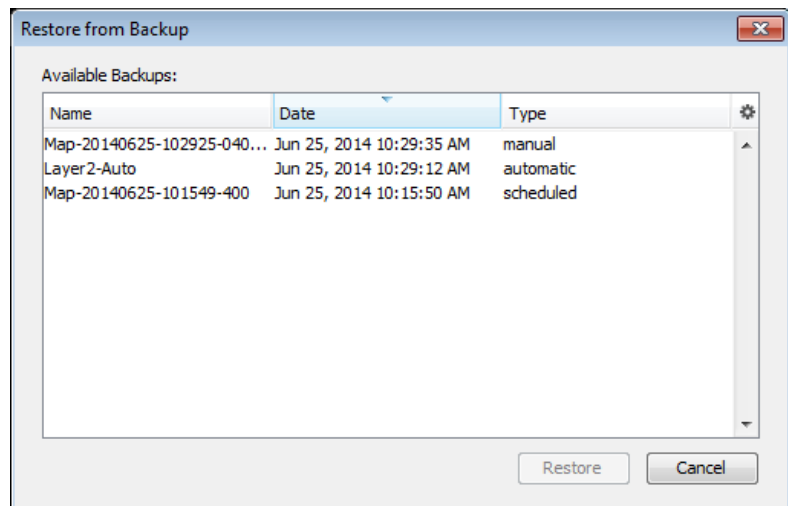
Data File

You can use the **Import > Map** command to import a map from a tab-delimited, comma-delimited, or XML file. For more information, see [Importing Data Into Maps](#).

Intermapper Map

Copies a map file saved on the Intermapper Remote Access machine to the Intermapper server and makes it available. (Use the Export command to save the file on the Intermapper Remote Access machine.)

Probes



Imports custom probe files to your server. For more information, see the Intermapper Developer Guide.

MIB

Imports an SNMP MIB file for a specific device or family of devices. You can use the MIB file information to enhance the formatting of the displayed data. For example, certain views (especially in log files and the SNMP Table views) use the MIB data to display numeric values as the human-readable strings.

Export (Submenu)

You can use the commands available from the Export submenu to save files from the server to the client machine in various formats .

For more information, see [Exporting Data From Maps](#).

Map

You can use the **Export > Map** command to save a copy of your map or one of several image file formats on your local machine's file system. This is an easy way to copy a map from one server to another. After you export the map file, you can import it to a different server.

You can also save visual representations of the map for uses such as marketing, presentations, or troubleshooting.

Save your map in Intermapper's native MAP format, or in PNG, SVG, or Visio (Microsoft Windows only).

NOTE:

To save your map in Visio format, you must have the full version of Vision 2013 or higher installed.

Data

You can use the **Export > Data** command to export data from the selected maps on your server in various text-based formats. Select the tables from which you want to export and the fields within each table you want to use.

Save your map in TAB, XML, HTML, CSV, or JSON format.

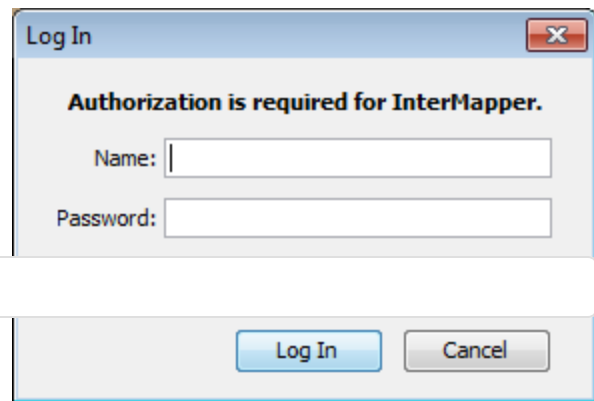
Server (Submenu)

Log In

From the Map List window, click the server you want to log into and select **Log In** from the File menu. An authentication window appears:

Enter a **Name** and **Password**. If you want to save the Name and Password, select **Save Name and Password**.

NOTE: SASL authentication is used for logins.



Log Out

From the Map List window, click a map on the server you want to log out from and click **Log Out**. You are disconnected from the selected server.

NOTE: Open windows for any maps on the selected server remain open after you log out, but the maps are dimmed to indicate that they are no longer active.

Page Setup

Opens a standard Page Setup dialog.

Print

From a map, this command prints the current window on the currently selected printer. This operation uses as many pages as necessary to print the entire map or window contents.

From the Flows window, this command prints a report using the Flows window's current time range and filter settings.

Exit/Quit

Exits the application.

Edit Menu

The Edit menu contains standard editing commands, as well as various commands for selecting and finding items.

Menu Command	Description
Undo (Pg. 356)	(Map window only) Reverses the previous operation. Most operations in InterMapper can be undone. Undo is multiple levels.

Menu Command	Description
Redo (Pg. 357)	(Map window only) Available after you execute the Undo command. Restores the state of the map before the Undo command was executed.
Revert (Pg. 357)	(Map window only) Restores the state of the map as it was when you last opened it for editing.
Cut (Pg. 357)	Cuts the selected items to the clipboard.
Copy (Pg. 357)	Copies the selected items to the clipboard.
Paste (Pg. 357)	Pastes the contents of the clipboard to the current window.
Delete (Pg. 357)	Removes the selected items from the map. Caution: This operation cannot be undone.
Select (submenu) (Pg. 357)	(Map window only) Offers a variety of commands to select objects in a variety of ways.
Select All (Pg. 358)	(Map List window only) Selects all maps and servers.
Find (submenu) (Pg. 358)	<ul style="list-style-type: none"> • Find (Pg. 358) - Opens the Find window. Enter a text string to search for. • Find Next (Pg. 358) - Searches for the next occurrence of the last defined text string. • Find Device... (Pg. 358) - Search for a device in a map on a connected server.
Map Settings (Pg. 359)	Opens the Map Settings window.
Server Settings (Pg. 359)	Opens the Server Settings window.
Preferences (Pg. 359)	<p>Opens the Preferences window for the Intermapper client application or Intermapper Remote Access client application.</p> <div> <p>NOTE: On macOS, this command is available from the Intermapper or IM Remote Access menu.</p> </div>

Undo

Reverses the previous operation. Most operations in Intermapper can be undone. Undo is multiple levels.

Redo

Re-performs the previous undo operation. Any operation that has been undone can be redone.

NOTE: The Undo/Redo function is sequential; if you undo multiple operations, then perform a different operation, all the operations you undid are gone.

Revert

Restores the state of the current map to its last state when it was last enabled for editing.

Cut

Cuts the selected items to the clipboard.

Copy

Copies the selected items to the clipboard.

Paste

Pastes the contents of the clipboard to the current window.

Delete

Removes the selected items from the current window.

Select (Submenu)

The following options are available in the **Select** submenu:

- **Select All** - Selects all map items.
- **Select Adjacent** - Selects all map objects connected to the current selection. The first time you run the command, all leaves are selected (a leaf is an object that has no other connections). Run the command a second time to select all other objects connected to the selected object. Keep running the command to continue expanding

the selection, first selecting the leaves, then the other objects.

NOTE: If you select a device connected to a network, use the Select Adjacent function. The network is selected, but none of the other devices connected to the network are selected. To select a network and its adjacent devices, select the network first, then click Select Adjacent.

- **All devices** - Selects all devices, but not links or networks.
- **DOWN devices** - Selects only the devices that are currently marked as down.
- **UP devices** - Selects only the devices that are currently marked as up.
- **All networks** - Selects all networks, but not the attached devices.
- **DOWN Interfaces** - Selects all interfaces currently marked as down.
- **Networks with** - Selects all networks with the specified number of attached devices.
- **Unselected** - Inverts the selection. Deselects all selected items; selects all deselected items.

Select All

Selects all maps and servers.

NOTE:

This operation is only available in the Map List window.

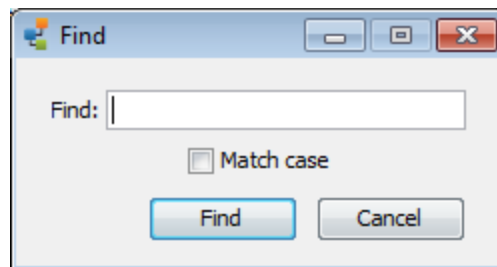
Find

Finds the first object containing the specified text in the current map. The device is highlighted when it is found.

Find Next

Finds the next item in the current map that matches the previously specified text string.

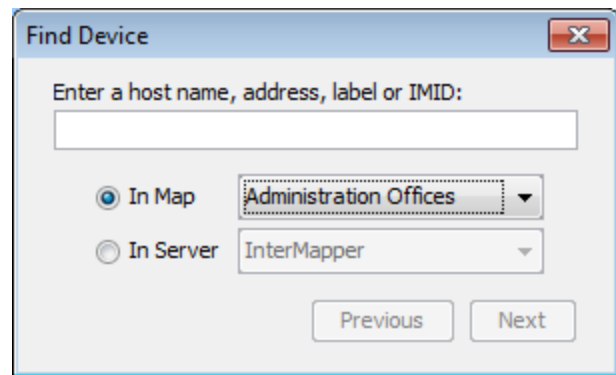
Find Device



Finds the a device on the specified map or server. You can search by host name, address, or IMID. For example, this can help you determine where a dataset is in the database.

Map Settings

You can use the Map Settings command to view and edit an individual map's color settings, specify a background image, and view and edit the list of default notifiers for the map. For more information, see [Map Settings \(Pg. 68\)](#). This command is available only in Edit mode.



Server Settings

You can use the Server Settings command to open the Server Settings window to view server information, and to view and edit all server preferences and settings. You can control the settings of the built-in web, Intermapper remote access, and Telnet servers. For more information, see [Server Settings \(Pg. 224\)](#).

Preferences

You can use the Preferences command to open the Preferences window to set preferences for the Intermapper client application or for Intermapper Remote Access. These settings affect only the copy of the application you are running.

View Menu

You can use the View menu in the Map window to specify how you want to look at a map. The view menu is available only from the Map window.

Menu Command	Description
Map	View as a map, with graphic objects representing devices, networks, and links.
List	View as a list of devices.
Device Notifiers	View as a list of devices, each showing the states for which the selected notifier sends notifications.
Link Notifiers	View as a list of interfaces, each showing the states for which the selected notifier sends notifications.

<u>Charts</u>	View a list of charts associated with the map.
<u>Datasets</u>	Select from a list of devices to view a list of datasets available for those devices.
<u>Actual Size</u>	In Map view, sets the zoom level to 100%.
<u>Zoom In</u>	In Map view, zooms in.
<u>Zoom Out</u>	In Map view, zooms out.
<u>Sort</u> <u>(submenu)</u>	<p>In any list view, select from a list of columns to sort the list by.</p> <div> <p>NOTE: You can also sort the list by clicking a column heading. Click again to reverse the sort.</p> </div>
<u>Columns</u> <u>(submenu)</u>	Select the columns you want to show in any list view.
<u>Filter</u> <u>(submenu)</u>	Select to view only those objects with the selected state.
<u>Expand All</u>	In List view, expands all hierarchical items in the Map and Device List windows.
<u>Collapse All</u>	In List view, collapses all hierarchical items in the Map and Device List windows.
<u>Show/Hide Toolbar</u>	(Map List Window only) Choose to show or hide the toolbar.
<u>Edit Map</u>	Toggles between Map Edit mode and Monitor mode.

Map

Keyboard Shortcut: Ctrl+1

View as a map, with graphic objects representing devices, networks, and links.

List

Keyboard Shortcut: Ctrl+2

View as a list of devices, networks, and links.

Device Notifiers

Keyboard Shortcut: Ctrl+3

View as a list of devices, each showing the states for which the selected notifier sends notifications.

Link Notifiers

Keyboard Shortcut: Ctrl+4

View as a list of interfaces, each showing the states for which the selected notifier sends notifications.

Charts

Keyboard Shortcut: Ctrl+5

View a list of charts associated with the map.

Datasets

Keyboard Shortcut: Ctrl+6

View a list of datasets available for selected devices.

Actual Size

Keyboard Shortcut: Ctrl+0

In Map view, sets the zoom level to 100%.

Zoom In

Keyboard Shortcut: Ctrl+Up Arrow

Zoom Out

Keyboard Shortcut: Ctrl+Down Arrow

Sort (Submenu)

From the **Sort** submenu, select a column by which you want to sort the list. Select it again to reverse the sort order. This function is not available in Map view.

NOTE: You can also click the column heading to sort by that column and click it again to reverse the sort order.

Columns

From the **Columns** submenu, select or clear the check box for a column to show or hide the column. This function is not available in Map view.

Filter (Submenu)

Views only those objects with the selected state. Filter devices with the selected state to view only those that are acknowledged or unacknowledged.

Expand All

Expands all hierarchical items in the Map List or Device List window.

Collapse All

Collapses all hierarchical items in the Map List or Device List window.

Show/Hide Toolbar

Shows or hides the toolbar.

Edit Map

Select this menu item, click the lock icon at the upper left of the map, or press the **Tab** key on your keyboard.

Toggles the map between Editing mode (where the map can be rearranged, edited, and changed) and Monitoring mode (where the map is uneditable, but displays the current state of the network). The check box for this menu item is selected when map editing is enabled.

NOTE: Many users can use Intermapper Remote Access to connect to an Intermapper server at the same time. At any given time, however, only one user can edit a map. If you try to change a map to Edit mode while it is being edited by another user, a message is displayed, telling you that someone is currently editing the map. You can interrupt the other user's editing session, at which time you gain the right to edit the map.

Monitor Menu

You can use the Monitor menu to re-probe one or more devices on a map, to edit information about one or more devices, and to open various windows related to map items. The Monitor menu is available only from a Map window.

Menu Command	Description
<u>Reprobe/Reprobe Selection</u>	Reprobe: If no device is selected, re-polls all devices on the map. Reprobe Selection: Re-polls the selected devices.
<u>Acknowledge</u>	Use this command to acknowledge a failure. This stops an icon's flashing and deactivates recurring notifications.
<u>Un-Acknowledge</u>	Use this command to remove an acknowledgment from the selected device, and to reactivate notifications.
<u>Info Window</u>	Opens the Info Window for the selected device or network.
<u>Status Window</u>	Opens the Status window for the selected device, network, or link.
<u>Interfaces > Window</u>	Opens the Interfaces window for the selected device.
<u>Interfaces > Error Thresholds</u>	Opens the Error Thresholds dialog. Sets error thresholds for one or more interfaces.
<u>Interfaces > Utilization Thresholds</u>	Opens the Utilization Thresholds dialog. Sets thresholds for utilization of one or more links.
<u>Interfaces > Discard Thresholds</u>	Opens the Discard Thresholds dialog. Sets packet discard thresholds for an interface.
<u>Interfaces > Behavior</u>	Opens a device's Behavior dialog. Specifies whether to allow periodic reprobes and whether to display unnumbered interfaces.
<u>Device Notifiers Window</u>	Opens the Device Notifiers window and shows a list of notifiers for the selected device.
<u>SNMPWalk</u>	Opens the SNMPWalk dialog.
<u>Flows Window</u>	Opens the Flows Window if Intermapper Flows is running.
<u>Show in Layer 2 (Pg. 318)</u>	Opens the Device List window in Layer 2 view and shows connections to the selected device.
<u>Set Info > Set Address</u>	Sets the IP address or name for the selected device.
<u>Set Info > Set Comment</u>	Allows you to enter a comment about the selected device(s).

Menu Command	Description
<u>Set Info > Set Community</u>	Sets the SNMP community string for the selected devices.
<u>Set Info > Set Data Retention</u>	Selects a Data Retention policy to use when storing data to the Intermapper Database.
<u>Set Info > Set Double-click (submenu)</u>	Defines the action to be taken when you double-click the selected device.
<u>Set Info > Set Kind...</u>	Sets the device kind you want to use when storing data to the Intermapper Database.
<u>Set Info > Set Latitude & Longitude</u>	Sets the latitude and longitude for the selected devices.
<u>Set Poll Interval</u>	Sets the poll interval for the selected devices.
<u>Set Info > Set Probe (Pg. 375)</u>	Sets the probe to be used with the selected devices.
<u>Set Info > Set Thresholds</u>	Sets the criteria for sending notifications that a device is down, in alarm, or in warning. These settings apply to all devices on the map.
<u>Set Info > Set Vantage Point</u>	Sets the selected device as the vantage point from which Intermapper views all other devices on the map.
<u>Reset Short-term Packet Loss</u>	Resets the accumulated value of short-term packet loss.
<u>Helper Apps (submenu)</u>	Launches a helper application or customize the list of applications.

Reprobe/Reprobe Selection

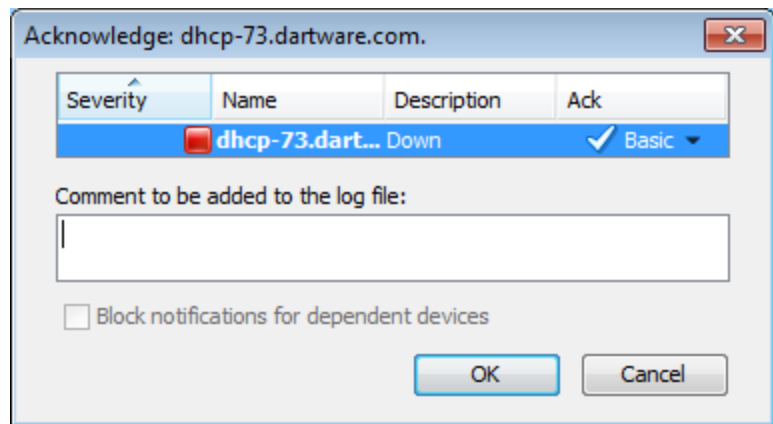
Re-polls the selected devices to retrieve the status of a device or detecting that it has returned to service.

- If a single device is selected, it is polled again as soon as possible.
- If multiple devices are selected, they are moved to the head of the poll queue so they are re-polled as soon as possible.
- If no devices are selected, all devices in the map are moved to the head of the poll queue and are re-polled as soon as possible.

Acknowledge

When Intermapper detects a problem with a device, the device's icon changes to yellow, orange, or red. This serves to attract attention to the failure, but can be distracting after corrective action has been initiated. It also masks further failures: if several items on a map are already in alarm, it is hard to notice new problems.

You can use the Acknowledgment command to indicate that the network administrator is aware of a problem and has initiated corrective action. Acknowledging an alarm turns the device's icon blue and stops repeated notifications for that device.



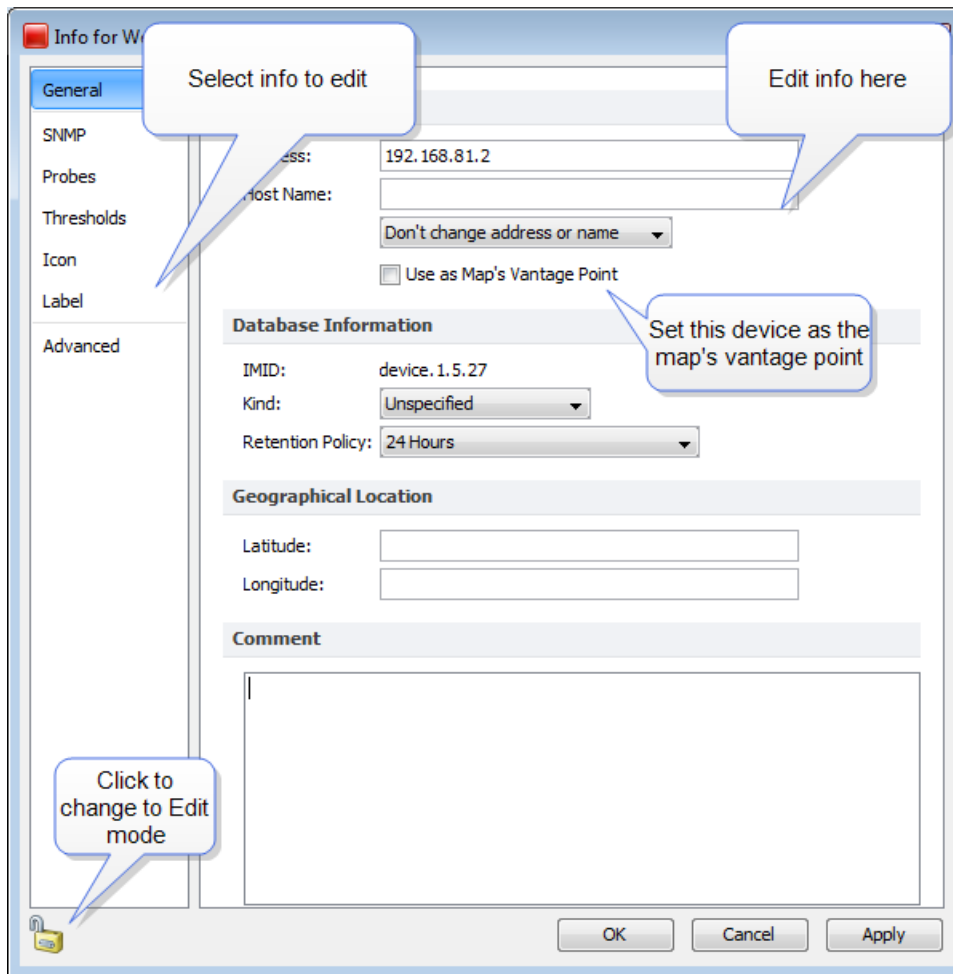
For more information on the Acknowledgments window, see [Acknowledging Device Problems](#).

NOTE: Another feature (dependencies) is useful for controlling the number of notifications you receive when there are failures of central equipment. For more information, see [Using Notification Dependencies](#).

Un-Acknowledge

You can use this command to restore the flashing icon for a device that has been acknowledged in error or which needs further attention. Un-acknowledging a device reactivates recurring notifications.

Info Window



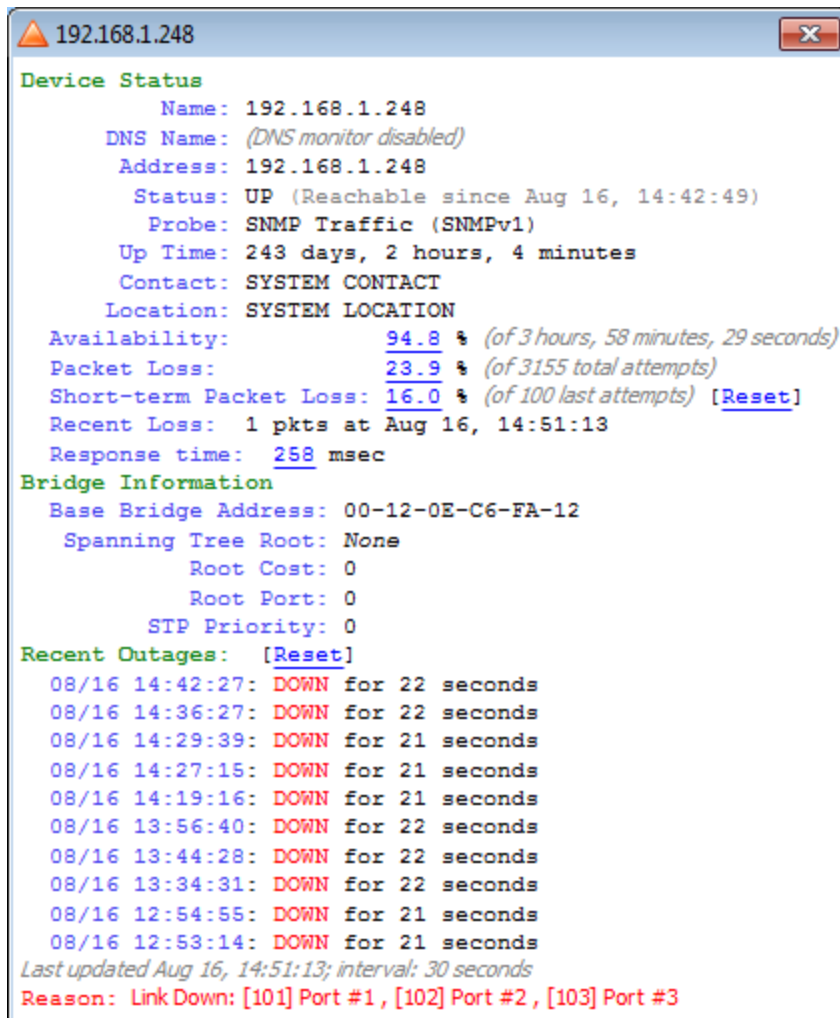
Use the [Info window](#) command to view information about the selected device or network.

- Click the lock icon to change to **Edit** mode.
- Click a button at left to view that **Info** pane.

Status Window

Open the [Status window](#) for the selected device. This command is active in Map Edit mode, which is useful for creating charts.

The following example shows a Device Status window. Status windows are also available for networks and links. For examples, see [Status windows](#).

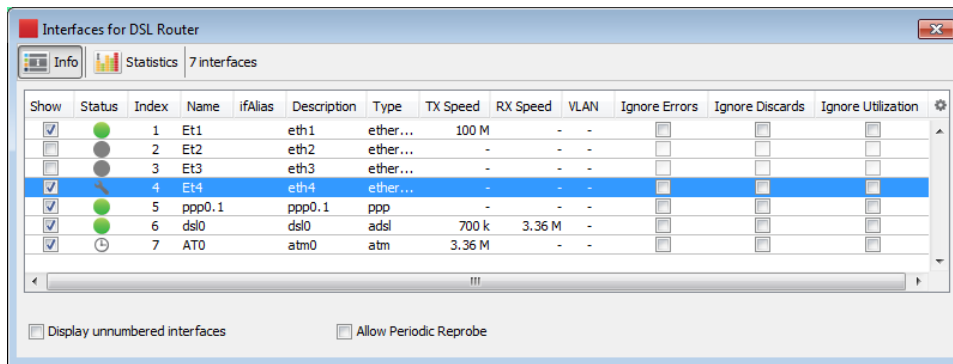


Interfaces Window

Open the [Interfaces window](#) for the selected device.

Info View

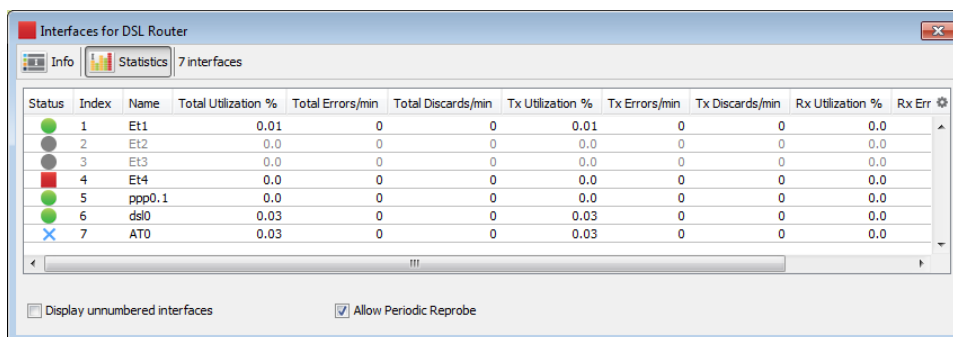
You can use the Info view of the Interfaces window to view the status of interfaces for the selected device, to hide or show them, to specify mapping behavior, and to specify what thresholds to ignore. You can also access the Interfaces submenu for one or more interfaces.



For more information, see [Interfaces window](#).

Statistics View

You can use the Statistics view of the Interfaces window to see various statistics for all interfaces on a device.



For more information, see [Interfaces window](#).

Error Thresholds Window

You can use the Error Thresholds window to override map defaults and set thresholds for link errors on the selected devices. For more information, see [Setting Thresholds](#).

Link Error Thresholds for Device 'DSL Router'

Set interface thresholds to alert you to network problems.

Error Thresholds

☒ Use map defaults

	Warning	Alarm	Critical	
Rx Errors (Received):	10	20	30	per minute
Tx Errors (Transmitted):	10	20	30	per minute
Total Errors (Rx + Tx):	10	20	30	per minute

OK Cancel

Utilization Thresholds Window

You can use the Utilization Thresholds window to override map defaults and set thresholds for link utilization on the selected devices. For more information, see [Setting Thresholds](#).

Link Utilization Thresholds for Device 'DSL Router'

Set interface thresholds to alert you to network problems.

Utilization Thresholds

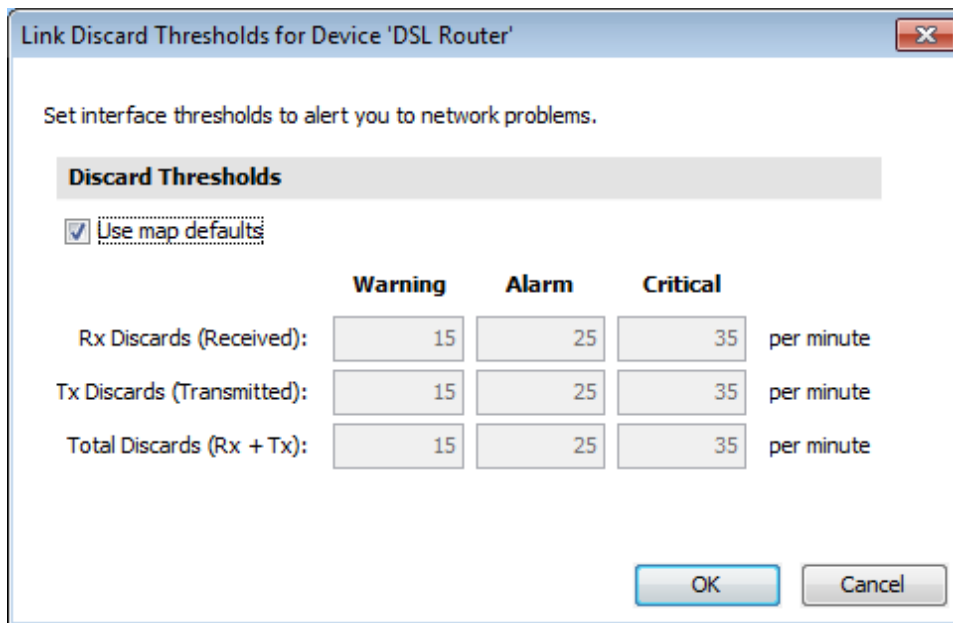
☒ Use map defaults

	Warning	Alarm	Critical	
Rx Utilization (Received):	75	85	95	%
Tx Utilization (Transmitted):	75	85	95	%
Total Utilization (Rx + Tx):	75	85	95	%

OK Cancel

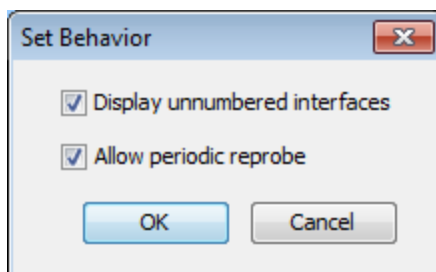
Discard Thresholds Window

You can use the Discard Thresholds window to override map defaults and set thresholds for discarded packets on the selected devices. For more information, see [Setting Thresholds](#).



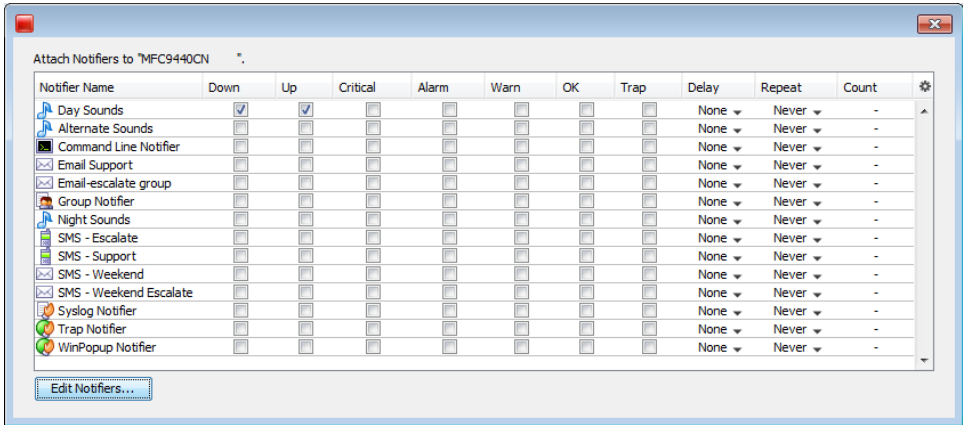
Behavior Window

You can use the Behavior window to set the display and polling behavior of the selected devices. This window is also available from the Context menu; the options are also available from the [Interfaces window](#).



Notifiers Window

Open the Notifiers window for the selected device.

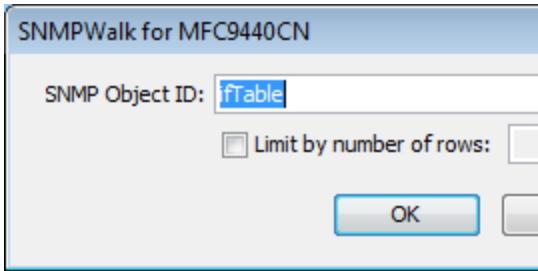


SNMPWalk

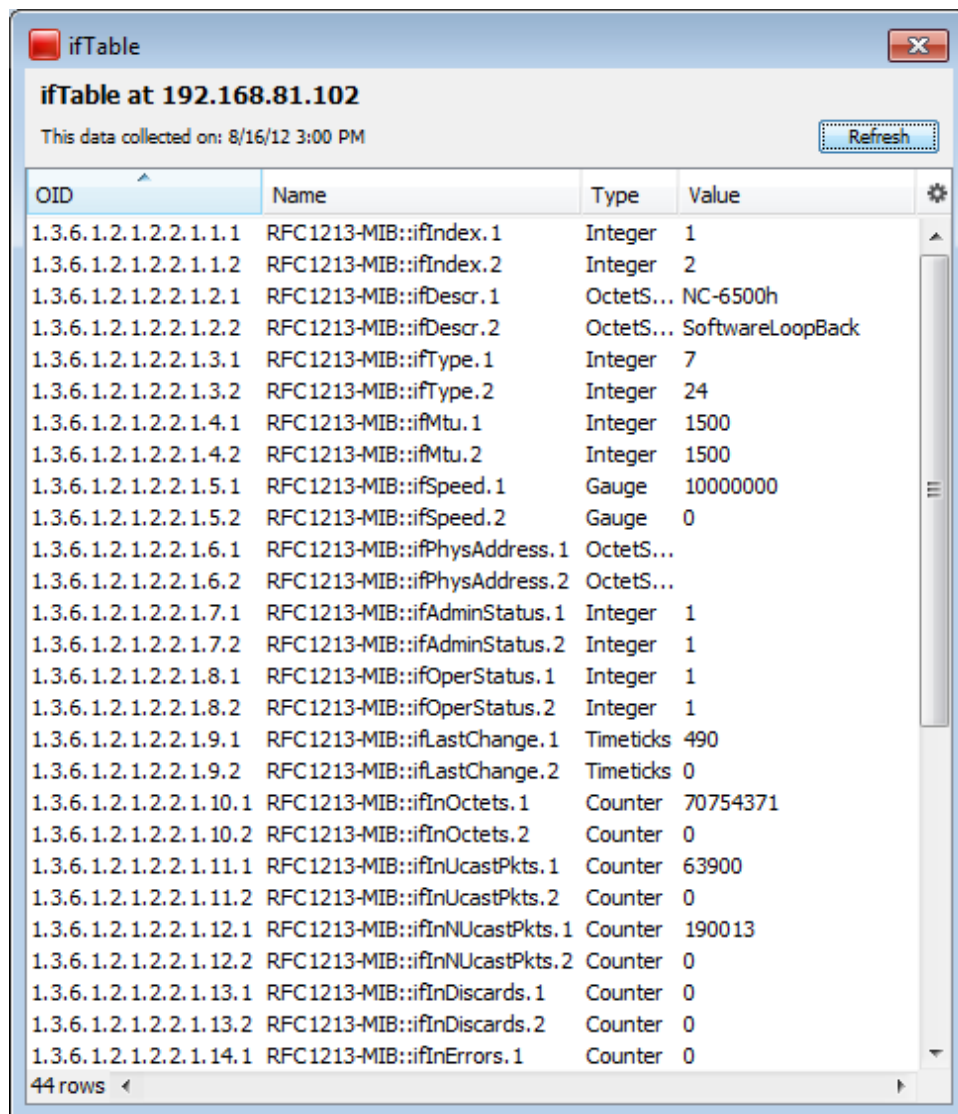
You can use the SNMPWalk command to execute an SNMPWalk on the specified SNMP enabled device. Enter a numeric or textual OID.

The following example shows the output of an SNMPWalk command with ifTable as the specified OID.

For more information on [SNMPWalk](#), see the Developer Guide.



The SNMPWalk dialog



ifTable at 192.168.81.102
This data collected on: 8/16/12 3:00 PM

OID	Name	Type	Value
1.3.6.1.2.1.2.2.1.1.1	RFC1213-MIB::ifIndex.1	Integer	1
1.3.6.1.2.1.2.2.1.1.2	RFC1213-MIB::ifIndex.2	Integer	2
1.3.6.1.2.1.2.2.1.2.1	RFC1213-MIB::ifDescr.1	OctetS...	NC-6500h
1.3.6.1.2.1.2.2.1.2.2	RFC1213-MIB::ifDescr.2	OctetS...	SoftwareLoopBack
1.3.6.1.2.1.2.2.1.3.1	RFC1213-MIB::ifType.1	Integer	7
1.3.6.1.2.1.2.2.1.3.2	RFC1213-MIB::ifType.2	Integer	24
1.3.6.1.2.1.2.2.1.4.1	RFC1213-MIB::ifMTU.1	Integer	1500
1.3.6.1.2.1.2.2.1.4.2	RFC1213-MIB::ifMTU.2	Integer	1500
1.3.6.1.2.1.2.2.1.5.1	RFC1213-MIB::ifSpeed.1	Gauge	10000000
1.3.6.1.2.1.2.2.1.5.2	RFC1213-MIB::ifSpeed.2	Gauge	0
1.3.6.1.2.1.2.2.1.6.1	RFC1213-MIB::ifPhysAddress.1	OctetS...	
1.3.6.1.2.1.2.2.1.6.2	RFC1213-MIB::ifPhysAddress.2	OctetS...	
1.3.6.1.2.1.2.2.1.7.1	RFC1213-MIB::ifAdminStatus.1	Integer	1
1.3.6.1.2.1.2.2.1.7.2	RFC1213-MIB::ifAdminStatus.2	Integer	1
1.3.6.1.2.1.2.2.1.8.1	RFC1213-MIB::ifOperStatus.1	Integer	1
1.3.6.1.2.1.2.2.1.8.2	RFC1213-MIB::ifOperStatus.2	Integer	1
1.3.6.1.2.1.2.2.1.9.1	RFC1213-MIB::ifLastChange.1	Timeticks	490
1.3.6.1.2.1.2.2.1.9.2	RFC1213-MIB::ifLastChange.2	Timeticks	0
1.3.6.1.2.1.2.2.1.10.1	RFC1213-MIB::ifInOctets.1	Counter	70754371
1.3.6.1.2.1.2.2.1.10.2	RFC1213-MIB::ifInOctets.2	Counter	0
1.3.6.1.2.1.2.2.1.11.1	RFC1213-MIB::ifInUcastPkts.1	Counter	63900
1.3.6.1.2.1.2.2.1.11.2	RFC1213-MIB::ifInUcastPkts.2	Counter	0
1.3.6.1.2.1.2.2.1.12.1	RFC1213-MIB::ifInNUcastPkts.1	Counter	190013
1.3.6.1.2.1.2.2.1.12.2	RFC1213-MIB::ifInNUcastPkts.2	Counter	0
1.3.6.1.2.1.2.2.1.13.1	RFC1213-MIB::ifInDiscards.1	Counter	0
1.3.6.1.2.1.2.2.1.13.2	RFC1213-MIB::ifInDiscards.2	Counter	0
1.3.6.1.2.1.2.2.1.14.1	RFC1213-MIB::ifInErrors.1	Counter	0

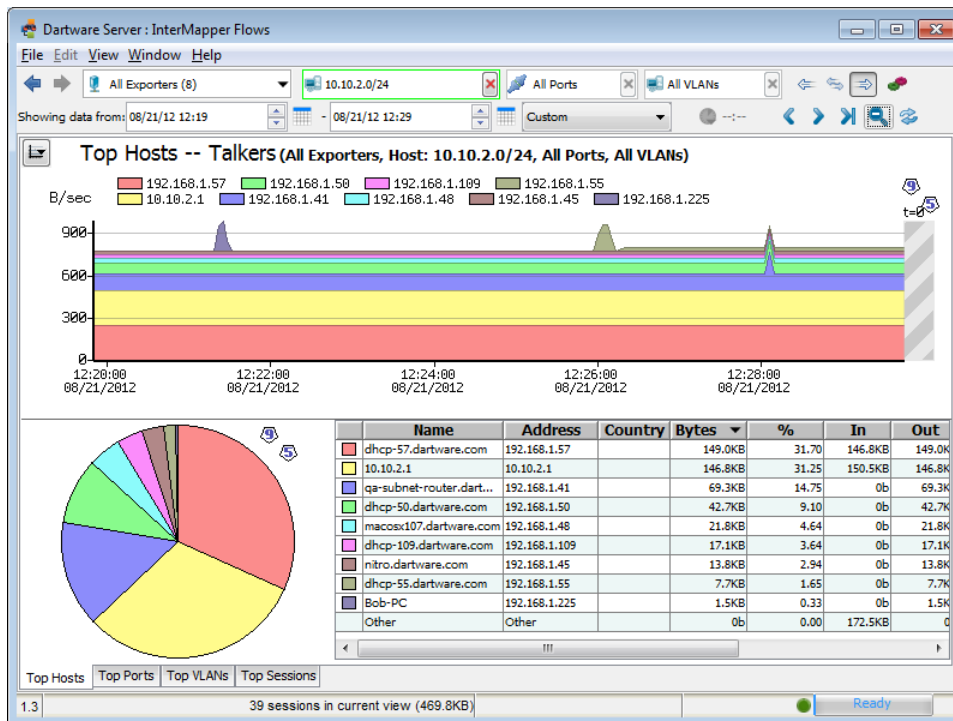
44 rows

NOTE: When using probe groups, you cannot perform an SNMPWalk on the entire probe group, only on individual probes.

To perform an SNMPWalk on a probe

1. From a map's **List** view, expand the probe group to view the individual probes.
2. Right-click the probe you want to perform the SNMPWalk and select **SNMPWalk**. The SNMPWalk window is displayed.
3. Complete the dialog as needed and click **OK**.

Flows Window



If InterMapper Flows is running, opens the Flows Window, which shows InterMapper Flows information. For more information on InterMapper Flows, see [InterMapper Flows](#).

Show in Layer 2

You can use the Show in Layer 2 command to open the Device List window in Layer 2 view and view the connections to the selected devices.

Reports

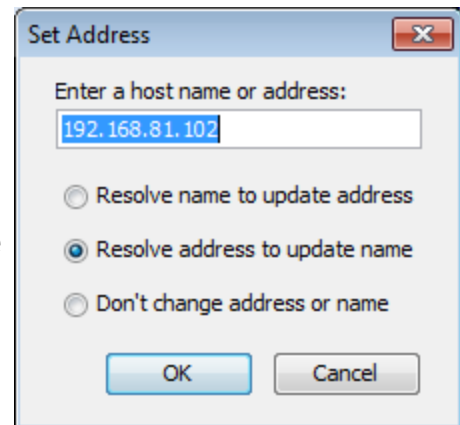
You can use the Reports command to open the Reports user interface in a browser window. You can use the Reports window to create, load, edit, and save reports.

Set Address

Enter a host name or address - enter a DNS name or IP address here. Intermapper uses this address to probe the device.

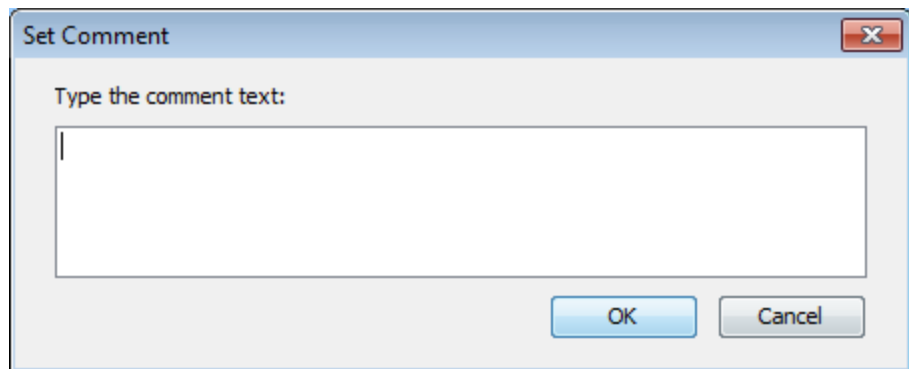
Resolve Name to Update Address - Intermapper queries the DNS for the given name, and uses the result to change the address it uses to poll the device.

Resolve Address to Update Name - keeps the specified IP address fixed, but might update the name from the DNS server if one is found.



Set Comment

The comment is displayed in the device's status window. This sets the comment for all the selected devices. For more information on the Comment field, see the Device Status window.

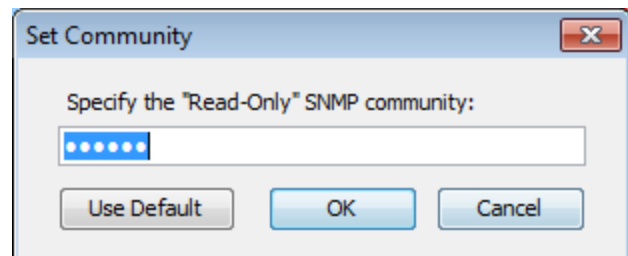


This information is saved as part of the map. You can use the Comment field to save the model and serial number of a device, telephone numbers, circuit numbers, or other information related to the item.

Set Community

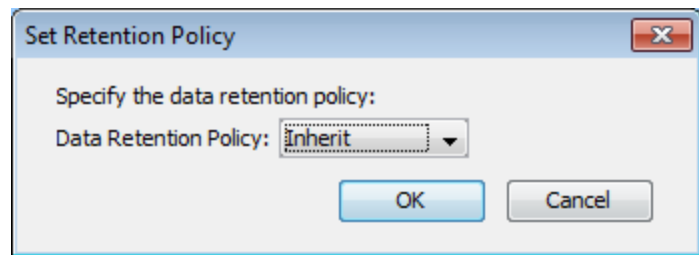
Sets the [read-only community string](#) for all selected devices.

The default community string for most SNMP devices is public.



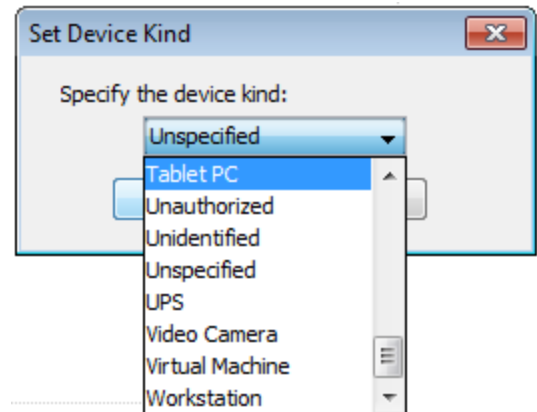
Set Data Retention

Selects the Data Retention Policy to use when storing data to the Intermapper Database. Data Retention Policies are defined using the Intermapper Database Settings page of the DataCenter Administration Panel.



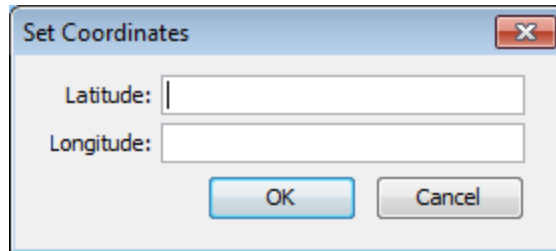
Set Kind

You can set a device kind for each device whose data is stored in the Intermapper database. This can be useful during data reporting or analysis. Use the Set Device Kind dialog to choose the device kind you want to store with the device data.



Set Latitude and Longitude

Enter valid latitude and longitude values in the text boxes and click **OK**. The device is moved to the appropriate location in the map, based on existing benchmarks.

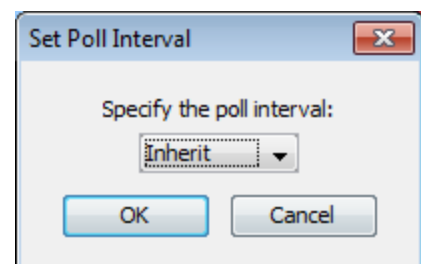


Set Poll Interval

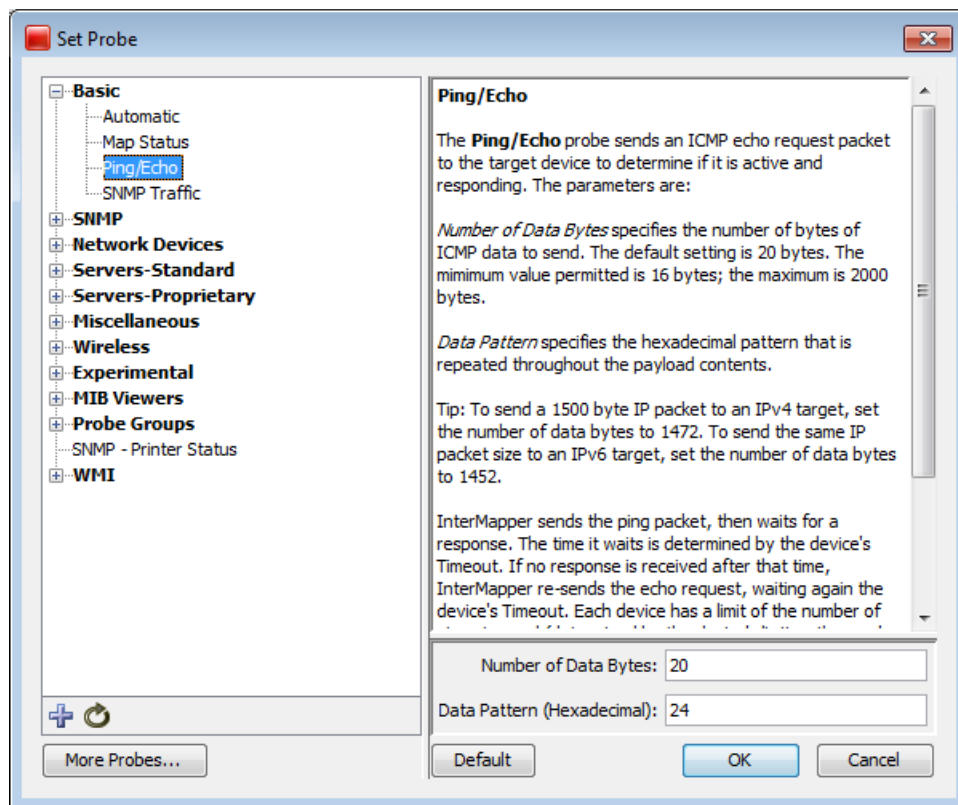
Sets the poll interval for selected devices. This interval is independent of and takes priority over the map's poll interval.

If the device's poll interval is set to Default, the map's poll interval is used.

If a map is set to No polling the device poll intervals are ignored and no devices are polled for that map.



Set Probe



Sets the probe used to query the selected device and the probe's parameters, if applicable. See [Probe Reference](#) for details on the available Intermapper probes. For information on creating your own Intermapper probes, see Custom Probes.

- Click the plus sign (+) in the left pane to expand a probe group.
- Click the minus sign (-) in the left pane to collapse a probe group.
- Click a probe in the left pane to select it. Information about the probe and controls for setting any available parameters are displayed in the right frame.
- Click **Default** to set the probe back to default setting for that probe type.

Set Thresholds

Device Thresholds for Web Server

Set thresholds to alert you to network problems.

☐ Ignore outages

☒ Use Map defaults

Down Thresholds

Specify the timeout in seconds (1-9600):

Number of lost packets (1 - 10):

Other Thresholds

	Warning	Alarm	Critical	
Short-term packet loss:	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="20"/>	of last 100
Response Time:	<input type="text" value="1000"/>	<input type="text" value="5000"/>	<input type="text" value="20000"/>	msec

OK Cancel

Set the criteria for sending a notification that a device is down, in an alarm state, or in a warning state. These settings apply to all the devices on the map.

- **Down** - the most serious condition. It means the device is no longer responding to probes. Specify the number of packets that can be lost before declaring the device down.
- **Critical** - the most serious condition in which responses are still being received. Specify the number of interface errors (per minute) allowed before marking the device as critical.
- **Alarm** - the next most serious condition. Specify the number of interface errors (per minute) allowed before marking the device in alarm.
- **Warning** - the least serious error state. Specify the number of interface errors (per minute) allowed before showing the device in warning.

Set Vantage Point

Sets the selected device as the Vantage Point from which Intermapper views all other devices on the map. If a device (such as a router or switch) between the Vantage Point and other devices fails, notifications are sent only for the failed device. The other devices are in the shadow of the failed device, and are dimmed on the map.

The Vantage Point specifies Intermapper's virtual point of presence, as if the Intermapper server is directly connected to that item. When the Vantage Point is set on a device, a star is displayed next to the icon.

The Vantage Point is used in conjunction with Intermapper's Notification Dependencies, which suppress notifications for devices that are assumed to be down because some other failure hides or shadows them. For more information, see [Notification Dependencies](#).

Reset Short-Term Packet Loss

Intermapper counts the number of dropped packets out of the last 100. This applies to all packets sent to the device (networks and links are not involved).

Short-term packet loss is displayed in the device's Status window as a percentage of the number of dropped packets in the last 100. Use this command to reset the current value to zero.

Helper Apps

Select a device and use this submenu to specify how to launch a helper application. You can also customize this to configure your helper applications.

Set Double-Click

Select one or more map items and use this submenu to specify what action is taken when any of the items is double-clicked. Use double-click actions to launch an Helper Application, URL, or Menu item.

For more information on Double-Click actions, see [Using Double-Click Actions](#).

Insert Menu

You can use the Insert menu to insert devices, networks, links, and blocks of text to your map. You can also use this menu to initiate the Auto-discovery and network-scanning processes.

The Insert menu is available only in the Map window and is active only when the Map Editor is on.

Menu Command	Description	
--------------	-------------	--

<u>Device (Pg. 379)</u>	Adds one or more devices to a map.	
<u>Network (Pg. 381)</u>	Adds a network (oval) to the map.	
<u>Link (Pg. 381)</u>	Connects two devices with a link.	
<u>Auto-Discover (Pg. 381)</u>	Scans a network to find network devices such as routers, hosts, switches, hubs, servers, workstations, and place them on the map. Specify a starting address and the kinds of devices Intermapper finds and limit the breadth of the search.	
<u>Scan Networks (Pg. 382)</u>	Scans a network to find network devices such as routers, hosts, switches, hubs, servers, workstations, and place them on the map. Limit the types of devices Intermapper looks for. This command is available only when a network is selected, but the Filter dialog is also available from the Automatic Device Discovery dialog.	
<u>Empty Probe Group (Pg. 383)</u>	Inserts one or more empty probe groups in the map.	
<u>Text (Pg. 383)</u>	Adds an object to the map containing the specified text.	
<u>Icon</u>	Inserts an icon into a map.	
<u>Map Benchmark Map Benchmark on page 384</u>	Inserts a benchmark to define the latitude and longitude of a point on the map.	
<u>Group</u>	Groups two or more selected devices into a probe group. Devices must have the same IP address.	
<u>Un-Group</u>	Removes all probes from the selected probe group, and create a single device for each probe.	

Device

Adds a new device to a map. Intermapper links the newly-added devices to networks already in the map. This example shows the Add Devices window.

To add a device:

1. Enter the one or more device names or addresses into the window.

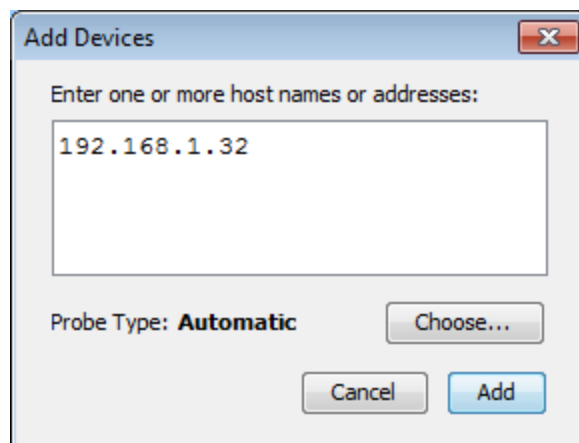
Enter the names manually or paste from some other source. The names must be separated with commas or whitespace

(spaces, tabs, or returns). The list of host names or IP addresses can be copied from a text file, from a traceroute program, or from other source of names and/or addresses. To resolve a domain name to an IPv6 address, enclose it in [square brackets] as shown in the example.

2. Select a probe type. **Automatic** uses SNMP or ICMP Echo for IP devices.

You can also select from a list of probes for web servers, mail servers, or any of the other probes shown in the menu. For a complete list of the built-in probes, see [Probe Reference \(Pg. 409\)](#).

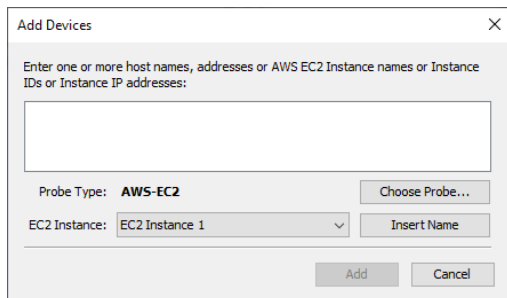
3. Enter a port number (if applicable to the probe).
4. Enter an SNMP Community string (if applicable).
5. Click **OK**.



To add an AWS device:

If you have AWS EC2 instances entered in Sever Settings, you may add AWS devices to any map. To add an AWS device:

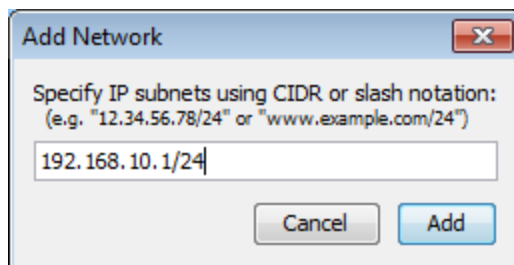
1. Click **Add Device**.
2. Click **Choose Probe...** The following dialog box appears:



3. Click **Insert Name** to insert AWS EC2 instance names into the edit box. (You can also manually type the AWS EC2 instance names into the edit box.)
4. Click **Add**. After a moment, you will see the devices with the AWS EC2 instances.

Network

Adds a network (oval) to the map. This is useful when Intermapper does not automatically detect the network because no SNMP-speaking devices are present.



The Add Network window is displayed. Enter the IP address. For more information on how IP network information is represented, along with a discussion of the /24 notation, see [Subnet Mask FAQ. \(Pg. 731\)](#)

After you click **OK**, a new network oval is displayed on the map representing that subnet. You can connect devices to this network by dragging their links as described in [Adding and Removing Links \(Pg. 52\)](#).

Link

You can use the Link command to manually add a link where none exists. This can be useful when a link is not added during the auto-discovery process or when you want to use links to specify that certain devices are dependent upon other devices. For more information on dependencies, see [Using Notification Dependencies \(Pg. 114\)](#).

To add a link manually:

1. Select two devices or networks. (The menu command is available only when two items are selected.) You can use Shift-click, Ctrl-click, or you can click and drag to draw a box around the items you want to select.
2. From the **Insert** menu, select **Link**. A link is displayed between the selected items. The link is permanently attached and remains connected when you move the items.

To remove a manually-added link:

Right-click the link and select **Remove**.

Auto-Discovery

You can use the Auto-Discover command to open the Automatic Device Discovery window. Using this command, you can automatically find network devices such as routers, hosts, switches, hubs, servers, and workstations and place them on the map. Specify the kinds of devices Intermapper finds and the breadth of its search.



Intermapper uses a starting address and scans for additional devices. By default, Intermapper starts with its router's address or its own [IP address \(Pg. 730\)](#).

You can, however, enter a different address or [DNS name \(Pg. 733\)](#) or [WINS name \(Pg. 739\)](#) (preceded by back slashes \\) as a starting point. If Intermapper finds SNMP-speaking routers with connections on other networks, it searches those networks, finding more devices (and possibly more routers) until the specified hop limit is reached.

The Autodiscovery window allows you to specify the starting address as well as specifying other options for the auto-discovery process.

Enter a starting host name, IP address, or IP subnet - Enter the name or address of a device that Intermapper should use to begin the auto-discovery process.

Specify a SNMP Community - Enter an additional SNMP read-only community string to be used to interrogate all devices. (Intermapper always attempts to read SNMP information using the default public community string. For more information, see [SNMP Frequently-asked Questions \(Pg. 734\)](#).)

Stay within __ hops of starting device - Stops auto-discovery after Intermapper searches the specified number of hops from the starting device.

Scan for devices on all networks - See [Scan Network \(Pg. 382\)](#).

Edit Filters - Click this button to open the Network Scanning window. See [Scan Network on page 382](#) below.

Automatically Layout - Select this check box to have the map laid out automatically (using the Organic layout).

Scan Networks

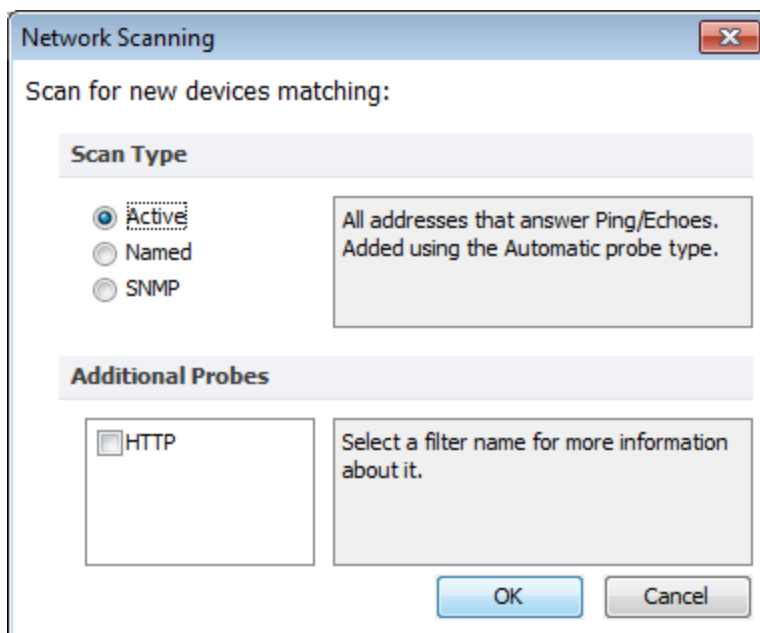
The auto-discovery process allows you to select which kinds of devices are added to the map. Intermapper applies a set of filters to the discovered devices. Only those that match the specified filters are added to the map.

Click **Edit Filter** from the **Automatic Device Discovery** window or select **Scan Networks** from the **Insert** menu to open the **Network Scanning** window.

The following options are available:

- **Active** - forces a complete IP address scan for each network. Intermapper sends an ICMP Ping request to each IP address in the subnet range.
- **Named** - each IP address in the subnet is looked up in the DNS. If a corresponding name is present, the device is added to the map.
- **SNMP** - Intermapper sends an SNMP GetRequest to each address in the range. Devices that respond are added to the map.
- **Additional Probes** - if the HTTP check box is selected, an HTTP probe is added if an HTTP response is received and the device becomes a probe group.

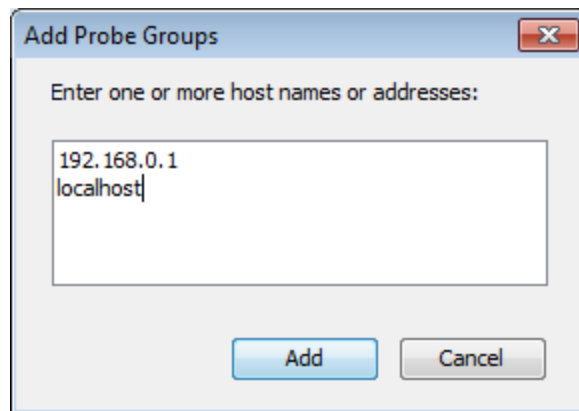
NOTE: You can select options that result in Intermapper's attempting to discover everything on a network. On a small or medium-sized network, this might be a reasonable approach. On large networks, Intermapper might discover far too many devices to make a workable map.



Empty Probe Group

Enter one or more addresses or domain names in the Add Probe Groups text box and click **Add**. An empty probe group is added for each name or address.

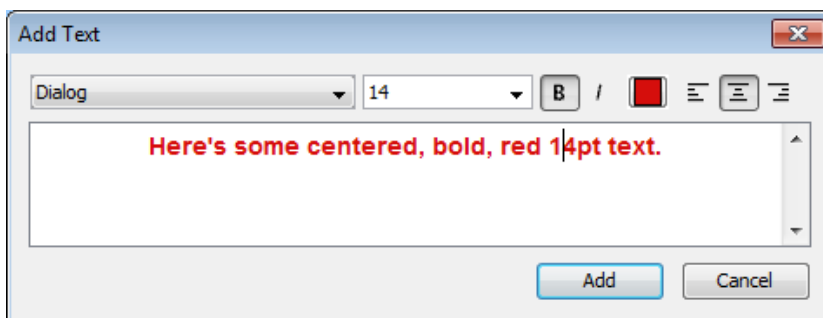
Text



You can use the Text command to place a block of text on a map at a specified location.

To add a text object to a map:

1. From the **Insert** menu, select **Text**. The Add Text window is displayed.
2. Enter the text you want to add to your map.
3. Use the formatting controls to format the text.
4. Click **OK**. A text object is displayed on the map.
5. Drag the text object to move it to the desired location.



Icon

You can use the Icon command to add an icon to a map. An icon inserted using this method is not associated with any device or network; it is simply a graphic element added to the map.

To add an icon to a map:

1. With the map editable, select **Icon** from the **Insert** menu. The Select an Icon window is displayed.
2. Select an icon and click **OK**. The icon is displayed in the map.

Map Benchmark

You can use the Map Benchmark command to define the latitude and longitude of a point on a map. This is useful if you are placing devices on the map using geographic coordinates. Each device is located on the map in relation to the map's benchmarks.

Group

You can use the Group command to create a probe group, a single device containing multiple probes. In order for the command to work, all selected devices must use the same IP address.

To create a probe group:

1. Select the devices you want to group. All selected devices must have the same IP address.
2. From the **Insert** menu, select **Group**. The selected devices are collapsed into a single device, containing a probe for each selected device.

NOTE: A probe group counts as one device in your device count.

Un-Group

You can use the Un-Group command to explode a probe group into individual devices.

To un-group a probe group:

1. Select the group you want to un-group.
2. From the **Insert** menu, select **Un-Group**. The probe group is replaced by individual devices, each configured with one of the probes from the original group.

NOTE: Each device counts as one device in your device count.

Format Menu

The Format menu contains commands that affect the appearance of individual items in the map. Items can be either devices (routers, servers, hosts, and so on) or networks (ovals, by default).

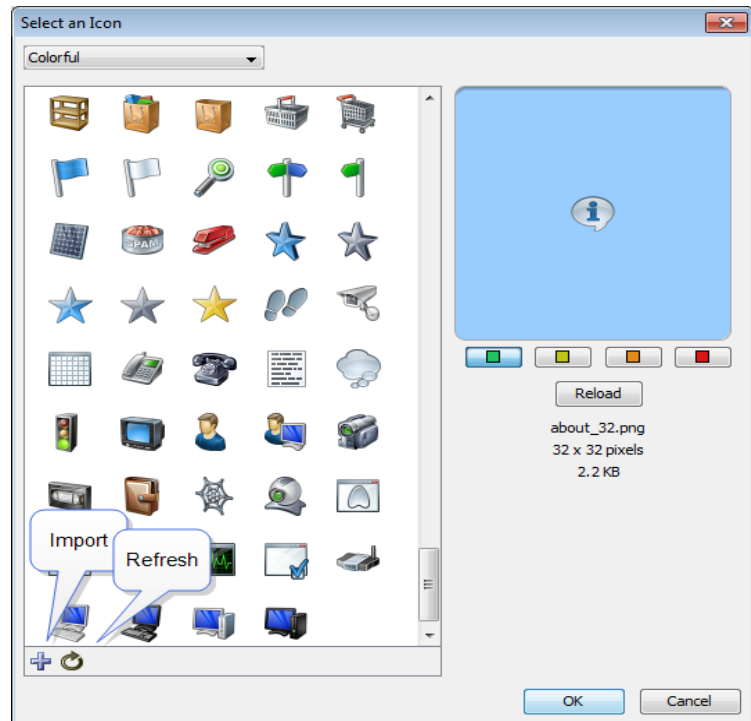
Menu Command	Description
Icon (Pg. 386)	Specifies the icon to associate with the selected items.
Label (Pg. 387)	Modifies the label of one or more items from the map. Devices and networks have text labels that identify the item. These labels can be generated automatically from information gathered from the device or contain static text that you manually enter.
Label Position (submenu) (Pg. 392)	Changes the position of the label relative to an item.
Align (Pg. 392)	Aligns the selected objects in relation to each other.
Rotate (Pg. 393)	Rotates the positions of the selected objects in relation to each other.
Scale (Pg. 393)	Scales the positions of the selected items in relation to each other.
Arrange (submenu) (Pg. 394)	Rearranges the selected items into a cycle, bus, or star.

Menu Command	Description
Context menu (Pg. 397)	Sets the font, size, and style of the selected devices from the Context menu.

Icon

Use the Icon command to select an icon for a device or network as it appears on your map. The Select an Icon window is displayed.

- Click an icon in the left box. It is displayed in the preview box on the right.
- Click **OK** to assign the icon to the selected devices or networks.
- From the menu at the top of the window, select a group of icons. The Built-in Shapes are displayed below.
- Click **Import** to import an image as an icon.
- When viewing groups of icons other than Built-in Shapes, click **Reload** to refresh the icon list in the left box.
- Drag an image to the window to import it as an icon.
- Drag a folder of images to the window to import the contents as a new icon group.








For more information, see [Custom Icons \(Pg. 81\)](#).

Built-In Shapes

You can use the icons in the Built-in Shapes icon group.

NOTE: Except for the Wire icon, all Built-in Shapes stretch to enclose the specified label text.

	Rectangle and Oval	<p>Rectangles and Ovals contain the text label within them.</p> <p>Rectangle is the default shape for a device. Oval is the default shape for a network.</p>
	Wire	<p>The Wire item is drawn as a straight line. Connections to the wire are drawn at right angles to the wire if possible.</p> <ul style="list-style-type: none"> • Drag the ends of the wire to resize it or change its orientation (angle). • From the Label Position submenu, select an option and position the label at one of nine positions.
	Cloud	Contains the textual label.
	Text	From the Format menu, you can configure font, style, and color of the text. The border of the item appears only when the item is selected.
	Icon	Select an icon from a set of default icons or create your own. For more information on adding icons to Intermapper's set, see Custom Icons (Pg. 81) .

Label

Each item in your map has a label. You can use the Label command from the Format menu to edit labels for the selected items.

Default Labels

- **Device** - the Smart Name of the device.
- **Network**- IP address or range of the network.

Edit Device Label Window

The following example shows the window for editing an item's label:

- **Top pane** - lists the label as it is displayed.

The entries in <...> are variables, which are filled in with the values from a particular device or network.

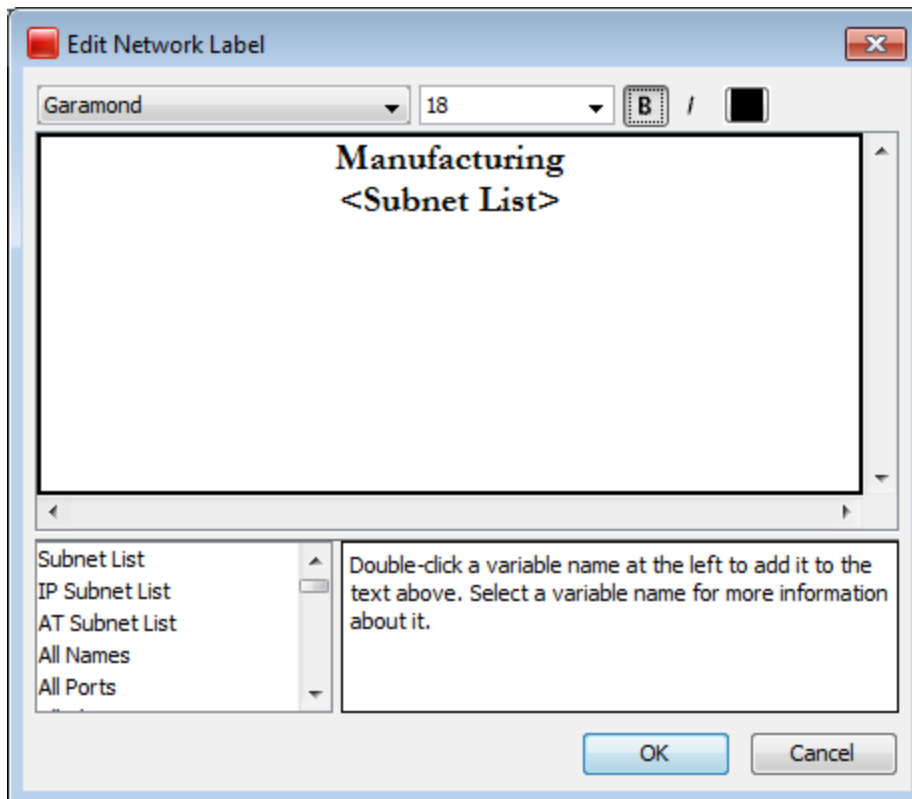
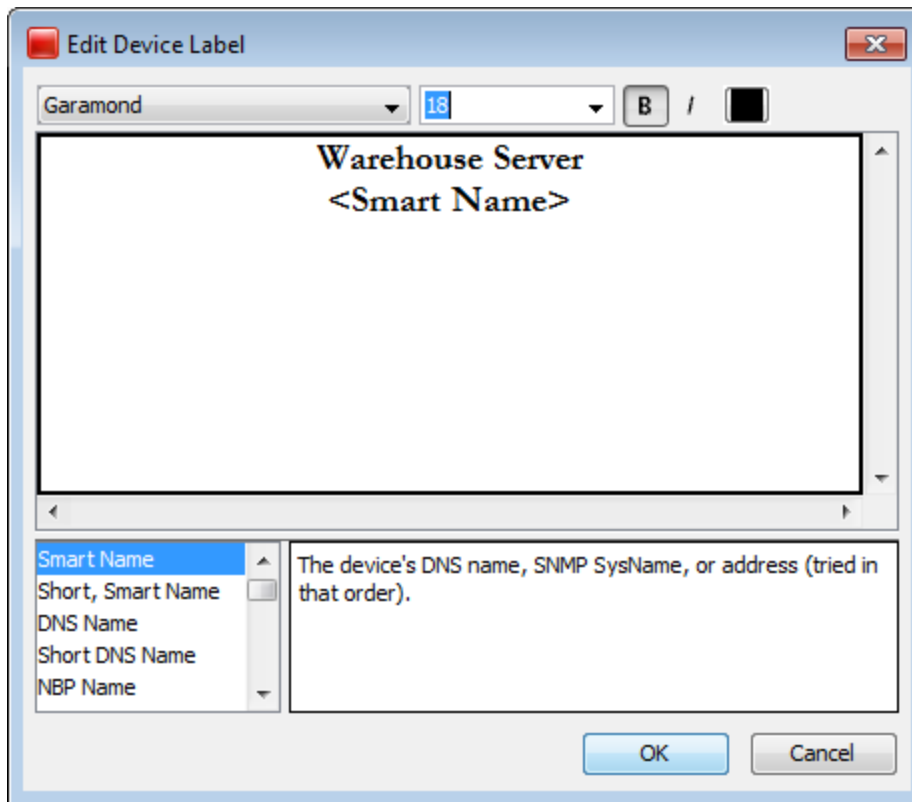
Press **Enter** to move text or variables to a new line.

- **Lower-left pane** - displays a list of variables that can be used in the top pane; the lower-right pane shows the definition of each variable

To insert a variable into the item's label:

1. From the top pane, place your cursor where you want to place the variable.
2. From the lower-left pane, double-click variable you want to insert. The variable appears in the top pane, enclosed in <...>.

Tip: To move text or a variable to a new line, place the cursor where you want the new line to start and press **Enter** on your keyboard.



Label Variables

You can use label variables to help you see information about the item you consider most important.

Device Variables

Smart Name (default)	The device's DNS name, SNMP SysName, or IP address, tried in that order.
Short, Smart Name	The leftmost part (up to the first period) of the device's Smart Name (except for IP addresses).
DNS Name	The full DNS name of the device (not the sysName or IP address).
Short DNS Name	The first part of the device's DNS name.
NBP Name	The device's Name Binding Protocol name.
SNMP SysName	The name of the device reported by the sysName variable.
SNMP SysDescr	The hardware and software information reported by the sysDescr variable.
SNMP SysContact	The contact person reported by the sysContact variable.
SNMP SysLocation	The location of the device reported by the sysLocation variable.
SNMP EnterpriseID	The enterprise ID of the device reported by the EnterpriseID variable.
SNMP EntSerialNum	The serial number of the device reported by the EntSerialNum variable.
SNMP EntMfgName	The manufacturer name of the device reported by the EntMfgName variable.
SNMP EntModelName	The model name of the device reported by the EntModelName variable.
Address	The network address of the device.
MAC Address	The device's MAC address. If the device has multiple interfaces, this field contains the MAC address associated with the device's main IP address (the same address as the address field).
Probe Type	The probe type used to test the device.
Comment	The comments associated with the device in the Get Info window.
TCP Port	The TCP port number that is being monitored if the device is using a TCP-based probe type.
WINS/NetBIOS Name	The device's WINS/NetBIOS name.

Network Variables

Subnet List (default)	A list of the subnets on the network.
IP Subnet List	A list of IP subnets on the network.
AT Subnet List	A list of AppleTalk subnets on the network.
All Names	List of interface names (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
All Ports	List of the device's ifIndex attached to the network, one per line.
All Aliases	List of interface aliases (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
All Descriptions	List of port descriptions attached to the network, one per line.
All Device-Names	List of device-labels: interface-name attached to the network, one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
All Device-Ports	List of device-label: ifIndex attached to the network, one per line.
All Device-Aliases	List of device-label: interface-alias attached to the network, one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
All Device-Descriptions	List of device-label: port-description attached to the network, one per line.
Switch Names	List of only switch's interface names (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
Switch Ports	List of only switch's ifIndex attached to the network, one per line.
Switch Aliases	List of only switch's interface alias (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
Switch Descriptions	List of only switch's port descriptions attached to the network, one per line.
Switch Device-Names	List of only switch's device-label: interface-name attached to the network, one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
Switch Device-Ports	List of only switch's device-label: ifIndex attached to the network, one per line.
Switch Device-Aliases	List of only switch's device-label: interface-alias attached to the network, one per line. This does not include devices that do not use SNMPv2c or SNMPv3.

Switch Device-Descriptions	List of only switch's device-label: port-description attached to the network, one per line.
Port Address	List of all numbered interfaces, one per line.
IP 3rd Octet	List of IP subnets on the network, one per line. Subnets are identified by their 3rd octet only.
VLAN	List of VLAN IDs on the network, one per line.
Port List	List of device-label: ifIndex attached to the network, one per line.
Interface Name	List of the interface names (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
Port Number	List of device's ifIndex attached to the network, one per line.
Interface Alias	List of interface alias (for devices that have them), one per line. This does not include devices that do not use SNMPv2c or SNMPv3.
Port Name	List of port descriptions attached to the network, one per line.

Label Position

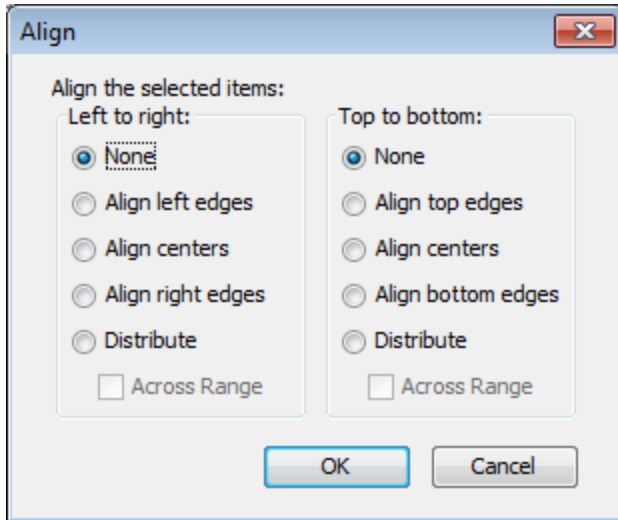
The following positions are available for labels:

- Top Left
- Top
- Top Right
- Left
- Center
- Right
- Bottom Left
- Bottom
- Bottom Right

NOTE: The label position affects only Wire and Icon shapes.

Align

You can align the selected items relative to each other. The Align buttons work like other drawing programs.



1. Select the items you want to align.
2. From the **Format** menu, select **Align**. The Set Alignment dialog is displayed.
3. Select the horizontal (left to right) and vertical (top to bottom) alignment options.
4. Click **OK**. The selected items are aligned as specified.

Distribute:

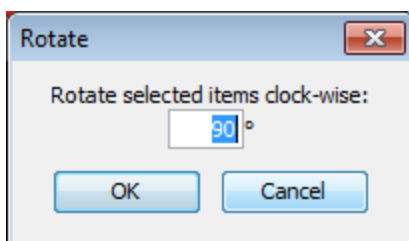
The Distribute option spaces the devices evenly.

Select the **Across range** check box to distribute the items evenly in the space that the items occupy.

Clear the **Across range** check box to draw the items with a small amount of space between the icons.

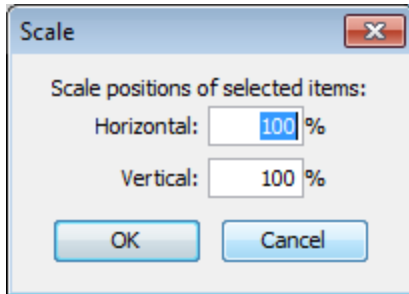
The example on the left shows the options for aligning items.

Rotate



Rotates the positions (but not the text or icons) of the selected items as a group. Items are rotated clockwise by the specified number of degrees . The example on the left shows the window for rotating items.

Scale



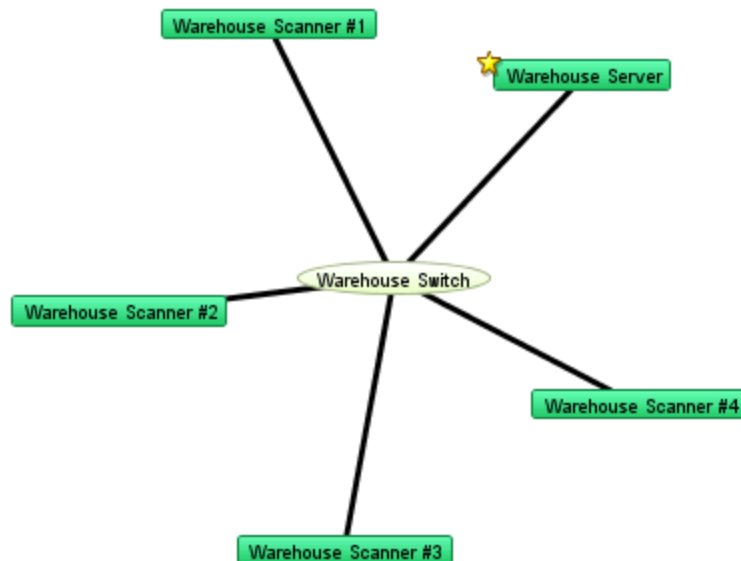
Specifies the amount (percentage) to change the positions both vertically and horizontally. Change the relative spacing of the selected items. This is useful after arranging items in a star to increase or decrease the diameter of the circle. The example on the left shows the window for scaling items.

Arrange (Submenu)

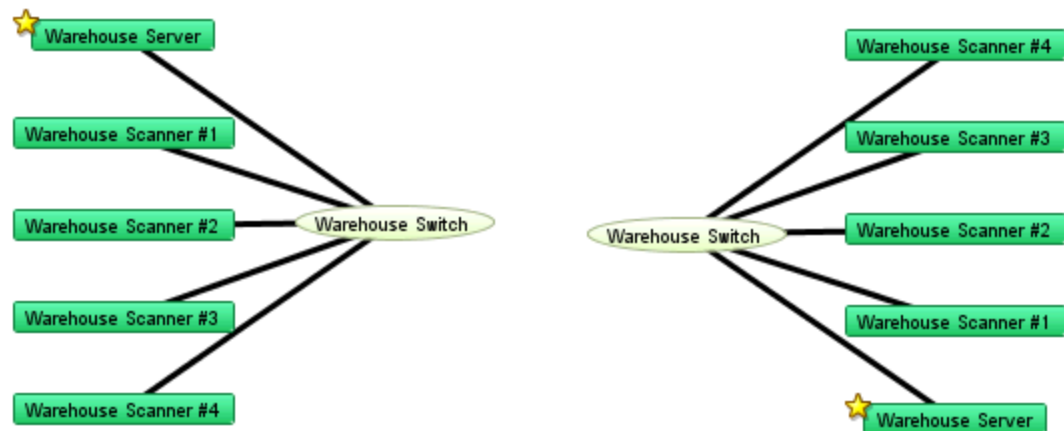
If no objects are selected, Organic and Tree commands work on all objects on a map. For Star and Bus, you must select at least one object. For Cycle, you must select at least two objects. All commands can work on two or more objects.

Organic

Arrange items with a minimum number of crossed links and overlaid objects.

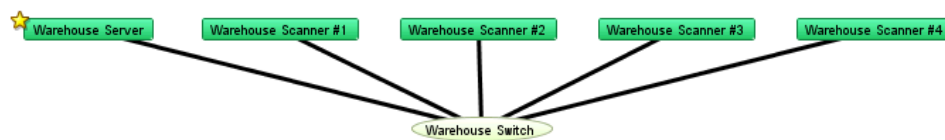


Tree

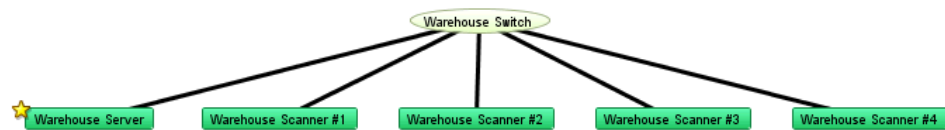


Tree - left

Tree - right



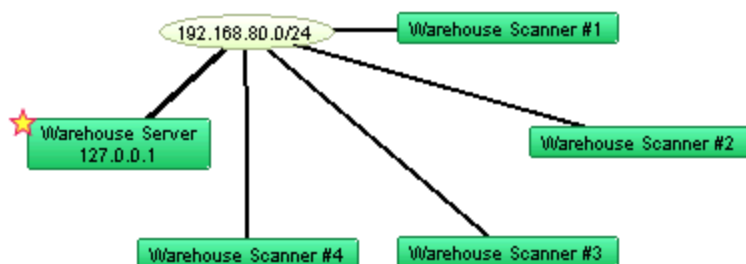
Tree - up



Tree - down

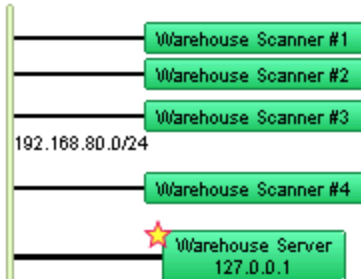
Cycle

You can move selected items into an oval around the edge of the window. This allows you to easily see the interconnections between devices on your network. The Cycle example in [Using the Arrange Commands \(Pg. 97\)](#) illustrates the Cycle command's action.



Bus

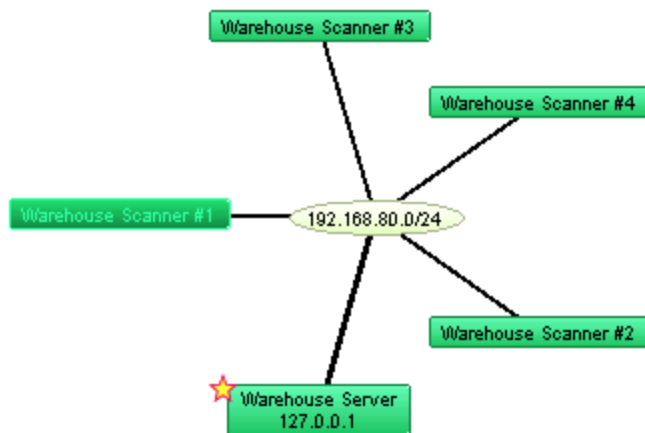
You can arrange items into a vertical column, changing the item that connects them into a vertical bus shape. This can represent a group of devices connected by an ethernet or other broadcast medium. The Bus example in [Using the Arrange Commands \(Pg. 96\)](#) illustrates the Bus command's action.



NOTE: The Bus command affects only items that are connected to networks.

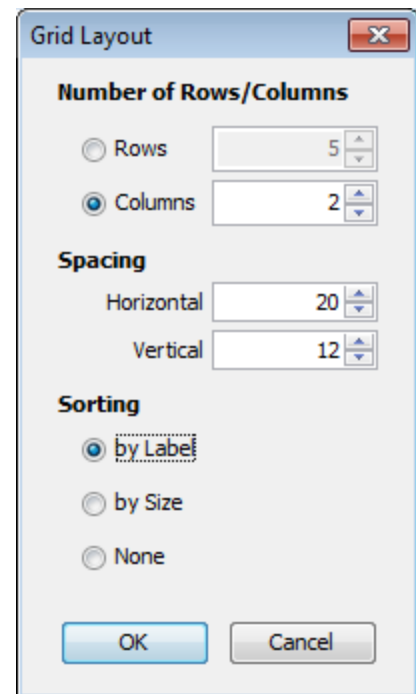
Star

You can arrange items so they surround a network or device that connects them. The devices are spaced equally around the circumference of a circle. The Star example in [Using the Arrange Commands \(Pg. 96\)](#) illustrates the Star command's action.



Grid

You can arrange items to form a grid with a specified number of columns or rows. You can sort the grid by Label, Size, or None. If you sort by None, the grid is created relative to the upper-left icon in the selection.



Features Available Only From the Context Menu

Font, Size, and Style

To change the attributes for each label in your map:

1. From the **Context** menu, select **Font**, **Size**, or **Style**.
2. Make your changes.
3. Click **OK**.

NOTE: The Font, Size, and Style attributes affect all labels in the selected objects. The Color attribute affects the text color only when the shape is set to Text. These functions are also available in the Edit Device Label dialog.

Window Menu

The Window menu lists all open maps. Using the Window menu, you can change certain aspects of window appearance and access other Intermapper windows.

Menu Command	Description
Minimize (Pg. 398)	Minimizes the front-most window.

Menu Command	Description
<u>Zoom (Pg. 398)</u>	Expands or contracts the front-most window to the size necessary to show all devices. If all items cannot be shown at the same time, this changes the current screen to its maximum size. If the Toolbar is shown, the minimum window width is the width of the toolbar.
<u>Send to Back (Pg. 398)</u>	Sends the front-most window to the back.
<u>Slideshow (Pg. 399)</u>	Rotates between open map windows.
<u>Logs (Pg. 399)</u>	A submenu of log files that allow you to view a history of events, outages, the Debug log, or custom logs.
<u>Charts (submenu) (Pg. 400)</u>	A submenu of defined charts. <div> NOTE: In the Charts window, a Show Chart context menu item has the same effect. </div>
<u>Map List (Pg. 400)</u>	Opens the Map List window or brings it to the front if it is already open.
<u>Device List (Pg. 401)</u>	Opens the Device List window.

Minimize

You can minimize the front-most Intermapper window.

Zoom

You can expand the front-most window to the largest size necessary to show all devices, or to the maximum size of its current screen, if all items cannot be shown at the same time.

Select **Zoom** to expand the front-most window or to return the window to its original size.

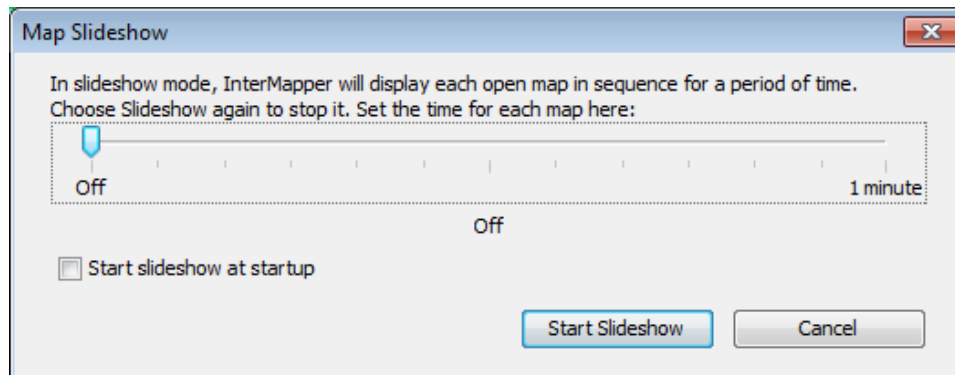
Send to Back

You can send the front-most window to the back.

Floating windows associated with that window, such as Status windows, are hidden.

Slideshow

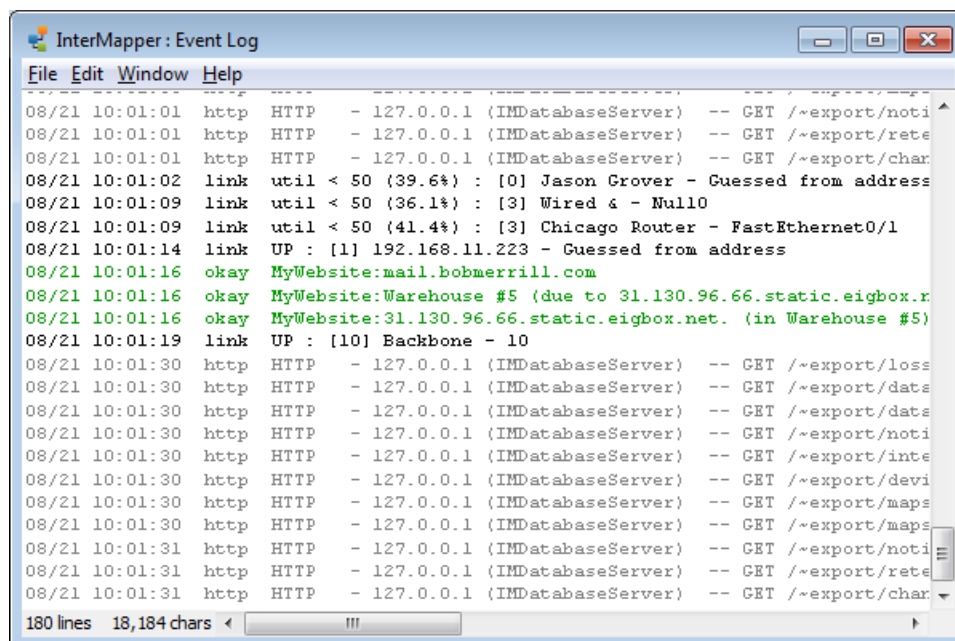
You can rotate the open map windows at a specified rate.



- From the **Window** menu, select **Slideshow** and specify the amount of time each map is shown.
- Select **Slideshow** again to stop the slideshow.

Logs

You can select from a submenu of log files to view a history of events, outages, connections to the web and remote servers, or custom logs.




Each time a device changes state, an entry is added to the event log window. In addition, Intermapper logs messages for the following events:

- Acknowledgments (including the text entered by the operator)
- Opening and closing maps
- Program startup
- DNS errors
- Errors when sending a notification
- Receipt of an SNMP trap

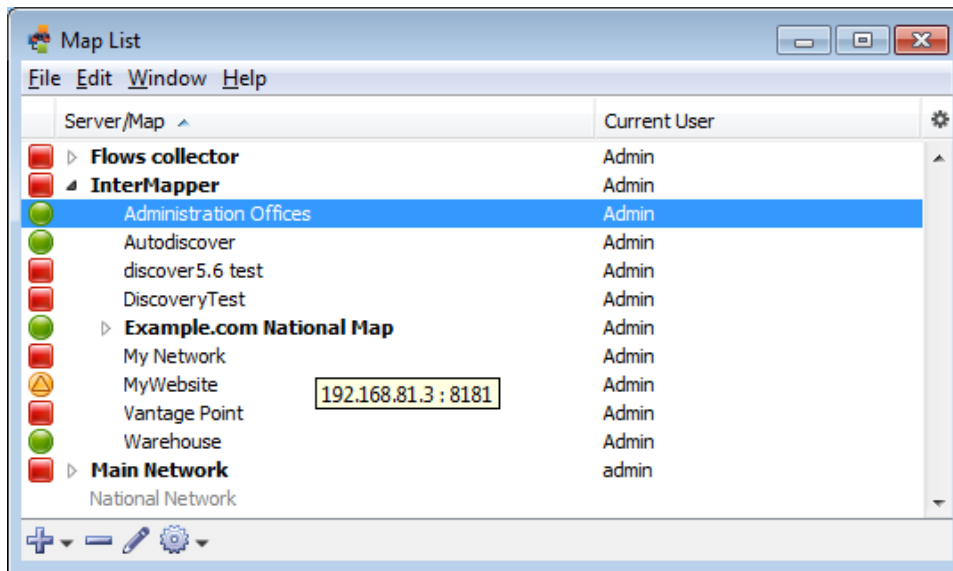
For more information, see the Overview of [Information and Log Windows \(Pg. 204\)](#).

Charts

	<p>This option lists all available charts for the current map window.</p> <ul style="list-style-type: none">• Select and clear the check box on individual charts from the submenu to show or hide them.• Select Show Charts to show all charts.• Select Hide Charts to hide all charts.
---	--

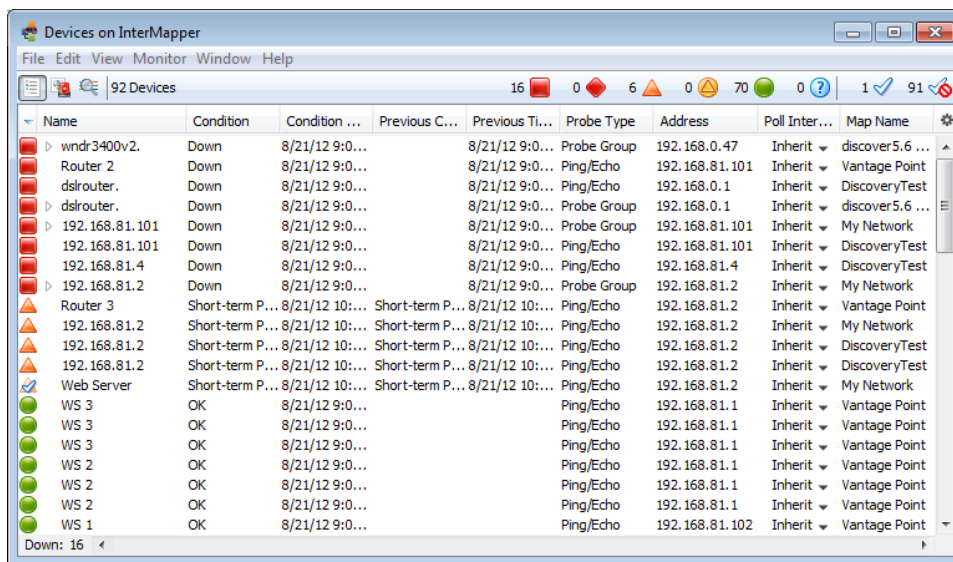
Map List

You can open the Map List window or bring it to the front.



Device List

You can view the Device List window, which shows a global device list. InterMapper maintains a server-wide list of all devices that are monitored on all enabled maps that the current logged-in user can see.



For more information, see [The Device List Window](#).

Help Menu

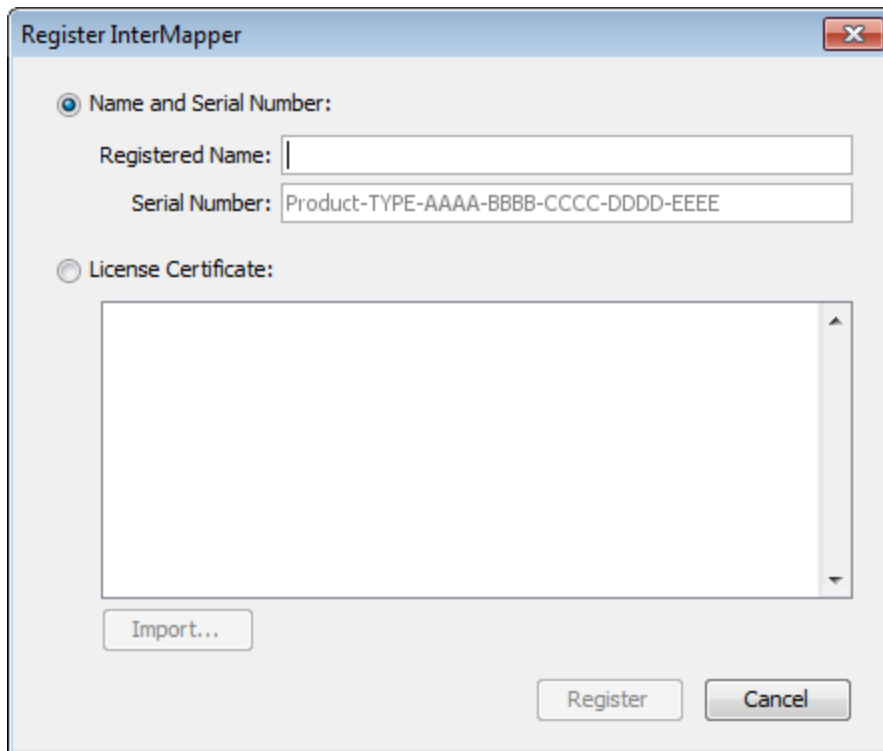
You can use the Help menu to view the online help system.

Menu Command	Description
About Intermapper	<p>Opens the Intermapper software information page.</p> <div> NOTE: On macOS systems, this command is available from the Intermapper or IM Remote Access menu. </div>
Register Intermapper, Register Intermapper RemoteAccess	Opens the Intermapper or Intermapper RemoteAccess registration window.
Intermapper Help, Intermapper RemoteAccess Help	Opens the Intermapper help system.
Send Feedback	Opens the Send Feedback window.
Send a Screenshot	Opens the Send Feedback window with a screenshot attached.
Diagnostics (submenu)	Lists available diagnostic commands, described below.

About Intermapper

This menu command opens the Intermapper software information page. From this page, you can view information about the software and its contributors, as well as information about memory use, platform, operating system, and the current Java version.

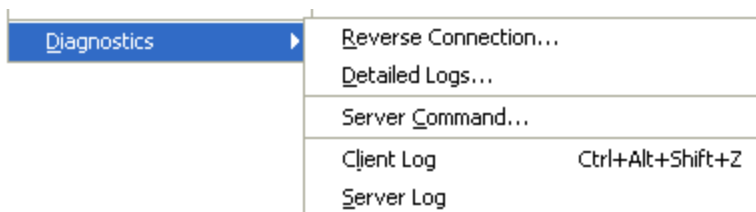
Registering Intermapper and Registering Intermapper RemoteAccess



The Register InterMapper menu command opens the Register InterMapper (or InterMapper RemoteAccess) window. This is the same window displayed when you click Add from the Registration pane, found in the Server Information section of the Server Settings window.

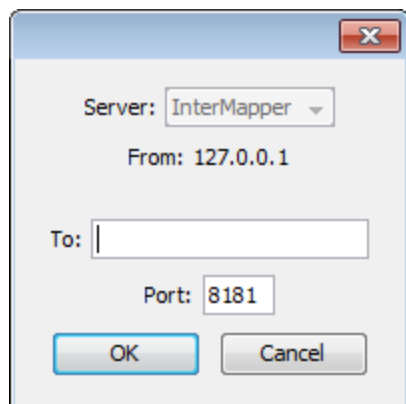
Diagnostics (Submenu)

You can create a Reverse Connection to a server for troubleshooting, to view Detailed Logs, to execute a server command, or to view the Client or Server log.



Reverse Connection

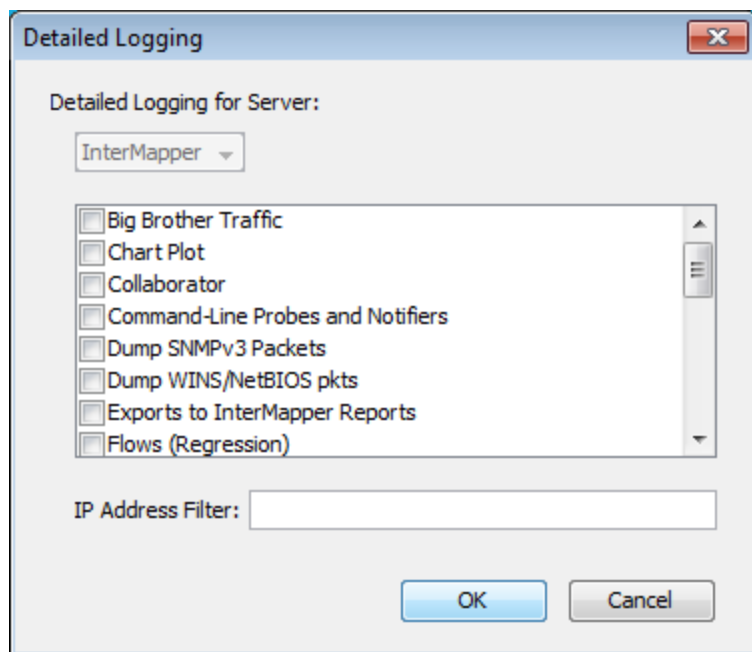
You can initiate a reverse connection from your InterMapper server to a copy of InterMapper RemoteAccess client for troubleshooting purposes. This allows tech support personnel to view a customer's server. Using a reverse connection, the customer can instruct their server to connect out to another InterMapper RemoteAccess without changing any firewall configurations.



Detailed Logs

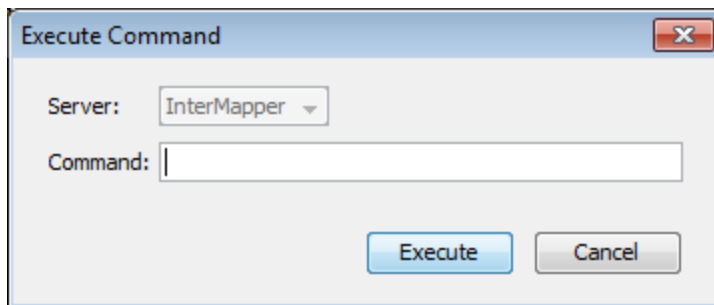
You can toggle detailed logging for a variety of different Intermapper events by specifying the type of event for which you want detailed logging to be displayed. Detailed information is sent to the server's Debug Log file. You can enter an IP address in the Filter field to limit the logged information to a particular IP address.

When detailed logging is enabled, a significant quantity of data can be logged in a relatively short period. To conserve server disk space, use this feature only when needed for troubleshooting.



Server Command

Intermapper RemoteAccess can instruct a server to execute certain commands, and to display the output in the Debug Log file. The major command is `snmpwalk`; it and other commands are described in the Developer Guide.



Client Log

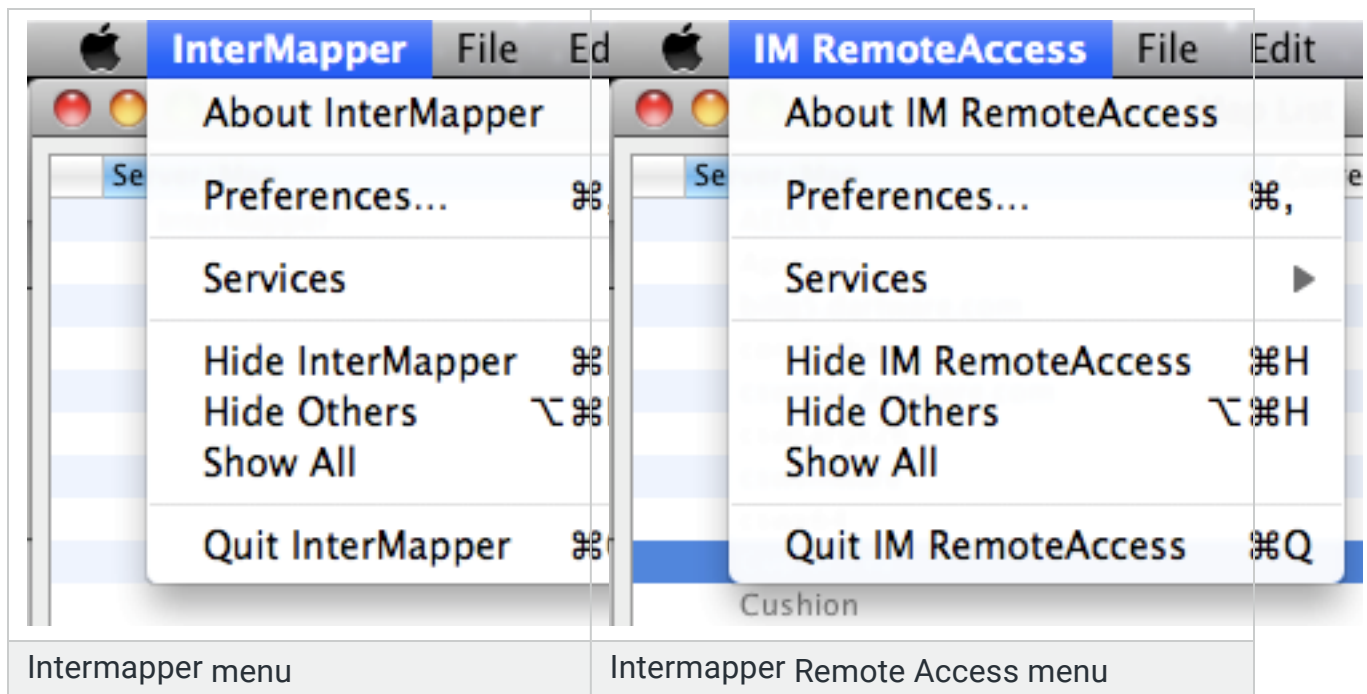
You can open the Client Log window, which contains the messages sent between the client and the Intermapper server. This information can be useful for debugging Intermapper problems.

Server Log

You can open the Debug log file for the server. It can also be opened from the Window > Logs > Debug menu.

Intermapper Menus

macOS systems add an Intermapper menu or IM Remote Access menu. These menus contain menu items that are normally displayed in other menus on other platforms.



The **About**, **Preferences**, and **Quit** menu items are displayed in these menus on macOS systems.

For information on these features, see the following topics:

- About Intermapper, About IM Remote Access: [Help menu](#)
- Preferences: [Edit menu](#)
- Quit: [File menu](#)

Context Menus

You can select options available for a particular device, network, link, map, window or other screen object. The options available in the Context menu change depending on the object you are using to activate the context menu.

To execute a command from the Context menu:

1. Right-click or Ctrl-click the object for which you want to activate the context menu. The Context menu is displayed.
2. Select a command. Commands appropriate to the selected object and current context are displayed.

Keyboard Shortcuts

Intermapper can run on multiple platforms. Since different platforms have different modifier keys (keys that change the function or meaning of another key), the keyboard shortcuts vary slightly from one platform to another.

General Rules

The primary difference is between macOS and Microsoft Windows systems. Use the following rules, depending on your platform:

To select a menu item using the keyboard:

macOS :	Command key
Windows, Linux:	Ctrl key

To choose an item from a context menu:

macOS :	Ctrl-click (hold Control, click with the mouse)
Windows, Linux:	Right-click

Finding Menu Item Shortcuts

Each menu item that has a shortcut shows the key required for the shortcut in the menu.



Keyboard Navigation











You can use the keyboard to speed up a number of operations. For a complete set of navigation keystrokes, see [Keyboard Navigation \(Pg. 407\)](#).

Other Shortcuts

A number of other shortcuts are available to help you work efficiently. For additional selection and scrolling techniques, see [Quick Reference - Editing Your Map \(Pg. 1\)](#).

Keyboard Navigation

 <p>(in Browse mode)</p>	Scrolls the view.
 <p>(in Edit mode)</p>	Micro-adjusts the position of the selected item.

    <p>Alt or Option <arrow key> (in Edit mode)</p>	Scrolls the view in Edit mode.
Home	Scrolls to Upper Left.
End	Scrolls to Lower Right.
Page Up	Scrolls one page up.
Page Down	Scrolls one page down.
Tab	Toggles between Browse and Edit Mode.
Cmd/Ctrl + Click	Centers the map.
Cmd/Ctrl + Drag	Scrolls map in any direction.
Cmd/Ctrl + Scroll Wheel	Zooms in or out dynamically.
Cmd/Ctrl + Option + Drag	Zooms in on selected rectangle.
Cmd/Ctrl + Up	Zooms In.
Cmd/Ctrl + Down	Zooms Out.
Cmd/Ctrl + 	Displays Icons.
Cmd/Ctrl + 	Displays List.
Cmd/Ctrl + 	Displays Notifiers.
Cmd/Ctrl + 	Displays Charts.
 (Numeric Keypad)	Zooms In.
 (Numeric Keypad)	Zooms Out.

Probe Reference

You can select the probe you want to use to query the device.

Using the Probe Selection Window

From the Probe Selection window, you can do the following:

- Click the plus sign (+) from the left pane to expand a probe group.
- Click the minus sign (-) from the left pane to collapse a probe group.
- Click a probe from the left pane to select the probe. Information about the probe and controls for setting any available parameters are displayed in the right frame.
- Click **Default** to set the probe back to default setting for that probe type.

About Probes

Intermapper includes a large number of built-in probes. For a full index and detailed descriptions of built-in probes, see the [Probe Index](#).

- [Basic Probes \(Pg. 412\)](#) - covers the majority of your needs for probing devices.
- [SNMP Probes \(Pg. 414\)](#) - performs a wide variety of queries on SNMP devices.
- [Network Devices \(Pg. 424\)](#) - queries network devices, such as routers, switches and UPS units.
- [PowerShell Probes](#) - obtains information from Microsoft Windows machines using PowerShell scripts.
- [Servers-Standard \(Pg. 465\)](#) - queries various devices using one of many Standard protocols.
- [Servers-Proprietary \(Pg. 498\)](#) - queries various devices using one of many Proprietary protocols.
- [Miscellaneous Probes \(Pg. 519\)](#) - used for a variety of uses. You can find the Demo, Non-Polling, and TCP Check probes. You can also find the Legacy probes (included to support older maps) and the template for developing Nagios and Command-line probes.
- [Wireless Probes \(Pg. 524\)](#) - obtains vendor-specific information from a number of wireless devices.

- [WMI Probes \(Pg. 576\)](#) - If Intermapper is installed on a Microsoft Windows machine, use these probes to get detailed information from Microsoft Windows systems through the Microsoft Windows Management Instrumentation (WMI) interface.

Packet-Based Probes

Probes such as Ping/Echo, SNMP Traffic, NNTP, and RADIUS send UDP packets to the device being tested and await a correctly formatted response.

For more information on packet-based probes, see [About Packet-based Probes \(Pg. 589\)](#) and [Network Device Probes \(Pg. 424\)](#).

Probe Timeout Period

You can configure the probe timeout period by selecting **Set Timeout** from the Set Probe Info submenu. If no response is received within the specified timeout period, Intermapper tries again by sending another request packet. This process is repeated until either a response is received or the number of requests sent exceeds the Number of Lost Packets threshold set for the map (the default is 3).

Response Packet Integrity

All packet-based probes check the integrity of the response they receive and some can set the status of the device (Alarm, Warning, and OK) based on the severity of a problem.

TCP-Based Probes

Probes such as HTTP, SMTP, LDAP, and others test the ability of a server to accept a TCP connection on a specific listening port and to respond to a scripted interchange.

For more information on TCP-based probes see [Server Probes - Standard \(Pg. 465\)](#).

TCP-Based Interchanges

1. Intermapper first attempts to connect to the specified port at the device's address.
2. If this connection attempt fails, Intermapper shows the device in the DOWN state.

If Intermapper successfully connects to the listening port, Intermapper sends protocol-specific commands through the TCP connection to test the server's responses and compare them to expected values.

3. Intermapper changes the status of the device (for example, ALARM, WARNING, OKAY, or DOWN) if an error condition is detected or if the probe is interrupted for any reason.
4. If Intermapper does not receive a proper response within 60 seconds, or if the TCP connection is lost while waiting for a response, the probe sets status of the device to the proper condition.

Miscellaneous Probes

Intermapper includes the following miscellaneous probes. They are described in detail in [Miscellaneous Probes \(Pg. 519\)](#).

- **Demo probe** - creates demonstration maps, which simulate a network and its activity.
- **Legacy probes** - probes that are superseded by other probes. These are included to support older maps.
- **Nagios** - selects plugins from the Nagios monitoring system. Intermapper can use these plugins to test devices. For more details, see the Nagios Plugins page in the Developer Guide.
- **Non-polling probe** - turns probing off for the specified probe.
- **Prototype SNMP probe** - creates custom SNMP probes.
- **TCP Check probe** - monitors the number of TCP connections to an SNMP-enabled device and to send an alarm when a specified number of connections is exceeded.

Troubleshooting PowerShell Probes

If you are having trouble getting PowerShell probes to work, you can look in the Debug Log information.

Each time a PowerShell probe is selected or its parameters change, a connectivity test is run. If the test is successful, the probe runs at the next polling interval. For the connectivity test and for each time a PowerShell probe runs, the following entries are created:

- One entry shows the input string sent to `stdin`.
- A second entry shows the variables returned by the probe, enclosed in `\{...}` and followed by the string assigned to `stdout`.

Basic

Automatic

This probe checks if the device responds to SNMP. If it does not, the probe is set to Ping/Echo.

Intermapper sends an SNMP GetNextRequest for the sysName, sysObjectID, and sysServices OIDs (1.3.6.1.2.1.1.5.5, 1.3.6.1.2.1.1.5.2, and 1.3.6.1.2.1.1.5.7, respectively) using the specified SNMP read-only community string. After a valid SNMP response is received, Intermapper sets the device's probe to SNMP. If not, the Ping/Echo probe is used.

Filename: `com.dartware.automatic`
Version: 1.7

Map Status

This probe allows Intermapper to monitor the state of a map running on an Intermapper server. Intermapper periodically queries the specified map and sets the device status to the status of the worst item on that map. Double-click the device to view specified map.

The easiest way to use this probe is to drag a map from the Map List to another editable map. You can also create a device using the DNS name or IP address of the Intermapper server containing the map or localhost for a local map. Specify the following:

Map Name - The name of the map on the remote server.

Username - A user name that has read-permission on the map.

Password - The password of the specified user.

Filename: `com.dartware.map.status`
Version: 1.8

Ping/Echo

This probe sends an ICMP echo request packet to the target device to determine if it is active and responding.

Number of Data Bytes - the number of bytes of ICMP data to send. By default, 20 bytes of data is sent. This value is between 16 bytes and 2000 bytes.

Data Pattern - the hexadecimal pattern repeated throughout the payload contents.

Tip: To send a 1500-byte IP packet to an IPv4 target, set the number of data bytes to 1472. To send the same IP packet size to an IPv6 target, set the number of data bytes to 1452.

Intermapper sends the ping packet and waits for a response for the specified Timeout. If no response is received within the specified time, Intermapper re-sends the echo request and waits again for the specified Timeout. When the probe reaches the device's limit of the number of pings to send (as determined by the device or map's limit) without receiving a response, the device status is changed to DOWN.

By default, the number of echo requests is 3 and the default timeout is 3 seconds. It can take up to 9 seconds to change a device status to DOWN.

Filename: `com.dartware.ping`
Version: 2.0

SNMP Traffic

This probe retrieves system and traffic information from an SNMP-enabled device. This information comes from the system and interfaces groups of SNMP MIB-II.

It shows traffic (bytes/second, packets/second, and errors/minute) for each interface. Right-click a link to open the interface's Status window.

The probe also shows sysLocation, sysContact, and sysUptime from the system group in the device's Status window.

NOTE: This is exactly the same probe as the SNMP MIB-II probe found in earlier versions of Intermapper. It has been renamed to more accurately reflect its purpose.

Filename: `com.dartware.snmp`
Version: 1.7

SNMP

Basic OID

This probe allows you to monitor a single, user-defined MIB variable.

Parameters

Object Name - (optional) the name of the value that you want to monitor. This parameter value is used only for display in the popup window and chart legend.

Object ID - the object identifier (OID) of the value that you want to monitor. To retrieve the value of a MIB variable that is not in a table, the OID must end with .0 (for example, 1.3.6.1.2.1.1.1.0).

This probe retrieves a lot of SNMP information from the device, including the MIB-II system group and the interfaces table. If you want to monitor a single SNMP variable, use the SNMP/Single OID probe.

Filename: `com.dartware.snmp.basic`
Version: `0.7`

BOM Trap

This probe is triggered by traps from the BOM and puts the icon in an alarm state. The alarms come in three types: warning, alarm, and critical. Upon receiving an OK, the icon returns to a normal state.

Format of Net-SNMP `snmptrap` command

```
snmptrap -v 1 -c commString localhost
1.3.6.1.4.1.10035 IPAddress generic-trap specific-trap uptime {Monitor
Items}
```

Where specific-trap

- InterMapper Warning : mxMonitorFailure = 20
- InterMapper Warning : mxMonitorFailure = 30
- InterMapper Warning : mxMonitorFailure = 32

- InterMapper Okay : mxStatusNormal = 21
- InterMapper Alarm : mxStatusWarning = 22
- InterMapper Critical : mxStatusCritical = 23

Display items are as follows:

- Device status : specific-trap
- Computer name : mxTargetComputer
- Instance ID : mxInstanceId
- Group name : mxGroupName
- Item name : mxMonitorName
- Action name : mxActionName
- Result code : mxResultCode
- Monitor value : mxMonitorValue
- Monitor status : mxMonitorStatus
- Exit code : mxExitCode
- User message : mxUserMsg

Parameters

None

Filename: `com.unfake.snmp.bomtrap.txt`
Version 1.0

Comparison

This probe retrieves a single SNMP MIB variable, compares it to a specified value, and uses the result to set the device's status. It also displays the value in the Status window.

Parameters

Variable - the MIB name or OID to retrieve. If you have imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Test - changes the status to ALARM if the device is **Equal** or **NotEqual** to the **Value** parameter.

Value - the value to compare against.

Severity - the status to use if the comparison fails.

Legend - a text string that identifies the variable in the Status window and strip charts. If left blank, the variable's name or OID is used.

Units (optional) a text string that is displayed next to the value in the Status window, intended for use as a unit of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidcomparison.txt`
Version: 1.11

High Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified thresholds below. If the value goes above any of the specified thresholds, the device changes to the specified state.

Parameters

Variable - the MIB name or OID to retrieve. If you imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter its OID.

Critical, Alarm, and Warning - the threshold that compares each severity. Thresholds can be positive or negative numbers.

Legend - a text string that identifies the variable in the Status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status window. This is usually used for units of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidhigh.txt`
Version: 1.6

Low Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified threshold. If the value goes below any of the thresholds, the device changes to the specified state.

Parameters

Variable - the MIB name or OID. If you imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter the OID.

Critical, Alarm, and Warning - compares each severity. Thresholds can be positive or negative numbers.

Legend - a text string that identifies the variable in the Status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status window. Usually used for units of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidlow.txt`

Version: 1.6

Range Threshold

This probe retrieves a single SNMP MIB variable and compares it to the specified thresholds. If the value goes outside the specified range, the device changes to the corresponding state.

Parameters

Variable - the MIB name or OID. If you imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter the OID.

Critical, Alarm, and Warning - compares each severity. Thresholds can be positive or negative numbers.

Legend - a text string that identifies the variable in the Status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status window. Usually used for units of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidrange.txt`

Version: `1.7`

Restricted Interface

This probe is identical to the Basic SNMP Traffic probe, except that it restricts the visible interfaces to those that match the specified Interface Description.

Parameter

Interface Description - specifies the interfaces to display. Any interface with a value of `ifDescr` that matches this pattern is visible on the map. Non-matching interfaces are hidden.

Filename: `com.dartware.snmp.restrictedint.txt`

Version: `0.2`

Single OID Viewer

This probe retrieves a single SNMP MIB variable and displays it in the device's Status Window.

Parameters

Variable - the MIB name or OID. If you imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter the OID.

Legend - a text string that identifies the variable in the Status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status window. Usually used for units of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidsingle.txt`

Version: 1.5

SNMP High PPS

This probe monitors the `ifInPackets` and `ifOutPackets` statistics of the specified device interface and sets the state of the device to Alarm or Warning when the packet rate (in packets/second) exceeds specified thresholds. It sets the state to Down if the interface's `ifOperStatus` is not equal to 1 (Up).

Parameters

Port Number - the `ifIndex` of the port to monitor.

Warn Threshold and **Alarm Threshold** - threshold values in packets-per-second.

Filename: `com.dartware.snmp.pps.txt`

Version: 0.6

SNMPv1 High Traffic

This probe monitors the `ifInOctets` and `ifOutOctets` traffic statistics of a particular interface on the device and sets the device to Alarm or Warning when the traffic exceeds specified thresholds. It sets the device's state to Down if the interface's `ifOperStatus` is not equal to 1 (up).

Parameters

Port Number - the `ifIndex` of the port to monitor.

Warn Threshold and **Alarm Threshold** - thresholds in bytes per second.

Filename: `com.dartware.snmp.traffic.txt`

Version: 0.4

SNMPv1 High Util

This probe monitors the utilization of ifInOctets and ifOutOctets traffic statistics of a particular interface on the device, and sets the device to Alarm or Warning when traffic exceeds specified utilization thresholds. It sets the device's state to Down if the interface's ifOperStatus is not equal to 1 (up)

Parameters

Port Number - the ifIndex of the port to monitor.

Warn Threshold and **Alarm Threshold** - threshold, specified as a percentage of bandwidth utilization.

Filename: `com.dartware.snmp.traffic-util.txt`
Version: 0.3

String Comparison

This probe retrieves a single SNMP MIB variable, compares it to a specified value, and sets the device's severity based on the comparison. It also displays the value in the Status Window.

Parameters

Variable - the MIB name or OID. If you imported the MIB for this device, enter the symbolic name for this value. Otherwise, enter the OID.

Test - specifies if the device is equal to the Value parameter or not.

Value - the value to compare with the MIB variable's value.

Severity - the severity level to use if the value does not match the specified value.

Legend - a text string that identifies the variable in the Status window and in strip charts. If left blank, the variable's name or OID is used.

Units - a text string displayed next to the variable's value in the Status window. Usually used for units of measure (packets/sec, degrees, and so on).

Tag - a short text string that identifies a particular class of dataset. Tags are used to correlate different variables from different probes that describe the same type of data, such as CPU% or temperature.

Filename: `com.dartware.snmp.oidstrcomparison.txt`

Version: 1.9

Table Viewer

This probe shows the contents of several useful tables from common SNMP MIBs. It retrieves its data by walking the SNMP data values in the tables.

Parameters

ifTable - The Interfaces table gives information about the physical and logical interfaces of the device. It is defined in MIB-II (RFC-1213) and updated in the IF-MIB. It shows the following columns:

- ifIndex
- ifDescr
- ifType
- ifSpeed
- ifPhysAddress
- ifOperStatus
- ifAdminStatus.

ifXTable - the Extended Interfaces table defined in IF-MIB. It adds the ifName and ifAlias fields/columns to those shown in the ifTable.

Traffic Counters -traffic counters ifInOctets and ifOutOctets from the MIB-II ifTable and the ifHCInOctets and ifHCOctets from the IF-MIB. To determine the traffic rate, refresh the window and compare two separate readings. The difference divided by the time between the refreshes (in seconds) is the number of bytes/second.

tcpConnTable - information about any present connections. It is defined in MIB-II. Variables include the following:

- tcpConnLocalAddress
- tcpConnLocalPort
- tcpConnRemAddress
- tcpConnRemPort.

udpTable - information about any present UDP listeners: Variables include udpLocalAddress, udpLocalPort. It is defined in MIB-II.

ipAddrTable - the IP address/mask/broadcast address for each interface. It is defined in RFC-1213, and updated in the IP-MIB. Includes the following:

- ipAdEntAddr
- ipAdEntIfIndex
- ipAdEntNetMask
- ipAdEntBcastAddr
- ipAdEntReasmMaxSize.

ipRouteTable - the table (currently deprecated) that comes from RFC-1213 (MIB-II).

ipCidrRouteTable and **ipForwardTable** - the tables that come from the IP-FORWARD-MIB. Shows information about CIDR multi-path IP Routes.

NOTE:

The ipForwardTable obsoletes the ipRouteTable of MIB-II and is in turn obsoleted by the ipCidrRouteTable.

ipNetToMediaTable - the Net Address-to-Media Address table (also known as the ARP Table). It is defined in RFC-1213. Includes the following:

- ipNetToMediaIfIndex
- ipNetToMediaNetAddress
- ipNetToMediaPhysAddress
- ipNetToMediaType.

dot1dTpFdbTable - the Bridge MIB (RFC1493) shows the forwarding database for transparent bridges.

A link to each table appears in the Status window. Click the link to see the contents of the table on the selected device.

Parameters

None

Filename: `com.dartware.snmp.tableviewer.txt`

Version: 1.10

Trap Viewer

This probe listens for trap packets and displays the contents of a trap in the Status window. It does not actively poll the device and takes no action based on the contents of the trap.

All variables parsed from the trap packet are displayed in the device's Status window. You can use this probe as a prototype for making your own trap probes.

How the Trap Viewer Probe Works

When a trap arrives, the probe parses the trap to retrieve values from the trap's header along with the first ten items in its Varbind List. Each value is assigned a variable for use by the probe; each is also shown in the Status window.

To see how this probe works, configure your equipment to send traps to Intermapper or use the `net-snmp snmptrap` command. Either way, the Status window shows the values present in any traps that arrive.

For more information on the `snmptrap` command, see the `net-snmp` documentation for the [trap tutorial](#) and the [snmptrap command](#).

Sending a Trap With Variables From the Dartware MIB

SNMPv1 Traps

1. Add a device to a map with the IP address `192.168.56.78`.
2. Set it to use this probe.
3. Issue the following `snmptrap` command below the command line (it should all be on one line):

```
snmptrap -v 1 -c commString localhost
1.3.6.1.4.1.6306 192.168.56.78 6 123 4567890
1.3.6.1.4.1.6306.2.1.1.0 s "05/08 23:26:35"
1.3.6.1.4.1.6306.2.1.2.0 s Critical
1.3.6.1.4.1.6306.2.1.3.0 s "Big Router"
1.3.6.1.4.1.6306.2.1.4.0 s "Critical: High Traffic"
1.3.6.1.4.1.6306.2.1.5.0 s "127.0.0.1"
1.3.6.1.4.1.6306.2.1.6.0 s "SNMP Traffic Probe"
```

SNMPv2c Traps

1. Add a device to the map with an IP address of **localhost**.
2. Set it to use this probe.
3. Issue the following `snmptrap` command from the command line (it should all be on one line):

```
snmptrap -v 2c -c commString localhost
4567890 1.3.6.1.4.1.6306
1.3.6.1.4.1.6306.192.168.56.78 6 123 4567890
1.3.6.1.4.1.6306.2.1.1.0 s "05/08 13:26:35"
1.3.6.1.4.1.6306.2.1.2.0 s Critical
1.3.6.1.4.1.6306.2.1.3.0 s "Big Router"
1.3.6.1.4.1.6306.2.1.4.0 s "Critical: High
Traffic"
1.3.6.1.4.1.6306.2.1.5.0 s "127.0.0.1"
1.3.6.1.4.1.6306.2.1.6.0 s "SNMP Traffic Probe"
```

NOTE: This probe file contains the above lines in a single-line format suitable for copying and pasting. The parameters in this probe are unused, but can be used to set thresholds for various alarms.

Parameters

MinValue - Unused

MaxValue - Unused

Filename: `com.dartware.snmp.trapdisplay.txt`
Version: 2.4

Network Devices

Apple > Apple AirPort (Extreme)

This probe monitors the custom MIB in an Apple AirPort Extreme Base Station. This probe monitors the number of clients using the base station and lists each with its signal strength.

The first version of AirPort Extreme was round; subsequent versions are square. The following are important differences between them:

- The original round version does not return complete information to clients using the public community string. To retrieve complete information from the original round version, set the community string to the AirPort Extreme's password.
- Subsequent versions have a settable SNMP community string. To use this probe on these versions, you must supply the SNMP community string as set in the AirPort Extreme.

Parameters

None.

Filename: `com.dartware.snmp.airport.ext`
Version: `1.6`

Apple > Apple AirPort (Graphite)

This probe monitors the custom MIB in an Apple AirPort Base Station (v1 = Graphite) using SNMPv1 and monitors the number of clients using the base station and lists each one with its signal strength.

Parameter

Read/Write Community - use the AirPort Base Stations's password.

An SNMP set-request is sent, instructing the AirPort Base Station to discover its clients periodically and test the signal strength of each.

Filename: `com.dartware.snmp.airport`
Version: `1.8`

Cisco > Cisco IP SLA Jitter

This probe extracts jitter test data from a Cisco IP SLA agent that is running on a Cisco router or switch. Typically these jitter tests are used to measure jitter, latency, and packet loss for VoIP and video conferencing applications.

Parameters

SNMP Index - the value used when configuring the IP SLA agent in the Cisco switch or router using the `ip sla monitor` command. This value identifies the jitter test and is the SNMP index used by Intermapper to probe the device. To probe for different instances of jitter tests on a single Cisco

switch or router, create separate devices on your Intermapper map, each using a different SNMP Index.

Latency Alarm Threshold - the ALARM threshold for latency in milliseconds. If Average Latency exceeds this threshold, the device enters the ALARM state.

Latency Warning Threshold - the WARNING threshold for latency in milliseconds. If Average Latency exceeds this threshold, the device enters the WARNING state.

Jitter Alarm Threshold - the ALARM threshold for Jitter. If Average Jitter exceeds this threshold, the device enters the ALARM state.

Jitter Warning Threshold - the WARNING threshold for Jitter. If Average Jitter exceeds this threshold, the device enters the WARNING state.

Packet Loss Alarm Threshold - the ALARM threshold for Packet Loss. If Percent Packet Loss exceeds this threshold, the device enters the ALARM state.

Example

The following is an example of IOS commands used for configuring an IP SLA jitter test to run on a Cisco router or switch:

```
ip sla monitor 250
  type jitter dest-ipaddr w.w.w.w dest-port 50505
  source-ipaddr x.x.x.x num-packets 2000 interval 20
  request-data-size 256
  owner yyyy
  tag zzzz
exit
```

The above example specifies 250 as the SNMP index. This can be any value as long as it is unique. `w.w.w.w` is the IP address of the remote IP SLA responder. `x.x.x.x` is the local IP address of this IP SLA agent. `yyyy` is any text information identifying the owner of the test (for example, the name of network service provider). `zzzz` is any text information identifying this particular test.

To schedule the IP SLA test to run forever:

Run the following command:

```
ip sla monitor schedule 66 life forever start-time now
```

To start the IP SLA responder on the remote IP SLA responder:

Run the following command:

```
ip sla monitor responder
```

In the above IOS commands, the jitter test does not specify a codec type, so ICPIF and MOS scores are not available. If the test is modified to include a codec type then minor revisions are required to this SNMP probe. Also, some routers and switches might not support MIB variables for ICPIF and MOS scores (depending on the IOS train).

For more information on configuring Cisco IP SLA, see www.cisco.com.

Filename: `com.dartware.snmp.cisco-ip-sla.txt`
Version: 2.4

Cisco > Cisco N5000 with FEX Traffic

This probe provides Basic SNMP Traffic probe functionality for the Nexus 5000 with Fiber Extender (FEX). The standard SNMP Traffic probe does not show the Fiber Extender's interfaces, so this probe incorporates special logic to retrieve that information.

This probe requires Intermapper Server version 5.6.6 or higher, which uses the special logic described above; otherwise, the speeds displayed for high speed interfaces are not shown correctly.

Parameters

None

Filename: `com.dartware.snmp.cisco.n5kfex.traffic.txt`
Version: 1.1

Cisco > Cisco Old CPU MIB

This probe monitors the CPU and Memory utilization of a Cisco router.

Parameters

CPU Busy - Alarm - the ALARM threshold for CPU utilization (in percentage). If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters the ALARM state.

CPU Busy - Warning - the WARNING threshold for CPU utilization (in percentage). If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters the WARNING state.

Low Memory - Alarm - the ALARM threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters the ALARM state.

Low Memory - Warning - the WARNING threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters the WARNING state.

Filename: `com.dartware.snmp.cisco`
Version: 1.9

Cisco > Cisco Process and Memory Pool

This probe monitors the CPU and Memory utilization in a Cisco router. It uses variables from CISCO-MEMORY-POOL-MIB and CISCO-PROCESS-MIB.

Parameters

CPU Busy - Alarm - The ALARM threshold for CPU utilization (in percentage). If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters the ALARM state.

CPU Busy - Warning - The WARNING threshold for CPU utilization (in percentage). If the average CPU usage over a 1 minute interval exceeds this threshold, the device enters the WARNING state.

Low Memory - Alarm - The ALARM threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters the ALARM state.

Low Memory - Warning - The WARNING threshold for the amount of free memory remaining (in bytes). If free memory drops below this threshold, the device enters the WARNING state.

Filename: `com.dartware.snmp.cisconewmib`
Version: 1.9

Cisco > Cisco Aironet

This probe uses SNMPv1 to monitor the custom MIB in a Cisco Aironet Wireless Access Point. It monitors the number of clients using the base station and lists each client with its signal strength.

The alarm and warning thresholds must be greater than 0, otherwise they are ignored.

Parameters

Number of Active Stations alarm - sets the threshold when the device goes into the ALARM state.

Number of Active Stations warning - sets the threshold when the device goes into the WARNING state.

Filename: `com.dartware.snmp.aironet`

Version: `1.6`

Cisco > Cisco ASA Firewall

This probe monitors a Cisco ASA firewall or security context (CPU utilization, memory utilization, active connections, connections per second, primary unit status, and secondary unit status).

This probe generates an ALARM if one of the following occurs:

- **CPU % busy** - averaged over 1 minute exceeds a threshold
- **Active connections** - exceeds a threshold
- **Connections per second** - averaged over 1 minute exceeds a threshold
- **Primary unit status** - abnormal
- **Secondary unit status** - abnormal

Parameters

CPU Utilization Threshold - the percentage of CPU usage required to generate an ALARM.

Active Connections Alarm Threshold - the maximum number of active connections required to generate an ALARM.

Connections Per Second Alarm Threshold - the maximum number of connections per second required to generate an ALARM.

Filename: `com.helpsystems.snmp.cisco.asa.firewall`
Version: 1.0

Cisco > Cisco ASR 1000

This probe monitors a Cisco ASR 1000 Series Aggregation Services Router. This probe has only been tested with a Cisco ASR 1009-X running Cisco IOS XE software. It should work with other chassis-based Cisco ASR 1000 models. If you encounter issues using this probe with other models, contact Fortra to request an enhancement.

The probe generates a Warning or Alarm alert if one of the following occurs:

- % CPU Busy of the RP Routing Processor exceeds a threshold
- % Memory Utilization of the RP Routing Processor exceeds a threshold
- % CPU Busy of any module over a 5 minute interval exceeds a threshold
- % Memory Utilization of any module exceeds a threshold
- The state of a module is abnormal
- A fan malfunctions or fails
- A power supply malfunctions or fails
- The hard disk state is not ok

Warning and alarm alerts can be turned on or off by adjusting the probe parameters. They are on by default.

NOTE:

- The Routing Processor (RP) contains two physical CPUs, but the CPUs are not monitored separately. CPU utilization is the aggregate result of both the CPUs and therefore the cpmCPUTotalTable object contains only one entry for RP CPU. This can occasionally cause the management stations to report CPU utilization above 100%.

For more information, see

<https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/118901-technote-snmp-00.html>.

- When you restart the Intermapper server or add a new Cisco ASR to a map, it can take several poll cycles for the probe to collect and display information about the switch in the Device Status window.
- You can report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **RP CPU Busy - Warning Threshold** - the RP Routing Processor % CPU Busy threshold required to place the device in Warning status.
- **RP CPU Busy - Alarm Threshold** - the RP Routing Processor % CPU Busy threshold required to place the device in Alarm status.
- **RP Memory Utilization - Warning Threshold** - the RP Routing Processor % Memory Utilization threshold required to place the device in Warning status.
- **RP Memory Utilization - Alarm Threshold** - the RP Routing Processor % Memory Utilization threshold required to place the device in Alarm status.
- **Module CPU Busy - Warning Threshold** - the Module % CPU Busy threshold required to place the device in Warning status.
- **Module CPU Busy - Alarm Threshold** - the Module % CPU Busy threshold required to place the device in Alarm status.
- **Module Memory Utilization - Warning Threshold** - the Module % Memory Utilization threshold required to place the device in Warning status.
- **Module Memory Utilization - Alarm Threshold** - the Module % Memory Utilization threshold required to place the device in Alarm status.

- **RP CPU Warnings** - Set to Off to suppress Warning alerts for RP Routing Processor % CPU Busy above the specified threshold. Default is On.
- **RP CPU Alarms** - Set to Off to suppress Alarm alerts for RP Routing Processor % CPU Busy above the specified threshold. Default is On.
- **RP Memory Warnings** - Set to Off to suppress Warning alerts for RP Routing Processor % Memory Utilization above the specified threshold. Default is On.
- **RP Memory Alarms** - Set to Off to suppress Alarm alerts for RP Routing Processor % Memory Utilization above the specified threshold. Default is On.
- **Module CPU Warnings** - Set to Off to suppress Warning alerts for Module % CPU Busy above the specified threshold. Default is On.
- **Module CPU Alarms** - Set to Off to suppress Alarm alerts for Module % CPU Busy above the specified threshold. Defaults to On.
- **Module Memory Warnings** - Set to Off to suppress Warning alerts for Module % Memory Utilization above the specified threshold. Default is On.
- **Module Memory Alarms** - Set to Off to suppress Alarm alerts for Module % Memory Utilization above the specified threshold. Default is On.
- **State Warnings** - Set to Off to suppress Warning alerts for abnormal module states. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal module states. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.

Filename: com.helpsystems.snmp.ciscoASR1000.txt
Version: 1.0

Cisco > Cisco Catalyst 3850

This probe monitors the following Cisco Catalyst switches:

- Single Cisco Catalyst 3850 switch
- Stack of Cisco Catalyst 3850 switches

This probe generates a Critical alert if the data stack ring fails (becomes non redundant). By default, Critical alerts are enabled, but can be disabled by adjusting the probe parameters.

The probe generates a Warning or Alarm alert if the following occurs:

- The Active Switch % CPU Busy over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a switch is abnormal.
- The state of a switch is abnormal.
- The outlet temperature of a switch exceeds normal operational limits.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.
- The data stack ring fails (becomes non redundant).
- The Active Switch is not the highest priority switch.

By default, Warning and Alarm alerts are enabled. They can be disabled by adjusting the probe parameters.

NOTE:

- When you restart the Intermapper server or add a new Catalyst switch to a map it can take several poll cycles for the probe to collect and display information about the switch or switch stack in the Device Status window. The more switches in a stack, the longer it takes to display information.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up to date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in the Warning status.

- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in the Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in the Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in the Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal switch states. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.
- **Stack Alarms** - Set to Off to suppress Alarms when the data stack ring fails (becomes non redundant). Default is On.
- **Stack Critical Alerts** - Set to Off to suppress Critical alerts when the data stack ring fails (becomes non redundant). Default is On.
- **Active Switch Warnings** - Set to Off to suppress Warning alerts when the Active Switch is not the highest priority switch. Default is On.

Filename: `com.helpsystems.snmp.catalyst3850`

Version: 1.0

Cisco > Cisco Catalyst 4500 X

This probe monitors a Cisco Catalyst 4500-X Series switch. It does not monitor a pair of Catalyst 4500-X switches stacked together into a Virtual Switching System (VSS).

This probe has been tested with IOS releases 03.04.00.SG, 03.06.04.E, 03.06.05.E, and 03.08.06.E.

The probe generates a Warning or Alarm alert if the following occurs:

- The % CPU Busy over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The outlet temperature of the base unit, the expansion module, or the CPU exceed normal operational limits.
- A switch fan or a power supply fan malfunctions or fails.
- A power supply malfunctions or fails.

By default, Warning and Alarm alerts are enabled. They can be disabled by adjusting the probe parameters.

NOTE:

- When you restart the Intermapper server or add a new Catalyst 4500-X switch to a map it can take several poll cycles for the probe to collect and display information about the switch in the Device Status window.
- Please report bugs and enhancement requests to Help Systems so that this probe can be enhanced and kept up to date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in the Warning status.
- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in the Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in the Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in the Alarm status.

- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.

Filename: `com.helpsystems.snmp.catalyst4500x`
Version: 1.0

Cisco > Cisco Catalyst 6500 6800 VSS

This probe monitors two Cisco Catalyst 6500 switches or two Catalyst 6800 switches paired together into a Virtual Switching System (VSS).

This probe has been tested with a pair of Catalyst 6500 switches running 15.5(1)SY and with a pair of Catalyst 6800 switches running 15.2(1)SY. It should work with other software releases. If you encounter issues using this probe with other software releases, contact Fortra to request probe enhancements.

This probe does not monitor two Catalyst 4500-X switches paired together into a Virtual Switching System (VSS).

The probe generates a Critical alert if the following occurs:

- The VSS Mode is Standalone (rather than Multinode).
- The Operational State of the Virtual Switch Link is Down.

Critical alerts can be turned on or off by adjusting the probe parameters. They are enabled by default.

The probe generates a Warning or Alarm alert if the following occurs:

- The % CPU Busy of the Routing Processor over a 5 minute interval exceeds a threshold.
- The % Memory Utilization of the Routing Processor exceeds a threshold.
- The % CPU Busy of any Module over a 5 minute interval exceeds a threshold.
- The State of a Module is abnormal.
- The Outlet Temperature of a Module exceeds normal operational limits.
- A Fan malfunctions or fails.
- A Power Supply malfunctions or fails.
- The VSS Mode is Standalone (rather than Multinode).
- The Operational State of the Virtual Switch Link is Down.

Warning and alarm alerts can be turned on or off by adjusting the probe parameters. They are on by default.

NOTE:

- Because Catalyst 6500 and Catalyst 6800 devices often have thousands of interfaces, this probe does not poll interfaces with SNMP. As a result, if you open the Interfaces window for a device, no interfaces are displayed. If you require interfaces to be polled and displayed, use the SNMP Traffic probe in addition to this probe.
- When you restart the Intermapper server or add a new VSS device to a map it can take several poll cycles for the probe to collect and display information in the Device Status window. The more modules there are in the switches, the longer it takes to display the information.
- Enabling Netflow on a module can cause the Module % CPU Utilization to spike.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **RP CPU Busy - Warning Threshold** - the Routing Processor % CPU Busy threshold required to place the device in Warning status.
- **RP CPU Busy - Alarm Threshold** - the Routing Processor % CPU Busy threshold required to place the device in Alarm status.
- **RP Memory Utilization - Warning Threshold** - the Routing Processor % Memory Utilization threshold required to place the device in Warning status.
- **RP Memory Utilization - Alarm Threshold** - the Routing Processor % Memory Utilization threshold required to place the device in Alarm status.
- **Module CPU Busy - Warning Threshold** - the Module % CPU Busy threshold required to place the device in Warning status.
- **Module CPU Busy - Alarm Threshold** - the Module % CPU Busy threshold required to place the device in Alarm status.
- **RP CPU Warnings** - Set to Off to suppress Warning alerts for Routing Processor % CPU Busy above the specified threshold. Defaults to On.
- **RP CPU Alarms** - Set to Off to suppress Alarm alerts for Routing Processor % CPU Busy above the specified threshold. Defaults to On.

- **RP Memory Warnings** - Set to Off to suppress Warning alerts for Routing Processor % Memory Utilization above the specified threshold. Defaults to On.
- **RP Memory Alarms** - Set to Off to suppress Alarm alerts for Routing Processor % Memory Utilization above the specified threshold. Defaults to On.
- **Module CPU Warnings** - Set to Off to suppress Warning alerts for Module % CPU Busy above the specified threshold. Defaults to On.
- **Module CPU Alarms** - Set to Off to suppress Alarm alerts for Routing Processor % CPU Busy above the specified threshold. Default is On.
- **State Warnings** - Set to Off to suppress Warning alerts for abnormal module states. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal module states. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Critical Alerts** - Set to Off to suppress Critical alerts. Default is On.

Filename:

`com.helpsystems.snmp.cisco.catalyst.6500.6800.VSS.txt`

Version: 1.0

Cisco > Cisco Catalyst 6500

This probe monitors a Cisco Catalyst 6500 or Catalyst 6509-E switch.

This probe does not monitor a pair of Catalyst 6500 switches stacked together into a Virtual Switching System (VSS).

It has been tested with Catalyst 6504-E, 6506, 6509, and 6509-E models running IOS releases 12.2(18)SXD3, 12.2(33)SXI4, 12.2(33)SXJ9, and 15.1(2)SY7.

The probe generates a Critical alert if the state of a module is MajorFault.

By default, Critical alerts are enabled. They can be disabled by adjusting the probe parameters.

The probe generates a Warning or Alarm alert if the following occurs:

- The average % CPU Busy of any CPU over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a module is abnormal.
- The outlet temperature of a module exceeds normal operational limits.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.

By default, Warning and Alarm alerts are enabled. They can be disabled by adjusting the probe parameters.

NOTE:

- Because Catalyst 6500 devices often have thousands of interfaces, this probe does not poll interfaces with SNMP. As a result, if you open the Interfaces window for a device, no interfaces are displayed and the CDP_Neighbors button does not display the Local Interface Names. You can use a text editor to remove the 'NOLINKS' option from the header section of this probe or use the basic SNMP Traffic probe.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in Warning status.
- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Defaults to On.

- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Defaults to On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Defaults to On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Defaults to On.
- **State Warnings** - Set to Off to suppress Warning alerts for abnormal switch states. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal switch states. Default is On.
- **State Critical Alerts** - Set to Off to suppress Critical alerts when a module has a major fault. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On..
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.

Filename: `com.helpsystems.snmp.catalyst6500.txt`
 Version: 1.0

Cisco > Cisco Catalyst 6800

This probe monitors a Cisco Catalyst 6800 switch. It does not monitor a pair of Catalyst 6800 switches stacked together into a Virtual Switching System (VSS).

It has been tested with Catalyst C6807-XL model running IOS release 15.5 (1)SY1. It should work with other Catalyst 6800 models. If you encounters issues using this probe with other models, contact Fortra so that this probe can be enhanced and kept up-to-date.

NOTE: This probe is identical to the Cisco Catalyst 6500 probe, but with a different probe name for clarity in probe picker window.

The probe generates a Critical alert if the state of a module is MajorFault.

By default, Critical alerts are enabled. They can be disabled by adjusting the probe parameters.

The probe generates a Warning or Alarm alert if the following occurs:

- The average % CPU Busy of any CPU over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a module is abnormal.
- The outlet temperature of a module exceeds normal operational limits.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.

By default, Warning and Alarm alerts are enabled. They can be disabled by adjusting the probe parameters.

NOTE:

- Because Catalyst 6800 devices often have thousands of interfaces, this probe does not poll interfaces with SNMP. As a result, if you open the Interfaces window for a device no interfaces are displayed and the CDP_Neighbors button do not display the Local Interface Names. If you require interfaces to be polled and displayed, you can use a text editor to remove the NOLINKS option from the header section of this probe, or use the basic SNMP Traffic probe.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in Warning status.
- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in Alarm status.

- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **State Warnings** - Set to Off to suppress Warning alerts for abnormal switch states. Default is On..
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal switch states. Default is On.
- **State Critical Alerts** - Set to Off to suppress Critical alerts when a module has a major fault. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.

Filename: `com.helpsystems.snmp.catalyst6800.txt`
Version: 1.0

Cisco > Cisco Catalyst 9300

This probe monitors the following Cisco Catalyst switches:

- Single Cisco Catalyst 9300 switch
- Entire stack of Cisco Catalyst 9300 switches

NOTE:

This probe is identical to the Cisco Catalyst 3850 probe, but with a different probe name for clarity in probe picker window.

The probe generates a Critical alert if the data stack ring fails (becomes non redundant).

By default, Critical alerts are enabled. They can be disabled by adjusting the probe parameters.

The probe generates a Warning or Alarm alert if the following occurs:

- The Active Switch % CPU Busy over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a switch is abnormal.
- The outlet temperature of a switch exceeds normal operational limits.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.
- The data stack ring fails (becomes non redundant).
- The Active Switch is not the highest priority switch.

By default, Warning and Alarm alerts are on. They can be turned on or off by adjusting the probe parameters.

NOTE:

- When you restart the Intermapper server or add a new Catalyst switch to a map, it can take several poll cycles for the probe to collect and display information about the switch or switch stack in the Device Status window. The more switches in a stack, the longer it takes to display the information.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in Warning status.
- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal switch states. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.
- **Stack Alarms** - Set to Off to suppress Alarms when the data stack ring fails (becomes non redundant). Default is On.
- **Stack Critical Alerts** - Set to Off to suppress Critical alerts when the data stack ring fails (becomes non redundant). Default is On.
- **Active Switch Warnings** - Set to Off to suppress Warning alerts when the Active Switch is not the highest priority switch. Default is On.

Filename: `com.helpsystems.snmp.catalyst9300`

Version: 1.0

Cisco > Cisco Catalyst 9500 Non StackWise

This probe monitors a single physical Catalyst 9500 switch that does not support the Cisco StackWise MIB.

The probe generates a Warning or Alarm alert if the following occurs:

- The Active Switch % CPU Busy over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The outlet temperature of the switch exceeds normal operational limits.
- A power supply malfunctions or fails.
- A fan malfunctions or fails.

Warning and alarm alerts are enabled by default. They can be disabled by adjusting the probe parameters.

NOTE:

- Some Catalyst 9500 switch models support the Cisco StackWise MIB and some don't. Models that support StackWise vary depending on the version of IOS XE that is running. For IOS XE 16.6.X StackWise is supported only on the C9500-24Q model. For IOS XE 16.9.X StackWise is supported only on the C9500-24Q, C9500-12Q, C9500-40X, C9500-16X models. Use the Cisco Catalyst 9500 StackWise probe to monitor models that support StackWise, and the Cisco Catalyst 9500 Non-StackWise probe to monitor models that don't support StackWise.
- When you restart the Intermapper server or add a new Catalyst switch to a map it can take several poll cycles for the probe to collect and display information about the switch in the Device Status window.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up to date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in Warning status.
- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.

Filename:

`com.helpsystems.snmp.catalyst9500.nonstackwise.txt`

Version: 1.0

Cisco > Cisco Catalyst 9500 StackWise

This probe monitors Catalyst 9500 switches that support the Cisco StackWise MIB. The probe can monitor a single physical Catalyst 9500 switch or a pair of two physical Catalyst 9500 switches clustered together into a StackWise Virtual switch.

The probe generates a Warning or Alarm alert if the following occurs:

- The Active Switch % CPU Busy over a 5 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a switch is abnormal.
- The outlet temperature of a switch exceeds normal operational limits.
- A power supply malfunctions or fails.
- A fan malfunctions or fails.

Warning and alarm alerts are enabled by default. They can be disabled by adjusting the probe parameters.

NOTE:

- Some Catalyst 9500 switch models support the Cisco StackWise MIB and some don't. Models that support StackWise vary depending on the version of IOS XE that is running. For IOS XE 16.6.X StackWise is supported only on the C9500-24Q model. For IOS XE 16.9.X StackWise is supported only on the C9500-24Q, C9500-12Q, C9500-40X, C9500-16X models. Use the **Cisco Catalyst 9500 StackWise** probe to monitor models that support StackWise, and the **Cisco Catalyst 9500 Non-StackWise** probe to monitor models that don't support StackWise.
- When you restart the Intermapper server or add a new Catalyst switch to a map it can take several poll cycles for the probe to collect and display information about the switch in the Device Status window.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- **CPU Busy - Warning Threshold** - the % CPU Busy threshold required to place the device in Warning status.

- **CPU Busy - Alarm Threshold** - the % CPU Busy threshold required to place the device in Alarm status.
- **Memory Utilization - Warning Threshold** - the % Memory Utilization threshold required to place the device in Warning status.
- **Memory Utilization - Alarm Threshold** - the % Memory Utilization threshold required to place the device in Alarm status.
- **CPU Warnings** - Set to Off to suppress Warning alerts for % CPU Busy above the specified threshold. Default is On.
- **CPU Alarms** - Set to Off to suppress Alarm alerts for % CPU Busy above the specified threshold. Default is On.
- **Memory Warnings** - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- **Memory Alarms** - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal switch states. Default is On.
- **Temperature Warnings** - Set to Off to suppress Warning alerts for temperature issues. Default is On.
- **Temperature Alarms** - Set to Off to suppress Alarm alerts for temperature issues. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.

Filename: `com.helpsystems.snmp.catalyst9500.stackwise.txt`
Version: 1.0

Cisco > Cisco Catalyst Switch

This probe monitors the following Cisco Catalyst switches:

- Fixed configuration Cisco Catalyst switch
- Entire stack of Cisco Catalyst switches

It has been tested with Catalyst 2960, Catalyst 3560, Catalyst 3750, Catalyst 3750X, Catalyst 3850, and Catalyst 9300 switches.

New probes are available for Catalyst 3850 and Catalyst 9300 switches. These new probes report the role and priority of each switch in the stack and can monitor the CPU utilization for each switch in the stack.

The probe generates a Critical alert if the stack ring is not redundant

By default, Critical alerts are enabled. They can be disabled by adjusting the probe parameters.

The probe generates a Warning or Alarm alert if the following occurs:

- The % CPU Busy over a 1 minute interval exceeds a threshold.
- The % Memory Utilization exceeds a threshold.
- The state of a switch is abnormal.
- The outlet exhaust temperature of a switch exceeds normal operational limits.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.
- The stack ring is not redundant.

By default, Warning and Alarm alerts are on. They can be turned on or off by adjusting the probe parameters.

NOTE:

- When you restart the Intermapper server or add a new Catalyst switch to a map, it takes several poll cycles for the probe to collect and display information about the switch or switch stack in the Device Status window. The more switches in a stack, the longer it takes to display the information. Newer switches like the Catalyst 3850 with fast SNMP processing display information twice as fast as older switches.
- Catalyst 3750X IOS Release 12.2(55) has a bug where SNMP does not return information for Fan 2 for the second and subsequent switches in the stack. This affects the #Fan column in the Device Status window. The #Fan column indicates only one fan is installed, when there might actually be two. To remedy this, upgrade to IOS Release 12.2(58) or later.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up-to-date.

Parameters

- *CPU Busy - Warning Threshold* - the threshold in CPU usage (percent) required to place the device in Warning status.
- *CPU Busy - Alarm Threshold* - the threshold in CPU usage (percent) required to place the device in Alarm status.
- *Memory Utilization - Warning Threshold* - the % Memory Utilization threshold required to place the device in Warning status.
- *Memory Utilization - Alarm Threshold* - the % Memory Utilization threshold required to place the device in Alarm status.
- *CPU Warnings* - Set to Off to suppress Warning status notifications for CPU usage above the specified threshold. Default is On.
- *CPU Alarms* - Set to Off to suppress Alarm status notifications for CPU usage above the specified threshold. Default is On.
- *Memory Warnings* - Set to Off to suppress Warning alerts for % Memory Utilization above the specified threshold. Default is On.
- *Memory Alarms* - Set to Off to suppress Alarm alerts for % Memory Utilization above the specified threshold. Default is On.
- *State Alarms* - Set to Off to suppress Alarm status notifications for abnormal switch states. Default is On..
- *PS Warnings* - Set to Off to suppress Warnings for power supply issues. Default is On.

- *PS Alarms* - Set to Off to suppress Alarms for power supply issues. Default is On.
- *Fan Warnings* - Set to Off to suppress Warnings for fan issues. Default is On.
- *Fan Alarms* - Set to Off to suppress Alarms for fan issues. Default is On.
- *Temperature Warnings* - Set to Off to suppress Warnings for temperature issues. Default is On.
- *Temperature Alarms* - Set to Off to suppress Alarms for temperature issues. Default is On.
- *Stack Alarms* - Set to Off to suppress Alarms when the stack ring is not redundant. Default is On.
- *Stack Critical Alerts* - Set to Off to suppress Critical alerts when the stack ring is not redundant. Default is On.

Filename: `com.helpsystems.snmp.catalystswitch`
Version: 1.1

Cisco > Cisco Firepower Threat Defence ASA

This probe monitors a Cisco Firepower Threat Defence ASA (CPU utilization, system memory utilization, active connections, and connection setups).

The probe generates an ALARM if the following occurs:

- % CPU Busy (5 min) exceeds a threshold.
- % System Memory Used exceeds a threshold.
- % Active Connections Used exceeds a threshold.
- Connections/Sec (5 min) exceeds a threshold.
- Connections Denied (1 min) exceeds a threshold.

Set a threshold to 0 to suppress the alarm for that threshold.

Parameters

CPU Utilization Alarm Threshold - the percentage of CPU required to generate an ALARM.

System Memory Used Alarm Threshold - the percentage of system memory required to generate an ALARM.

Active Connections Alarm Threshold - the maximum number of active connections required to generate an ALARM.

Connections Per Second Alarm Threshold - the maximum number of connections per second required to generate an ALARM.

Denied Connections Per Minute Alarm Threshold - the maximum number of denied connections per minute required to generate an ALARM.

NOTE:

- You cannot poll consolidated data for Firepower Threat Defense clusters. Each individual Firepower Threat Defense device is polled separately using its Local IP address and is displayed on the Intermapper map. For example, if your cluster has two Firepower Threat Defense devices, two devices are displayed on the Intermapper map.
- This probe monitors only the ASA part of the Firepower Threat Defence Device. The IPS (snort) and DDOS (radware) parts cannot be monitored.

Filename:

`com.helpsystems.snmp.cisco.firepowerthreatdefence.asa`

Version: 1.0

Cisco > Cisco Nexus

This probe monitors a Cisco Nexus Series Switch.

This probe has been tested only with a Cisco N5K-C5548U running NX-OS 7.3 software, a Cisco N7K-7009 running NX-OS 6.2 software, and a Cisco N9K-C9372PX-E running NX-OS 7.0 software. It might not work with other Nexus models. If you encounter issues using this probe with other models, contact Fortra so that this probe can be enhanced and kept up-to-date.

The probe generates a Warning or Alarm alert if the following occurs:

- The % CPU Busy of the Active Supervisor exceeds a threshold.
- The % Memory Utilization of the Active Supervisor exceeds a threshold.

- The % CPU Busy of a module exceeds a threshold.
- The % Memory Utilization of a module exceeds a threshold.
- The state of a module is abnormal.
- A fan malfunctions or fails.
- A power supply malfunctions or fails.

Warning and alarm alerts are enabled by default. They can be disabled by adjusting the probe parameters.

NOTE:

- When you restart the Intermapper server or add a new Nexus device to a map it will take several poll cycles for the probe to collect and display information in the Device Status window. The more modules there are in the switch the longer it will take to display the information.
- Having Netflow enabled on a module can cause the Module % CPU Utilization to spike.
- Report bugs and enhancement requests to Fortra so that this probe can be enhanced and kept up to date.

Parameters

- **Supervisor CPU Busy - Warning Threshold** - the Supervisor % CPU Busy threshold required to place the device in Warning status.
- **Supervisor CPU Busy - Alarm Threshold** - the Supervisor % CPU Busy threshold required to place the device in Alarm status.
- **Supervisor Memory Utilization - Warning Threshold** - the Supervisor % Memory Utilization threshold required to place the device in Warning status.
- **Supervisor Memory Utilization - Alarm Threshold** - the Supervisor % Memory Utilization threshold required to place the device in Alarm status.
- **Module CPU Busy - Warning Threshold** - the Module % CPU Busy threshold required to place the device in Warning status.
- **Module CPU Busy - Alarm Threshold** - the Module % CPU Busy threshold required to place the device in Alarm status.
- **Module Memory Utilization - Warning Threshold** - the Module % Memory Utilization threshold required to place the device in Warning status.

- **Module Memory Utilization - Alarm Threshold** - the Module % Memory Utilization threshold required to place the device in Alarm status.
- **Supervisor CPU Warnings** - Set to Off to suppress Warning alerts for Supervisor % CPU Busy above the specified threshold. Default is On.
- **Supervisor CPU Alarms** - Set to Off to suppress Alarm alerts for % Supervisor CPU Busy above the specified threshold. Default is On.
- **Supervisor Memory Warnings** - Set to Off to suppress Warning alerts for Supervisor % Memory Utilization above the specified threshold. Default is On.
- **Supervisor Memory Alarms** - Set to Off to suppress Alarm alerts for Supervisor % Memory Utilization above the specified threshold. Default is On.
- **Module CPU Warnings** - Set to Off to suppress Warning alerts for Module % CPU Busy above the specified threshold. Default is On.
- **Module CPU Alarms** - Set to Off to suppress Alarm alerts for Module % CPU Busy above the specified threshold. Default is On.
- **Module Memory Warnings** - Set to Off to suppress Warning alerts for Module % Memory Utilization above the specified threshold. Default is On.
- **Module Memory Alarms** - Set to Off to suppress Alarm alerts for Module % Memory Utilization above the specified threshold. Default is On.
- **State Warnings** - Set to Off to suppress Warning alerts for abnormal module states. Default is On.
- **State Alarms** - Set to Off to suppress Alarm alerts for abnormal module states. Default is On.
- **PS Warnings** - Set to Off to suppress Warning alerts for power supply issues. Default is On.
- **PS Alarms** - Set to Off to suppress Alarm alerts for power supply issues. Default is On.
- **Fan Warnings** - Set to Off to suppress Warning alerts for fan issues. Default is On.
- **Fan Alarms** - Set to Off to suppress Alarm alerts for fan issues. Default is On.

Filename: `com.helpsystems.snmp.ciscoNexus.txt`

Version: 1.0

Cisco > Cisco WLC

This probe monitors a Cisco WLC (Wireless LAN Controller).

This probe generates an ALARM if the following occurs:

- Memory Utilization exceeds a threshold.
- CPU Utilization exceeds a threshold.
- Internal Temperature exceeds a threshold.
- Power Supply Status is FAIL.
- Connected Clients exceeds a threshold.

Parameters

Memory Threshold - enter a memory usage value (in Mb) required to generate an ALARM. Enter 0 to suppress Memory Utilization alarms.

CPU Utilization Threshold - enter a percentage of CPU usage required to generate an ALARM. Enter 0 to suppress CPU Utilization alarms.

Internal Temperature Threshold - enter an internal temperature (in Celsius) required to generate an ALARM. Enter 0 to suppress Internal Temperature alarms.

Connected Clients Threshold - enter a maximum number of connected clients required to generate an ALARM. Enter 0 to suppress Connected Clients alarms.

NOTE:

- This probe has been tested with several models of Cisco WLC including the 3504, 5508, and 8540 models. It should work with other models but has not been tested. Monitoring of power supplies and SSO Sync Status is release dependent.
- This probe monitors a Cisco WLC for up to 16 WLAN SSIDs. If you need to monitor more than 16 WLAN SSIDS you will need to modify the probe.

Filename: `com.helpsystems.snmp.cisco.wlc`

Version: 1.1

Juniper > Netscreen VPN

This probe monitors the status of VPN Tunnels in a Netscreen Firewall. It uses the `nsVpnMonTable` to monitor the Netscreen's active tunnels. Each active tunnel is treated and mapped as a separate interface.

Some statistics might be available only if the monitoring status for the tunnel as reported by `nsVpnMonMonState` is on.

Parameters

None

Filename: `com.dartware.snmp.netscreen.txt`

Version: 1.2

Karlnet Wireless

This probe monitors the custom MIB in a Karlnet Wireless Base Station using SNMPv1. It monitors the number of clients using the base station and lists each, along with its signal strength.

This probe sends SNMP set-requests to the Karlnet Base Station, causing it to discover and test the signal strength of each client. For the set-requests to work, enter the read/write community string for the base station.

Parameter

Read/Write Community - SNMP Read/Write community string.

Filename: `com.dartware.snmp.karlnet`

Version: 1.6

UPS > APC UPS AP961x

This probe works best with devices which have implemented the following MIBs:

- **APC UPS MIB** - [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]
- **APC Environmental Monitoring MIB** - [... enterprises.apc.products.hardware.environmentalMonitor / ... 1.3.6.1.4.1.318.1.1.10]

Values

- **UPS** - model, firmware, and status
- **Battery** - capacity, time remaining, temperature, and replacement status
- **Output** - load percent, volts, amps, and frequency
- **Input** - volts, voltage range over last minute, frequency, and last input failure
- **Environmental Monitor** - probe name, number of probes, current temperature, humidity, high threshold configurations, and low threshold configurations

Alarms

- If unit goes onto battery or goes off-line
- If battery needs replacement
- If the UPS internal temperature and humidity threshold is exceeded (must also be enabled)

Warnings

If unit goes onto Smart Trim or Smart Boost

Parameters

None

Filename: `com.dartware.ups.apc-ap961x.txt`

Version: 3.6

UPS > APC UPS

Use this probe with APC UPS devices.

This probe works best with devices which have implemented the following MIB:

- **APC UPS MIB** - [... enterprises.apc.products.hardware.ups / ... 1.3.6.1.4.1.318.1.1.1]

Values

- **UPS** - model, firmware, and status
- **Battery** - capacity, time remaining, temperature, and replacement status
- **Output** - load percent, volts, amps, and frequency
- **Input** - volts, voltage range over last minute, frequency, and last input failure

Alarms

- If unit goes onto battery or goes off-line
- If battery needs replacement
- If the battery temperature exceeds user-specified thresholds (see Parameters below)

Warnings

- If unit goes onto Smart Trim or Smart Boost
- If the battery temperature exceeds user-specified thresholds (see Parameters below)

Parameters

- **Units of Temperature (C / F)** - Determines how the following thresholds are interpreted.
- **Alarm Threshold - Low Temp** - Low threshold for alarm state.
- **Alarm Threshold - High Temp** - Threshold for alarm state.
- **Warning Threshold - Low Temp** - Low threshold for warning state.
- **Warning Threshold - High Temp** - High threshold for warning state.

Filename: `com.dartware.ups.apc.txt`

Version: 3.6

UPS > BestPower UPS

Use this probe with BestPower UPS devices.

This probe works best with devices which have implemented the following MIB:

- BestPower MIB - [... enterprises.bestPower.bestLink / ... 1.2947.1]

Values

vendor, model, firmware version, VA Rating, time on battery, time remaining, (*input & output*: voltage, current, frequency), output power, internal temperature.

Alarms

- **Warning** - If UPS loses AC power.
- **Alarm** - If minutes of battery life remaining is less than specified threshold.

Parameter

- **BatteryRemainingAlarm** - Threshold for alarm state.

Filename: `com.dartware.ups.bestpower.txt`

Version: 2.12

UPS > Exide UPS

Use this probe with Exide UPS devices.

This probe works best with devices which have implemented the following MIB:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]
- Exide XUPS MIB [... enterprises.powerware / ... 1.534]

Values

- **UPS** - vendor, model, software version, firmware version
- **Battery** - output source, battery status, battery voltage, battery current
- **Input** - Hz, volts, amps, kWatts
- **Output** - Hz, volts, amps, kWatts, output load percent

Alarms

If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).

Parameters

None

Filename: `shef.ac.uk.ups.exide.txt`

Version: 2.12

UPS > Liebert UPS EXM

Use this probe with the Liebert EXM Power System line of UPS devices.

This probe works best with devices which have implemented the following MIB:

- Liebert UPS MIB - [... enterprises.emerson.liebertCorp.liebertUps / ... 1.476.1.1]

Values

MIB, vendor, model, and software version

Parameters

None

Filename: `com.dartware.ups.liebert-exm.txt`

Version: 1.2

UPS > Liebert UPS OpenComms

Use this probe with Liebert UPS equipped with an OpenComms Network Management Card.

This probe works best with devices which have implemented the following MIBs:

- **UPS MIB (RFC 1628)** - [... mib-2.upsMIB / ... 1.33]
- **Liebert Global Products MIB** - [... enterprises.emerson.liebertCorp.liebertGlobalProducts / ... 1.476.1.42]

Values

- **UPS** - vendor, model, software version, and firmware version
- **Battery** - output source, battery status, battery voltage, and battery current
- **Input** - Hz, volts, amps, and kWatts

- **Output** - Hz, volts, amps, kWatts, and output load percent
- **Temperature** - battery and ambient

Alarms

If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).

Parameters

None

Filename: `com.dartware.ups.liebert-opencomms.txt`
Version: 2.13

UPS > Liebert UPS Series 300

Use this probe with the Liebert Series 300 line of UPS devices.

This probe works best with devices which have implemented the following MIB:

- LIEBERT-SERIES-300-UPS-MIB\p\ [... enterprises.emerson.liebertCorp.liebertUps.luExtensions.luCore / ... 1.476.1.1.1.1] and [... luExtensions.luUPStationS / ... 1.2]

Values

- **UPS** - vendor, model, software version, and firmware version
- **Battery** - output load (%), battery status, battery voltage, and battery current
- **three input, output, and bypass phases** - voltage and current
- **frequencies** - input, output, and bypass

Alarms

If the device is reporting any alarms. (The MIB includes a comprehensive list of alarms).

Parameters

None

Filename: `com.dartware.ups.liebert-series300.txt`

Version: 2.9

UPS > Liebert UPS

This probe is meant to aid Dartware's development of probes for the Liebert product line.

Check other probes to see if one exists for your Liebert UPS device. If not, select this probe, copy the contents of the status window, and email it to support.Intermapper@fortra.com. Fortra can try to develop a probe for your device.

This probe works best with devices which have implemented the following MIB:

- Liebert UPS MIB - [... enterprises.emerson.liebertCorp.liebertUps / ... 1.476.1.1]

Values

MIB, vendor, model, and software version

Parameters

None

Filename: `com.dartware.ups.liebert-ups.txt`

Version: 2.10

UPS > Standard UPS (RFC1628)

Use this probe with UPS devices.

This probe works best with devices which have implemented the following MIB:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]

Values

- **UPS** - vendor, model, software version, and firmware version
- **Battery** - output source, battery status, battery voltage, and battery current

- **Input** - Hz, volts, amps, and kWatts
- **Output** - Hz, volts, amps, kWatts, and output load percent

Alarms

- Alarm: If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).
- Alarm: If the battery temp exceeds a user-defined threshold.

Parameter

UserHighBatteryTemperatureAlarm - Threshold for alarm state. This alarm is disabled when the threshold is set to the default value of 0.

Filename: `com.dartware.ups.standard.txt`

Version: 3.6

UPS > TrippLite UPS

Use this probe with TrippLite UPS devices.

This probe works best with devices which have implemented the following MIBs:

- UPS MIB (RFC 1628) [... mib-2.upsMIB / ... 1.33]
- TrippUPS MIB [... enterprises.triplite.trippUPS.trippUpsEnvironment / 1.850.0.3]

Values

- **UPS** - vendor, model, software version, and firmware version
- **Battery** - output source, battery status, battery voltage, and battery current
- **Input** - Hz, volts, amps, and kWatts
- **Output** - Hz, volts, amps, kWatts, and output load percent
- **Environment** - ambient temperature, and ambient humidity

Alarms

If the device is reporting any alarms. (The UPS MIB includes a comprehensive list of alarms).

Parameters

None

Filename: `com.dartware.ups.tripplite.txt`

Version: 2.13

UPS > Victron UPS

This probe monitors important values in the Victron UPS.

Parameters

UPS Battery Status - Alarm - ALARM threshold for Battery Status. This can be any of the following:

- 2 - the UPS is working normally.
- 1 - the UPS is on bypass and the device enters Alarm state.

UPS Battery Remaining - Warning - WARNING threshold for the estimated battery time remaining. If the Battery Remaining is less than this threshold, the device is set to Warning.

UPS Battery low Voltage - Warning - WARNING threshold for the min. battery voltage. If the Battery voltage is less than this threshold, the device is set to Warning.

Low Input Voltage line [1,2, or 3] - Alarm - ALARM threshold for the minimum specified input voltage on phase 1, 2, or 3. If the input voltage drops below this threshold, the device is set to Alarm.

Low Output Voltage line [1,2, or 3] - Alarm - ALARM threshold for the minimum specified output voltage on phase 1, 2, or 3. If the output voltage drops below this threshold, the device is set to Alarm.

Filename: `de.medianet.freinet.ups.victron.txt`

Version: 3.1

Servers-Standard

Basic TCP

This basic TCP probe tests whether a TCP port accepts connections. If the specified port fails to accept the TCP connection within sixty seconds, the device state is set to Down.

Parameters

None

Filename: `com.dartware.tcp.basic`

Version: 1.6

Basic TCP (Blocked)

This basic TCP probe tests that a TCP port is **not** accepting connections. This probe may be used to test that a firewall is working properly, or that a particular TCP service is never operating on an important machine.

If the specified port accepts the TCP connection, the device state is set to the selected state. Otherwise, the device status is set to **OKAY**.

Parameter

Failure Status - The device status upon successful connection. The default state is DOWN.

Filename: `com.dartware.tcp.blocked`

Version: 1.6

Custom TCP

This probe sends the specified string over a TCP connection, and sets the status of the device based on the response. Six parameters control the operation of this probe:

Parameters

String to send - The initial string sent to the device via TCP. This could be a command which indicates what to test, or a combination of a command and a password. The string is sent on its own line, terminated by a CR-LF.

Seconds to wait - The number of seconds to wait for a response. If no response is received within the specified number of seconds, the device's status is set to Down.

OK Response - The substring to match the device's "ok response". If it matches the first line received, the device is reported to have a status of OK.

WARN Response - The substring to match the device's Warning response.

ALRM Response - The substring to match the device's Alarm response.

CRIT Response - The substring to match the device's Critical response.

DOWN Response - The substring to match the device's Down response.

If Intermapper cannot connect to the specified TCP port, the device's status is set to Down.

Filename: `com.dartware.tcp.custom`

Version: 1.9

CVS Server

This probe tests a CVS server by connecting to the specified port and authentication strings as shown below. By default, the port is 2401.

```
BEGIN AUTH REQUEST<lf>
```

```
CVSROOT_Path<lf>
```

```
Username<lf>
```

```
Scrambled_password<lf>
```

```
END AUTH REQUEST<lf>\p\
```

If the response is "I LOVE YOU", then the authentication succeeded.

If the response is "I HATE YOU", then either the authentication failed or the path to CVSROOT is incorrect.\p\

Parameters

CVSROOT_path - path to the CVS server

Username - Username for the CVS server

Password - Password used with Username

Filename: `com.dartware.tcp.cvs`

Version: 1.6

DHCPv4/BOOTP

DHCP is the protocol used by IP clients to obtain an IPv4 address and other parameters for using TCP/IP. Depending on your setup, this probe may work only if your computer is already using an IP address acquired using BOOTP or DHCP.

NOTE: On macOS, this probe only works if no DHCP, Bootp, or PPP interfaces are enabled.

The probe sends DHCP-INFORM requests to test the DHCP mechanism for an IP subnet.

Parameters

BOOTP Relay Address - the IP address to which all DHCP requests are addressed. Normal BOOTP/DHCP requests are broadcast to the local subnet (255.255.255.255), where they are picked up by the BOOTP agent in a router and relayed to the BOOTP/DHCP server. If this parameter is left blank, Intermapper sends the DHCP requests directly to the device's IP address.

DHCP Client ID - an optional parameter included with the DHCP-INFORM request that can be used to identify the DHCP client as Intermapper. If this parameter is blank, Intermapper does not include the DHCP Client ID option in its DHCP probe.

DHCP Subnet Mask - an optional parameter that specifies the expected value of the subnet mask returned by the DHCP server. If this parameter is blank, Intermapper accepts any subnet mask value.

DHCP Router Address - an optional parameter that specifies the expected value of the router address returned by the DHCP server. If this parameter is blank, Intermapper accepts any router address value.

DHCP Message Type - the type of DHCP message to send. Typically, you should use DHCP-INFORM, since this type will not cause the DHCP server to allocate an IP address. A DHCP server may respond to a DHCP-DISCOVER request by leasing an IP address which will never be used.

Hardware Address - an optional parameter that specifies the MAC address of the network interface used to send the DHCP request.

Request Seconds - an optional parameter that specifies the number of seconds to claim we have been sending DHCP requests. Certain DHCP servers (such as the one supplied with OS X 10.5 with the default settings) do not respond until the client claims to have been trying for at least 10 seconds.

Filename: `com.dartware.dhcp`
Version: 2.1

Domain Name (DNS) > DNS: (A) Address

DNS is the protocol used by TCP/IP network clients to translate Internet names into IP addresses, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the IP address for a specified domain name.

Parameters

Domain Name - the fully qualified domain name you are attempting to resolve.

IP Address - optional parameter specifies an IP address the domain name should resolve to. If this parameter is not blank, Intermapper reports the status specified in *Failure Status* if one of the returned IP addresses doesn't match this address.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is True, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of False.

Failure Status - the device status Intermapper should report when the IP address in a DNS response doesn't match the specified IP Address parameter. By default, an IP address mismatch sets the device to Alarm. (Down is reserved for complete lack of response by the DNS server.)

Filename: `com.dartware.dns`
Version: 1.9

Domain Name (DNS) > DNS: (MX) Mail Server

The protocol used by TCP/IP network clients to translate Internet names into Mail servers, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the mail server for a specified domain name.

Parameters

Domain Name - the fully qualified domain name to be resolved.

Mail Server - optional - specify a mail server the domain name should resolve to. If this parameter is non-empty, and one of the returned mail servers doesn't match the one provided, a status as specified in Failure Status is returned.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is True, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of False.

Failure Status - specifies the device status returned when the DNS response returns a mail server that doesn't match the specified Mail Server. You can choose Down, Alarm or Warning. By default, mail server mismatches return an Alarm condition; Down is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.mx`
Version: 1.2

Domain Name (DNS) > DNS: (NS) Name Server

The protocol used by TCP/IP network clients to translate Internet names into name servers, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the name server for a specified domain name. CNAME records are accepted if no NS records are present in the response.

Parameters

Domain Name - the fully qualified domain name to be resolved.

Name Server - optional - specify the name server the domain name should resolve to. If this parameter is non-empty, and one of the returned name servers doesn't match the one provided, a status as specified in Failure Status is returned.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is True, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of False.

Failure Status - specifies the device status returned when the DNS response returns a name server that doesn't match the specified Name Server. You can choose Down, Alarm or Warning. By default, name server mismatches return an Alarm condition; Down is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.ns`
Version: 1.2

Domain Name (DNS) > DNS: (PTR) Reverse Lookup

The protocol used by TCP/IP network clients to translate IP addresses into Internet names, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the domain name for a specified IP address. Both PTR and CNAME records are accepted in the response.

Parameters

IP Address - the fully qualified IP address to be resolved.

Domain Name - optional - specify a domain name the IP address should resolve to. If this parameter is non-empty, and one of the returned domain names doesn't match the one provided, a status as specified in Failure Status is returned.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is True, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of False.

Failure Status - specifies the device status returned when the DNS response returns a domain name that doesn't match the specified Domain Name. You can choose Down, Alarm or Warning. By default, mail server mismatches return an Alarm condition; Down is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.ptr`
Version: 1.2

Domain Name (DNS) > DNS: (TXT) Text Record

The protocol used by TCP/IP network clients to translate Internet names into Text records, as defined in [RFC 1034](#) and [RFC 1035](#). This probe sends a DNS request to look up the text record for a specified domain name.

Parameters

Domain Name - the fully qualified domain name to be resolved.

Text Substring - optional - specify a substring of a text record the domain name should resolve to. If this parameter is non-empty, and one of the returned text records doesn't contain the substring provided, the device's condition is set as specified in Failure Status.

Recursion Desired - If the target DNS server cannot resolve the given domain name, and this parameter is True, the DNS server may query an authoritative DNS server. To prevent this behavior, use the default setting of False.

Failure Status - specifies the device status returned when the DNS response text record in a DNS response does not contain the specified Text Substring. You can choose Down, Alarm or Warning. By default, mail server mismatches return an Alarm condition; Down is reserved for when the DNS server fails to respond at all.

Filename: `com.dartware.dns.txt`
Version: 1.2

FTP > FTP (Login)

The standard protocol for transferring files on TCP/IP internets, as defined in [RFC 959](#). The default TCP port number for FTP control connections is port 21.

This TCP probe connects to the FTP server's control port (21). It then logs in using the specified User ID and Password and issues a NOOP command. If the connection is successful, the probe issues the QUIT command and sets the status to Okay.

Parameters

User ID - the account name used to login to the FTP server.

Password - the account password used to verify the User ID's identity.

NOTE: If the probe queries the FTP server often, and at regular intervals, the FTP server's log files contain a succession of Login and Logout log lines.

Filename: `com.dartware.tcp.ftp.login`

Version: 1.9

FTP > FTP (No Login)

The standard protocol for transferring files on TCP/IP internets, as defined in [RFC 959](#). The default TCP port number for FTP control connections is port 21.

This TCP script connects to the FTP server's control port (21). It then issues a NOOP command without logging in. If the connection is successful, the probe issues the QUIT command and sets the status to Okay.

NOTE: Use this script if you are going to be probing the FTP server frequently. Unlike the FTP (login) probe, this probe does generate numerous entries in your FTP logs.

Parameters

None

Filename: `com.dartware.tcp.ftp.nologin`

Version: 1.9

Gopher

The document search and retrieval protocol described in [RFC 1436](#). The default TCP port number for Gopher connections is port 70.

This script connects to a Gopher server and sends the specified *Selector string*. By default, the *Selector string* is empty; the Gopher server returns top level information as a sequence of lines. This script simply checks that data is returned by the gopher server; it does not validate the data's contents.

Parameter

Selector string - the string sent to the Gopher server. By default, this string is empty.

Filename: `com.dartware.tcp.gopher`
Version: 1.7

Host Resources

This probe uses SNMP to monitor elements of the Host Resources MIB of the target device.

Parameters

Processor Load Alarm % - Specifies the threshold, as a percentage of processor load, to enter ALARM state.

Processor Load Warning % - Specifies the threshold, as a percentage of processor load, to enter state.

Disk Usage Alarm % - Specifies the threshold, as a percentage of disk usage, to enter ALARM state.

Disk Usage Warning % - Specifies the threshold, as a percentage of disk usage, to enter WARNING state.

Memory Usage Alarm % - Specifies the threshold, as a percentage of memory usage, to enter ALARM state.

Memory Usage Warning % - Specifies the threshold, as a percentage of memory usage, to enter WARNING state.

One-minute Load Average Alarm - Specifies the one-minute load average value to enter ALARM state.

One-minute Load Average Warning - Specifies the one-minute load average value to enter WARNING state.

Five-minute Load Average Alarm - Specifies the five-minute load average value to enter ALARM state.

Five-minute Load Average Warning - Specifies the five-minute load average value to enter WARNING state.

Fifteen-minute Load Average Alarm - Specifies the fifteen-minute load average value to enter ALARM state.

Fifteen-minute Load Average Warning - Specifies the fifteen-minute load average value to enter WARNING state.

Ignore storage table indices After the device is polled, select the storage table entries you want to ignore. The selected entries do not cause alarms or warnings and are not be displayed in the Status window.

Filename: `com.dartware.snmp.hrmib`
Version: `1.13`

HTTP & HTTPS > HTTP

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML.

Parameters

Host Name - the domain name of the web server (for example, `www.Intermapper.com`). This can be derived from the host name part of the URL that you want to test. Only enter an IP address or domain name; do not add `http://`.

URL Path - the full path of the desired file on the web server (for example, `/index.html`). This can be empty to get to the root page of the site.

String to verify - the string to verify in the data returned by the HTTP server. For example, if you are retrieving a web page, you might search for "`<HTML`" or "`<P>`" to verify that the data is HTML. If this string is not found, the device will go into alarm.

User ID - the user name typed into the web browser's password dialog. The default is to leave this blank. You should set this parameter if you want to test a web page that requires authentication.

Password - the password for the web browser's dialog. The default is to leave this blank. Set this parameter if you want to test a web page that requires authentication.

HTTP & HTTPS > HTTP (Don't Match)

Use this probe to search for a string that should not match.

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. If the string is present, then the device goes to a warning state.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). This can be derived from the host name part of the URL that you want to test. Only enter an IP address or domain name; do not add http://.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

String to detect - a string is not expected in HTTP server's response. If the string is present, the device goes to a Warning severity.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Filename: com.dartware.tcp.http-nomatch.txt

Version: 2.5

HTTP & HTTPS > HTTP (Follow Redirects)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. This probe will follow a limited number of page redirects to the same HTTP server.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). This can be derived from the host name part of

the URL that you want to test. You must enter a valid Host Name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add http://.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to request the root page of the site.

String to verify - a string to verify in the HTTP server's response. For example, if you are retrieving a web page, you could search for <HTML or <P> to verify that the data is HTML. If the string is not found, the device goes into Alarm.

User ID - the user name typed into the web browser's password dialog. Leave this blank unless you want to test a web page that requires authentication.

Password - the password for the web browser's dialog. Leave this blank unless you want to test a web page that requires authentication.

Redirect Limit - the maximum number of redirects to follow.

Filename: com.dartware.tcp.http.follow
Version: 1.3

HTTP & HTTPS > HTTP (Post)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you post form results to a specific web CGI and verify that the POST operation worked.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). This can be derived from the host name part of the URL that you want to test. Only enter an IP address or domain name; do not add http://.

URL Path - the full path to the desired CGI on the web server (for example, /index.cgi). This can be empty to get to the root page of the site.

Form Data - the encoded data sent in the body of the POST message.

String to verify - a string expected in HTTP server's response. For example, if you post form data that is designed to generate an error, you might search for sorry or could not be processed to verify that the CGI is properly rejecting the data. If this string is not found, the device goes into alarm.

Filename: `com.dartware.tcp.http.cgi.post`

Version: 2.8

HTTP & HTTPS > HTTP (Proxy)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server can be accessed using a remote proxy server as an intermediary. For example, this probe can check if your web server is accessible from some remote location on the Internet.

Parameters

Host Name - the domain name of the web server (for example, `www.Intermapper.com`). This is the host name part of the URL that you want to test.

NOTE:

The host name is likely to be different from that of the actual device on the map. If the host name is not specified, the probe assumes it is included in the URL Path, and no adjustment to the path is made.

URL Path - the relative URI of the desired file on the web server (e.g. `/index.html`). This can be empty to get to the root page of the site. If Host Name is empty, this should contain the absolute URI.

Proxy User ID - your user ID for the proxy server. Leave this field blank if no authentication is required to use the proxy server.

Proxy Password - your password for the proxy server. Leave this field blank if no authentication is required to use the proxy server.

String to verify - a string expected in HTTP server's response. For example, if you are retrieving a web page, you might search for `<HTML` or `<P>` to verify that the data is HTML. If this string is not found, the device goes into alarm.

User Agent - the string that identifies this Intermapper client probe to the proxy web server. Some proxy servers block traffic at the proxy based on the User-Agent identity. This parameter allows you override Intermapper's default User-Agent setting. Leave this parameter blank to send a User-Agent string of Intermapper/version" where version is the current version number of Intermapper.

Filename: `com.dartware.tcp.http.proxy`
Version: 2.12

HTTP & HTTPS > HTTP (Redirect)

HTTP (Redirect)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server is redirecting certain URL's to a specific URL.

Parameters

Host Name - the domain name of the web server (for example, `www.Intermapper.com`). This can be derived from the host name part of the URL that you want to test.

URL Path - the full path of the desired file on the web server (for example, `/index.html`). This can be empty to get to the root page of the site.

Redirect URL - the complete URL that the given URL Path is redirected to. The URL should begin with `http://`.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter if you want to test a web page that requires authentication.

Filename: `com.dartware.tcp.http.redirect`
Version: 1.15

HTTP & HTTPS > HTTPS

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML.

Parameters

Host Name - the domain name of the web server (e.g. "www.intermapper.com"). Use the host name part of the URL that you want to test. You must enter a valid "Host Name" to test web servers which implement virtual hosts.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

String to verify - the string to verify in the data returned by the HTTP server. For example, if you are retrieving a web page, you might search for <HTML or <P> to verify that the data is HTML. If this string is not found, the device will go into alarm.

User ID - the login user name. Set this parameter to test a web page that requires authentication.

Password - the login password. Set this parameter to test a web page that requires authentication

Filename: `com.dartware.tcp.https`

Version: 2.9

HTTP & HTTPS > HTTPS TLSv1.0

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). Use the host name part of the URL that you want to test. You must enter a valid host name to test web servers which implement virtual hosts.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

String to verify - a string expected in the HTTP server's response. For example, if you are retrieving a web page, you might search for <HTML or <P> to verify that the data is HTML. If this string is not found, the device goes into Alarm.

User ID - the login user name. Set this parameter to test a web page that requires authentication.

Password - the login password. Set this parameter to test a web page that requires authentication.

Filename: com.dartware.tcp.https-tlsv10.txt
Version: 2.10

HTTP & HTTPS > HTTPS (Follow Redirects)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTPS connections is port 443.

This TCP probe lets you download a specific web page and scan it for a specific string of HTML. This probe will follow a limited number of page redirects to the same HTTPS server.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). This can be derived from the host name part of the URL that you want to test. You must enter a valid host name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add http://.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

String to verify - a string to verify in the server's response. For example, if you are retrieving a web page, you could search for <HTML or <P> to verify that the data is HTML. If the string is not found, the device goes into Alarm.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Redirect Limit - the maximum number of redirects to follow.

Filename: `com.dartware.tcp.https.follow`
Version: 1.2

HTTP & HTTPS > HTTPS (Post)

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTPS connections is port 443.

This TCP probe lets you post form results to a specific web CGI over a secure connection and verify that the POST operation worked.

Parameters

Host Name - the domain name of the web server (for example, `www.Intermapper.com`). This can be derived from the host name part of the URL that you want to test. You must enter a valid host name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add `http://`.

URL Path - the full path to the desired CGI on the web server (for example, `/index.cgi`). This can be empty to get to the root page of the site.

Form Data - the encoded data sent in the body of the POST message.

String to verify - a string to verify in the server's response. For example, if you post form data that is designed to generate an error response, you might search for "sorry" or "could not be processed" to verify that the CGI is properly rejecting the data. If the string is not found, the device goes into Alarm.

NOTE: The implementation of this probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.https.cgi.post`
Version: 1.14

HTTP & HTTPS > HTTPS (Redirect)

The protocol used to transfer web pages on the World Wide Web, defined in [RFC 2068](#) and [RFC 1945](#). The default TCP port number for HTTP connections is port 80.

This TCP probe lets you test that a web server is redirecting certain URL's to a specific URL.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). This can be derived from the host name part of the URL that you want to test. You must enter a valid host name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add "http://".

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

Redirect URL - the complete URL that the given URL Path is redirected to. The URL should begin with https://.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

Filename: com.dartware.tcp.https.redirect.txt
Version: 1.5

HTTP & HTTPS > HTTPS (SSLv3)

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML. Unlike the default HTTPS probe, this probe does not attempt to auto-negotiate a TLSv1 connection, making it compatible with some older application servers.

This probe lets you establish a secure connection to a web server, download a specific web page, and scan it for a specific string of HTML. Unlike the default HTTPS probe, this probe will not attempt to auto-negotiate a TLSv1 connection, making it compatible with some older application servers.

Parameters

Host Name - the domain name of the web server (for example, `www.Intermapper.com`). This can be derived from the host name part of the URL that you want to test. You must enter a valid host name to test a web server that implements a virtual host. Add only an IP address or domain name; do not add `http://`.

URL Path - the full path of the desired file on the web server (for example, `/index.html`). This can be empty to get to the root page of the site.

String to verify - a string to verify in the server's response. For example, if you are retrieving a web page, you could search for `<HTML` or `<P>` to verify that the data is HTML. If the string is not found, the device goes into Alarm.

User ID - the user name typed into the web browser's password dialog. Set this parameter to test a web page that requires authentication.

Password - the password for the web browser's dialog. Set this parameter to test a web page that requires authentication.

NOTE: The implementation of this probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.https.notls.txt`
Version: 1.5

HTTP & HTTPS > HTTPS-TLSv1.0

The protocol used for secure transfer of web pages on the World Wide Web. The default TCP port number for HTTP connections is port 443.

This probe establishes a secure connection to a web server, downloads a specific web page, and scans it for a specific string of HTML.

Parameters

Host Name - the domain name of the web server (for example, www.Intermapper.com). Use the host name part of the URL that you want to test. You must enter a valid "Host Name" to test web servers which implement virtual hosts.

URL Path - the full path of the desired file on the web server (for example, /index.html). This can be empty to get to the root page of the site.

String to verify - a string expected in the HTTP server's response. For example, if you are retrieving a web page, you might search for <HTML or <P> to verify that the data is HTML. If this string is not found, the device goes into Alarm.

User ID - the login user name. Set this parameter to test a web page that requires authentication.

Password - the login password. Set this parameter to test a web page that requires authentication.

Filename: `com.dartware.tcp.https`
Version: 2.9

IPMI v2.0

This probe implements version 2.0 of the Intelligent Platform Management Interface (IPMI) over a LAN. It sends UDP-based RMCP+ packets to a Baseboard Management Controller (BMC) located within a server or workstation. The BMC is hardware which permits network-based management of the computer even when it is turned off, i.e. "lights-out management".

Parameters

User - (required) administrator-level user name to the BMC.

Password - (required) the password for the specified user.

Dialect - The variant of the IPMI protocol. There are subtle differences in implementations of IPMI in various products.

- To use this probe with an Apple XServe 2008 or earlier, set the Dialect parameter to XServe.

- For Dell Servers, the Apple XServe 2009, and any other product set the Dialect parameter to Other.

This probe supports one-key, non-anonymous logins only. Internally, it uses RAKP-HMAC-SHA1 and AES-CBS-128 for authentication and confidentiality, respectively. The firewall configuration of the BMC must permit UDP packets from Intermapper.

Filename: `com.dartware.ipmi.txt`
Version: 1.2

IRC

This probe tests whether Intermapper can register a connection with an IRC server. This probe establishes a connection to the IRC server and issues the PASS, NICK, and USER commands. It verifies that the IRC server returns a particular string, in its welcome message, for example.

Parameters

Password - the connection password. This parameter is passed using the PASS command.

Nickname - the connection nickname. This parameter is passed using the NICK command.

Username - username, hostname, servername and realname of the new user. Typically, the hostname and servername are ignored for client connections. The realname must be prefixed with a ':'.

String to verify - a string to verify in the data returned by the IRC server. For example, you might check for a string returned in the IRC server's welcome message.

Filename: `com.dartware.tcp.irc`
Version: 1.6

LDAP > LDAP

The protocol used to access directories supporting the X.500 models, as described in [RFC 2251](#).

This probe connects to the LDAP server and binds using the designated Bind Name and Bind Password (if specified).

Parameters

Bind Name - the LDAP name to be authenticated

Bind Password - the password to be used with the Bind Name. It is sent as clear text to authenticate the probe.

Field to Match - after you are logged in, the probe sends a SearchRequest for Field to Match, searching for an equality match of Name to Lookup, and counts the number of LDAP records returned.

Search Base - If specified, this value is used as the base of the search. Otherwise, the Bind Name is used for the Base DN.

Filename: `com.dartware.tcp.ldap`
Version: `1.10`

LDAP > LDAP SSL

The protocol used to access directories supporting the X.500 models, as described in [RFC 2251](#).

This probe connects to the LDAP server through a secure connection, and binds using the designated Bind Name and Bind Password (if specified).

Parameters

Bind Name - the LDAP name to be authenticated

Bind Password - the password to be used with the Bind Name. It is sent as clear text to authenticate the probe.

Field to Match - after you are logged in, the probe sends a SearchRequest for Field to Match, searching for an equality match of Name to Lookup, and counts the number of LDAP records returned.

Search Base - if specified, this value is used as the base of the search. Otherwise, the Bind Name is used for the Base DN.

Filename: `com.dartware.tcp.ldap.ssl`
Version: `1.10`

LPR

The print server protocol used to print over a TCP/IP network, as defined in [RFC 1179](#). The default TCP port number for LPR connections is port 515.

Parameter

Queue Name - a queue name if applicable to your printer.

Filename: `com.dartware.tcp.lpr`
Version: 1.8

Mail > IMAP4

The protocol used for accessing and manipulating email messages on a server, as defined in [RFC 2060](#). The default TCP port number for IMAP4 connections is port 143.

This TCP script connects to the IMAP4 server and issues a CAPABILITY command, a NOOP command, and finally terminates with a LOGOUT command. The script checks the server's response to the CAPABILITY command to verify that the server supports IMAP4 or IMAP4rev1.

Parameters

None

Filename: `com.dartware.tcp.imap4`
Version: 1.8

Mail > IMAP4 SSL

The protocol used for accessing and manipulating email messages on a server, as defined in [RFC 2060](#). This probe tests a secure connection to the IMAP server. The default TCP port number for secure IMAP connections is port 993.

This TCP script connects to the IMAP4 server and issues a CAPABILITY command, a NOOP command, and finally terminates with a LOGOUT command. The script checks the server's response to the CAPABILITY command to verify that the server supports IMAP4 or IMAP4rev1.

Parameters

None

Filename: `com.dartware.tcp.imap4.ssl`
Version: 1.8

Mail > POP3

The protocol used to access email messages from a central maildrop server, as defined in [RFC 1939](#). The default TCP port number for POP3 connections is port 110.

Parameters

User Name - the POP3 account user name. If left empty, this probe verifies that the server sends +OK as its initial greeting, then immediately sends the QUIT command.

Password - the POP3 account password. If User Name is specified, this probe attempts to login to the POP3 server using the specified password. If the probe fails to authenticate, the device will be marked in warning.

Use APOP if supported - by default, this probe uses the APOP command to authenticate the user if the APOP command is supported by the server. To authenticate using the USER and PASS commands for a particular user, set the Use APOP if supported parameter to False.

NOTE:

The Use APOP if supported option has no effect if APOP is not supported by the server.

Filename: `com.dartware.tcp.pop3`
Version: 2.7

Mail > POP3 SSL

The protocol uses PO3 over SSL to access email messages from a central maildrop server, as defined in [RFC 1939](#). The default TCP port number for POP3-SSL connections is port 995.

Parameters

User Name - the POP3 account user name. If left empty, this probe verifies that the server sends +OK as its initial greeting, then immediately sends the QUIT command.

Password - the POP3 account password. If User Name is specified, this probe attempts to login to the POP3 server using the specified password. If the probe fails to authenticate, the device will be marked in "warning".

Use APOP if supported - by default, this probe uses the APOP command to authenticate the user if the APOP command is supported by the server. To authenticate via USER and PASS commands for a particular user, set the Use APOP if supported parameter to False.

NOTE:

The Use APOP if supported option has no effect if APOP is not supported by the server.

Filename: `com.dartware.tcp.pop3.ssl`

Version: 2.7

Mail > Roundtrip IMAP

This probe tests an IMAP server and measures the time it takes to send a message (via SMTP) and retrieve it (via IMAP). It sends a short message to the specified SMTP server, and continually attempts to retrieve the message via IMAP from the device being tested. The probe alerts if the server fails to respond properly or the round-trip time exceeds the specified timeout.

Parameters

SMTP Server - the server to receive the SMTP message. If left blank, the device being tested is used as the target.

SMTP User and **SMTP Password** (optional) - the user name and password to be used when sending the message. Leave blank if not required.

Email To - the email address to which the message is sent.

Email From - the From: address in the message.

IMAP User and **IMAP Password** - the user name and password used to log into the IMAP server to retrieve the message.

Timeout - the specified timeout, measured in seconds.

Filename: `com.dartware.email.imap.txt`

Version: 1.4

Mail > SMTP

The standard protocol used to transfer electronic mail on the Internet, as defined in [RFC 821](#). The default TCP port number for SMTP connections is port 25.

This probe tries to verify that a specified email address exists on the SMTP server, using the VRFY command. It connects to the SMTP server, introduces itself using the HELO command, then issues a VRFY command for the specified email address. When it has received a response, the script sends the QUIT command before closing its connection to the server.

Parameter

Email Address - the name or email address that we are attempting to verify.

Filename: `com.dartware.tcp.smtp`
Version: 2.0

Mail > SMTP TLS

The standard protocol used to transfer electronic mail on the Internet, as defined in [RFC 821](#). This probe tests a secure connection to the SMTP server. The default TCP port number for secure SMTP connections is port 25.

This probe tries to verify that a specified email address exists on the SMTP server, using the VRFY command. It connects to the SMTP server, introduces itself using the HELO command, then issues a VRFY command for the specified email address. When it has received a response, the script sends the QUIT command before closing its connection to the server.

Parameter

Email Address - the name or email address that we are attempting to verify.

Filename: `com.dartware.tcp.smtp.tls`
Version: 1.8

Multimedia > Multicast Listener

This probe lets you listen for UDP packets directed to a specific UDP port. If you specify a multicast IP address, Intermapper will listen for packets

directed to that multicast address. This probe will change the device status to the DOWN if a packet isn't received within specified number of seconds (the default is 10 seconds).

The Multicast Listener probe can be used to verify that a multicast source is broadcasting, for example, a live QuickTime broadcaster.

This probe is passive; it only listens, and does not inject any traffic into the network.

Parameters

Multicast IP Address - (optional) multicast IP address to listen on.

Seconds to wait - the maximum number of seconds to wait between packets. If a packet is not received within the specified number of seconds, the device's status is set to DOWN. The "Seconds to wait" timer is reset every time a packet is received.

Verify Source Address - specifies whether the probe should count packets only from the IP address of the targeted device.

Filename: `com.dartware.udplistener`

Version: 2.1

Multimedia > RTSP

The protocol used to control real-time streams, defined in [RFC 2326](#) and [RFC 1889](#). The default TCP port number for RTSP connections is port 554.

This TCP probe lets you check that the server is up and responding.

The specifics of the commands that the probe must send to the server vary somewhat depending upon the version of RFC2326 that the server implements. If the server you're monitoring implements RFC2326bis-02 or later, then set RFC2326bis-02 or later to Yes. If you're not sure, leave it set to No. If the device goes into warning with the reason set to [RTSP] Unexpected response to PLAY command. (RTSP/1.0 460 Only Aggregate Option Allowed), then set it to Yes.

Parameters

Movie Name - the name of the media you want to use to test server status

Seconds to play - the number of seconds to play the media before returning a status

RFC2326bis-02 or later - specify whether the server implements RFC2326bis

Filename: `com.dartware.tcp.rtsp`
Version: 2.2

Network Time

The protocol used to synchronize time between computers, defined in [RFC 1119](#).

This probe sends a client-mode current-time request to the NTP server. By default, NTP requests are sent to UDP port 123.

Parameters

None

Filename: `com.dartware.ntp`
Version: 1.6

NNTP

The protocol used to read network news on TCP/IP Internets, as defined in [RFC 977](#). The default TCP port number for NNTP connections is port 119.

This script connects to the news server and uses the GROUP command to ask for information about a specific newsgroup name. The script then issues the QUIT command to tell the server it is closing the connection.

Parameter

Newsgroup - the name of the newsgroup that you want to verify.

Filename: `com.dartware.tcp.nntp`
Version: 1.7

RADIUS

The protocol used by remote access servers to authenticate dial-in users, as defined in [RFC 2138](#). This probe tests a RADIUS server by sending an Access-Request packet to authenticate a specific user name and password. Before you can use this probe with a particular RADIUS server, you must add the Intermapper computer's IP address to the RADIUS server and choose a "shared secret" for it. The "shared secret" is used by the RADIUS protocol to encrypt passwords in RADIUS requests. A RADIUS server does not answer access-requests from a client it doesn't recognize.

The official port number for RADIUS is 1812. Some RADIUS servers, however, use port number 1645 for historical reasons.

Parameters

Shared Secret - Intermapper's unique password into the RADIUS server. Since it is used for authentication, the same value must be configured in the RADIUS server as well.

User Name - The user name to be used for Intermapper's authentication.

Password - The password for the specified user name. The password is not sent in the clear; it is encrypted using the shared secret.

Filename: `com.dartware.radius`
Version: 1.9

SIP over UDP

The protocol used to set up voice communications for Voice-over-IP (VOIP), as described in [RFC 3261](#). This probe sends a SIP request in a single UDP packet and checks for a valid SIP response.

By default, this probe sends an OPTIONS command to the target device. However, some VOIP systems do not answer un-authenticated OPTIONS requests. For these devices, change the command to REGISTER.

Parameters

URI - The SIP uniform resource identifier in the request.

Command - The SIP command to send in the request.

Filename: `com.dartware.sip.txt`
Version: 1.1

SNPP

This protocol transfers pager information across the Internet, as defined in [RFC 1861](#). The default TCP port number for SMTP connections is port 444.

This SNPP probe verifies that an SNPP server is working by connecting to it and issuing a PAGE <pagerid> command. If it receives a valid response code, the probe issues a QUIT command and exits, setting device status to OK.

If an Invalid Pager ID response is received, the probe issues a QUIT command and exits, setting device status to Alarm.

If no connection was made, or if an unexpected response is received, device status is set to Down.

Parameter

PagerID - your Pager ID on the specified SNPP server.

Filename: `com.dartware.tcp.snpp`

Version: 1.6

SSH

The protocol used for secure remote login. The default TCP port number for SSH connections is port 22.

This probe opens a TCP connection to the specified port and looks for the identification string that indicates an SSH server as specified in [RFC 4253](#).

Parameter

Require SSH 2.0 - If set to **true** and the server doesn't require SSH 2.0, the device is set to Alarm.

Filename: `com.dartware.tcp.ssh.txt`

Version: 1.4

Subversion > SVN (Apache)

This probe tests a Subversion server running as an Apache module. The subversion module lets Apache function as a WebDAV/DeltaV server. Since the server responds normally to HTTP GET requests, testing whether it is up is the same as performing an HTTP GET request and checking to ensure the

location was found.

Parameters

Host Name - the domain name of the subversion server (for example, svn.collab.net). Includes only the IP address or domain name; do not include http://.

URL Path - the path to the repository. The first and last characters must be a forward slash (/).

User ID - the user name used for authentication by the subversion server, if required.

Password - the password used for authentication by the subversion server, if required.

Subversion is a version control system intended as a replacement for CVS. The software is released under an Apache/BSD style open-source license. The project can be found at <http://subversion.tigris.org>.

Filename: `com.dartware.tcp.svn.apache`
Version: 1.1

Subversion > SVN (Svnserve)

This probe tests a stand-alone svnserve Subversion server. It connects to the svnserve using its default port 3690. The server returns a response to indicate it is running. If a repository location is specified, the probe then tries to connect to that repository. If a username is specified, the probe tries to authenticate using CRAM-MD5, otherwise it connects anonymously.

Parameters

Repository - the subversion repository path (for example, svn/experimental). It should not begin with a forward slash (/).

User ID - the user name used for authentication by the subversion server, if required.

Password - the password used for authentication by the subversion server, if required.

Subversion is a version control system intended as a replacement for CVS. The software is released under an Apache/BSD style open-source license. The project can be found at <http://subversion.tigris.org>.

A description of the custom protocol used by svnserve can be found at http://svn.collab.net/repos/svn/trunk/subversion/libsvn_ra_svn/protocol.

Filename: `com.dartware.tcp.svn.svnserve`

Version: `1.1`

Telnet

The protocol used for terminal-to-terminal communication and distributed computation as described in [RFC 854](#). The default TCP port number for Telnet connections is port 23.

This probe lets you Telnet to a device, login with a name and password, and optionally enter a command. This probe is specifically designed to reject any Telnet options proffered by the Telnet server; the TCP connection always remains in the base "network virtual terminal" state. This probe lets you enter data at up to three prompts.

If the probe times out while trying to match a "string-to-match" field, returns a Down status

NOTE: The "string-to-match" fields accept regular expressions.

Parameters

Intro String to Match - a string to match in the welcome banner sent by the Telnet server when you first connect. Leave this parameter blank if you want to match anything in the welcome banner.

First Prompt - the string to match in the first prompt. (for example, Login)

Reply #1 - your reply to the first prompt. (for example, your response to the Login prompt)

Second Prompt - the string to match in the second prompt. (for example, Password) If this parameter is empty, the probe ignores the prompt string and it does not send its reply.

Reply #2 - your reply to the second prompt. (for example, your response to the Password prompt.)

Third Prompt - the string to match in the third prompt. If this parameter is empty, the probe ignores the prompt string and its reply.

Reply #3 - your reply to the third prompt.

Final String to Match - The final string to match. This could be a response to a command you entered in the previous step.

Filename: `com.dartware.tcp.telnet`
Version: 1.9

VNC Server

Attempt to connect to a VNC Server. VNC uses RFB (Remote Frame Buffer) protocol for communication between clients and server. The probe waits to receive a RFB `###.###` string. If it arrives, the VNC server is assumed to be up and the probe simply disconnects.

The Virtual Network Computer (VNC) protocol was originally designed at AT&T Labs in Cambridge. There are many implementations: the developers now support it from the RealVNC site at <http://www.realvnc.com/>.

Parameters

None

Filename: `com.dartware.tcp.vnc`
Version: 1.8

Servers-Proprietary

4D Server

This probe attempts to connect to a 4D server listening on port 19813. If the response contains the database name, the probe exits with OKAY status; if not, the result is WARN. If no response is received within the timeout, the probe exits with a WARN status.

Parameters

database name - the name of an existing database on the 4D server.

timeout - the number of seconds to wait for a response before returning a WARN status.

Filename: `com.dartware.tcp.4D`

Version: 1.6

Apache

This probe monitors an Apache Web server with the Apache Status module enabled (`mod_status`). The Apache Status module allows a server administrator to find out how well an Apache server is performing. This probe reads output of provided by the Status module that presents the current server statistics, using the `?auto` parameter.

To enable status reports for this probe, add the following to the `httpd.conf` file on the target server:

```
<Location /server-status>
SetHandler server-status
Order Deny,Allow
Deny from all
Allow from Intermapper-Address
</Location>
```

This probe supports the Apache `ExtendedStatus` directive, if enabled.

Parameters

Host Name - the name of the host server.

URL Path - the path to the server status page.

User ID - the server administrator username.

Password - the administrator password.

Filename: `com.dartware.tcp.apache.txt`

Version: 1.1

Apple > AppleShareIP

The file-sharing protocol used by Apple computers over TCP/IP. The default TCP port number for AppleShareIP connections is port 548.

This TCP probe connects to the AppleShareIP port and issues a Get Server Info request. If the probe does not receive the expected response, the device's status is set to Down.

This probe sends a request; it does not create an AppleShare session.

Parameters

None

Filename: `com.dartware.tcp.appleshareip`
Version: 1.6

Apple > OS X Server > AFP

This TCP probe queries a [macOS Server](#) installation for various details about its Apple File Sharing using the Server Admin port and protocol.

Sends a request for status information via an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An administrator user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS .

Filename: `com.dartware.tcp.osxserver.afp.txt`
Version: 1.0

Apple > OS X Server > FTP

This TCP probe queries a [macOS Server](#) installation for various details about its FTP server using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.ftp.txt`

Version: 1.0

Apple > OS X Server > Info

This TCP probe queries a [macOS Server](#) installation for various details using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.info.txt`

Version: 1.0

Apple > OS X Server > NAT

This TCP probe queries a [macOS Server](#) installation for various details about its NAT service using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port. The server responds with XML data that is then parsed by the probe.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.nat.txt`

Version: 1.0

Apple > OS X Server > Print

This TCP probe queries a [macOS Server](#) installation for various details about its Print Server using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.print.txt`

Version: 1.0

Apple > OS X Server > QTSS

This TCP probe queries a [macOS Server](#) installation for various details about its QuickTime Streaming server using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.qtss.txt`

Version: 1.0

Apple > OS X Server > Web

This TCP probe queries a [macOS Server](#) installation for various details about its Web server using the Server Admin port and protocol.

This probe requests status information using an HTTPS post to the Server Admin port and parses an XML response.

Parameters

User - the name of any user on the specified server. An admin user is not required.

Password - the user's password.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.osxserver.web.txt`

Version: 1.0

Apple > RTMP

This probe sends an AppleTalk RTMP RDR Request query of type 3 and waits for a RTMP response.

Parameters

None

Filename: `com.dartware.rtmp`

Version: 1.5

Apple > Xserve > Xserve G4

This TCP probe queries an Xserve G4 for various details using the Server Monitor port and protocol.

NOTE:

This probe monitors Xserve G4s running macOS 10.3.9 and lower. For Xserves running 10.4 or higher, select the Xserve Tiger probe.

This probe requests status information using an HTTPS post to the Server Monitor port. The server responds with XML data that is then parsed by the probe.

Parameters

User - the name of any user on the specified server.

Password - the password of the user.

OS Version - the version of macOS server that is running on Xserve.

The following options allow you to display or ignore corresponding data. These options correspond to the tabs in the Server Monitor application on the macOS server.

Info - general information about the server, such as amount of RAM, operating system name, and operating system version.

Drives - information about drives installed on the server. This information includes the manufacturer, model, and capacity of each drive.

Power - information about the power supply.

Network - information about the network. Includes the hardware address, IP address, traffic information, and type of each interface.

Temperature - the ambient temperature of the server.

Blowers - the speed of the server's cooling fans.

Security - monitors the state of the security lock and the enclosure.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.xserve.details`

Version: 1.0

Apple > Xserve > Xserve G5

This TCP probe queries an [Xserve G5](#) for various details using the Server Monitor port and protocol.

This probe requests status information using an HTTPS post to the Server Monitor port and parses an XML response.

Parameters

User - the name of any user on the specified server.

Password - the password of the specified user.

The following options allow you to display or ignore data in the response. These options correspond to tabs in the Server Monitor application on the macOS server.

Info - general information about the server. Includes amount of RAM, operating system name, and operating system version.

Drives - information about the drives installed on the server. Includes the manufacturer, model, and capacity of each drive.

Power - information about the power supply.

Network - information on the network. Includes the hardware address, IP address, traffic information, and type of each interface.

Temperature - the ambient temperature of the server.

Blowers - information on the speed of the server's cooling fans.

Security - the state of the security lock and the enclosure.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.xserve.g5.txt`

Version: 1.0

Apple > Xserve > Xserve RAID

This TCP probe queries an [Xserve RAID](#) for various details using the RAID Admin port and protocol.

This probe sends requests to an Xserve Raid using an HTTPS post on a series of HTTP POSTs and parses an XML responses.

Parameter

Password - the RAID administrator's monitoring password.

Filename: `com.dartware.tcp.xserve.raid.txt`
Version: 1.0

Apple > Xserve > Xserve Tiger (PPC)

This probe queries an [Xserve](#) running macOS 10.4 using the Server Monitor port and protocol. Because of this, the probe requires an administrator name and password to access information. Due to significant hardware differences, there are separate probes for G4 Xserves, G5 Xserves, and Intel Xserves.

Apple preconfigured several thresholds for various properties, such as temperatures, blower speeds, and power supply values. The Server Monitor protocol specifies these thresholds. The error message and status are reflected by this probe.

This probe requests status information using an HTTPS post to the Server Monitor port and parses an XML response.

Parameters

User - the name of any user on the specified server.

Password - the password of the specified user.

The following options allow you to display or ignore data in the response. These options correspond to tabs in the Server Monitor application on the macOS server.

Info - general information about the server. Includes the amount of RAM, operating system name, and operating system version.

Drives - information about the drives installed on the server. Includes the manufacturer, model, and capacity of each drive.

Power - information about the power supply.

Network - information about the network. Includes the hardware address, IP address, traffic information, and type of each interface.

Temperature - the ambient temperature of the server.

Blowers - information on the speed of the server's cooling fans.

Security - the state of the security lock and the enclosure.

NOTE: This probe uses OpenSSL on macOS.

Filename: `com.dartware.tcp.xserve.tiger.txt`

Version: 1.0

Barracuda > Barracuda HTTP

This TCP probe queries a [Barracuda Spam Firewall](#) for various performance statistics.

The BASIC > Status page of the Administrators interface is retrieved using HTTP.

Parameters

User - the name of the firewall administrator.

Password - the password of the firewall administrator.

Port - the Web Interface HTTP Port of the firewall as set on the BASIC > Administration page.

Thresholds

Set thresholds as follows:

In/Out Queue Size - the returned value should normally be less than 100. An In or Out Queue value that consistently exceeds 100 for more than 30 minutes can indicate a problem that needs attention.

NOTE: The returned value can rise temporarily, then go back down after 10 or 15 minutes.

- For the Inbound Queue, this is normal behavior, but can also be the result of an orchestrated attack. Barracuda attempts to read as many messages as it can, which results in a slower processing rate, which in turn increases the number of messages in the queue.
- For the Outbound Queue, an increase usually indicates that the destination server is unavailable or the local DNS is not functioning properly.

Recommended Settings

- **Warnings** - a value exceeding 100 for more than 15 minutes.
- **Alarms** - a value exceeding 500 for more than 30 minutes.

Average Latency - The average time, in seconds, to receive, process and deliver the last 30 messages. The value should be under 50 seconds. If the latency consistently exceeds 50 seconds for more than 30 minutes, there might be a problem that needs attention. Sometimes the value rises temporarily and goes back down after 10 or 15 minutes. This is normal behavior.

Recommended Settings

- **Warnings** - a value exceeding 50 seconds for more than 15 minutes.
- **Alarms** - a value exceeding 150 seconds for more than 30 minutes.

Last Message - The time, in minutes, since the last message was received. For a busy machine, this value should be less than 5 minutes. A value consistently exceeding 20 minutes for more than 30 minutes might indicate a problem that needs attention. Sometimes the value rises temporarily and goes back down after 2 or 3 minutes. This is normal behavior.

Recommended Settings

- **Warnings** - a value exceeding 15 minutes.
- **Alarms** - a value exceeding 30 minutes.

CPU 1/CPU 2 Fan Speed - Should be between 3,000 and 5,000 (RPM)

Recommended Settings

- **Warnings** - a value for either CPU fan that falls below 2500.
- **Alarms** - a value for either CPU fan that falls below 500.

Firmware Storage - the typical value is between 60% and 80%. A value above 80% usually means that a debug file needs to be deleted. This can be done on a non-emergency basis.

Recommended Settings

- **Warnings** - a value above 80%.
- **Alarms** - a value above 90%.

Mail/Log Storage - the typical value is between 1% and 70%.

Recommended Settings

- **Warning** - a value above 70%.
- **Alarm** - a value above 80%.

System Load - The system's load (in percentage). During normal operation, this value can vary wildly, anywhere between 1 and 100%. A value that remains at 100% for more than 2 hours might indicate a problem that needs attention. Sometimes the value rises and goes back down after 2 or 3 minutes. This is normal behavior.

Recommended Settings

- **Warning** - a value above 80%.
- **Alarm** - a value above 90% for more than 3 hours.

CPU Temperature - Should be between 40 and 70 degrees C.

Recommended Settings

- **Warning** - a value above 70 degrees C for more than 30 minutes.
- **Alarm** - a value above 80 degrees C for more than 1 hour.

Filename: `com.dartware.tcp.barracuda.http.txt`
Version: 3.1

Barracuda > Barracuda HTTPS

This TCP probe queries a [Barracuda Spam Firewall](#) for various performance statistics.

The BASIC > Status page of the Administrators interface is retrieved using HTTPS.

Parameters

User - the administrator name for the firewall.

Password - the administrator password for the firewall.

Port - the Web Interface HTTP Port for the firewall as set on the BASIC > Administration page.

Thresholds

Set thresholds as follows:

In/Out Queue Size - this value should be less than 100. An In or Out Queue value that consistently exceeds 100 for more than 30 minutes might indicate a problem that needs attention. Sometimes the returned value rises temporarily and goes back down after 10 or 15 minutes.

- For the Inbound Queue, this is normal behavior, but can also be the result of an orchestrated attack. Barracuda attempts to read as many messages as it can, which results in a slower processing rate, which in turn increases the number of messages in the queue.
- For the Outbound Queue, an increase usually indicates that the destination server is unavailable or the local DNS is not functioning properly.

Recommended Settings

- **Warning** - a value exceeding 100 for more than 15 minutes.
- **Alarm** - a value exceeding 500 for more than 30 minutes.

Average Latency - the average time, in seconds, to receive, process, and deliver the last 30 messages. The value should be below 50 seconds. Latency that consistently exceeds 50 seconds for more than 30 minutes might indicate a problem that needs attention. Sometimes the value rises temporarily and goes back down after 10 or 15 minutes. This is normal behavior.

Recommended Settings

- **Warning** - a value exceeding 50 seconds for more than 15 minutes.
- **Alarm** - a value exceeding 150 seconds for more than 30 minutes.

Last Message - the time, in minutes, since the last message was received. For a busy machine, this value should be less than 5 minutes. Values consistently exceed 20 minutes for more than 30 minutes might indicate a problem that needs attention. Sometimes the value rises temporarily and goes back down after 2 or 3 minutes. This is normal behavior.

Recommended Settings

- **Warning** - a value exceeding 15 minutes.
- **Alarm** - a value exceeding 30 minutes.

CPU 1/CPU 2 Fan Speed - should be between 3,000 and 5,000 (RPM).

Recommended Settings

- **Warning** - a value for either CPU fan that is below 2500.
- **Alarm** - a value for either CPU fan that is below 500.

Firmware Storage - the typical value is between 60% and 80%. A value above 80% usually means that a debug file needs to be deleted. This can be done on a non-emergency basis.

Recommended Settings

- **Warning** - a value above 80%.
- **Alarm** - a value above 90%.

Mail/Log Storage - the typical value is between 1% and 70%.

Recommended Settings

- **Warning** - a value above 70%.
- **Alarm** - a value above 80%.

System Load - the system's load (in percentage). During normal operation, this value can vary wildly, anywhere between 1 and 100%. A value that remains at 100% for more than 2 hours might indicate a problem that needs attention. Sometimes, this value rises temporarily and goes back down after 2 or 3 minutes. This is normal behavior.

Recommended Settings

- **Warning** - a value above 80% for more than 1 hour.
- **Alarm** - a value above 90% for more than 3 hours.

CPU Temperature - should be between 40 and 70 degrees C.

Recommended Settings

- **Warning** - a value above 70 degrees C for more than 30 minutes.
- **Alarm** - a value above 80 degrees C for more than 1 hour.

Filename: `com.dartware.tcp.barracuda.https.txt`
Version: 3.1

Big Brother Probe

This probe allows you to use Intermapper as a Big Brother BBDISPLAY to collect information sent by Big Brother clients.

Parameter

Purple Time - sets the number of minutes to wait without a report before indicating a problem. In a Big Brother server, this is thirty minutes; Big Brother shows a device as purple if it goes this long without a report from the device. This probe shows it as DOWN.

Filename: `com.dartware.bigbrother`
Version: 1.7

BlitzWatch

This probe monitors the performance of a BlitzMail server.

BlitzMail is a TCP/IP-based client-server electronic mail system developed at Dartmouth College. In the BlitzMail system, all mail and mail preferences are stored on one or more BlitzMail servers, providing access to email from anywhere.

This probe provides a simple view into the current state of a single BlitzMail server, showing simultaneous user count, CPU utilization, and disk transfer statistics.

Parameter

None

Filename: `com.dartware.blitzwatch`

Version: 1.5

Citrix Server

This probe connects to a Citrix server, using default port 1494. It checks for the presence of the ICA string in the response, which indicates that the Citrix server is running.

This probe sets the device to Alarm if the following occurs:

- a disconnect is received unexpectedly.
- doesn't receive a response within 30 seconds after connecting
- the response doesn't contain the string "ICA"

Parameters

None

Filename: `com.dartware.tcp.citrix.txt`

Version: 1.2

Dartware > DataCenter > IMAuth

This TCP probe queries an [Intermapper DataCenter](#) server to verify that IMAuth is configured and running on that server. This only works with Intermapper DataCenter 5.1 or higher.

Parameters

User - the DataCenter admin user's name.

Password - the DataCenter admin user's password.

Port - the port the DataCenter server listens on.

Filename: `com.dartware.tcp.imauth`

Version: 0.4

Dartware > DataCenter > IMDatabase

This TCP probe queries an [Intermapper DataCenter](#) server to verify that IMDatabase is configured and running on that server. This only works when run against Intermapper DataCenter 5.1 or higher.

Parameters

User - the DataCenter admin user's name.

Password - the DataCenter admin user's password.

Port - the port the DataCenter server listens on.

Filename: `com.dartware.tcp.imdatabase`

Version: `0.4`

DND Protocol

The protocol used to lookup directory entries and validation information in a DND server. The DND is a centralized authentication/directory service developed at Dartmouth College. The default TCP port number for DND connections is port 902.

Parameters

Name - the DND admin user's name.

Port - the port the DND server listens on.

FileMaker Pro

This probe attempts to connect to a Filemaker Pro database server. By default, the port is 5003. If a successful connection is made, the device status is set to Okay.

Parameters

None

Filename: `com.dartware.tcp.filemaker`

Version: `1.7`

FirstClass Server

This probe connects to a FirstClass mail server. It sends two carriage returns and expects to receive a banner. The default contains FirstClass System. By default, it listens on port 510.

Parameter

banner - the banner text received from the FirstClass server.

Filename: `com.dartware.tcp.firstclass`

Version: `1.7`

KeyServer

This probe tests the operation of Sassafras KeyServer using TCP/IP. [KeyServer](#) is a software license management tool for Microsoft Windows, macOS, and thin-client based computers.

The probe sends a proprietary status request to the KeyServer. For more information, see [Sassafras Software](#). By default, the server accepts UDP requests on port 19283.

NOTE:

KeyServer is a registered trademark of Sassafras software.

Parameters

None

Filename: `com.dartware.keyserver`

Version: `1.7`

Lotus Notes

Lotus Notes uses Port 1352 for its Remote Procedure Call and Notes Replication.

This probe establishes a connection to the indicated port, which should be a Lotus Notes server. If the connection is successful, the device status is set to OK; otherwise, its status is DOWN.

Parameters

None

Filename: `com.dartware.tcp.lotusnotes`
Version: 1.5

MeetingMaker

The MeetingMaker server listens on port 649. This probe attempts to connect and exits with OKAY status if it succeeds.

Parameters

None

Filename: `com.dartware.tcp.meetingmaker`
Version: 1.5

Microsoft > DHCP Lease Check

This probe monitors the count of free DHCP leases on a Microsoft DHCP server. If the count goes below the specified thresholds, the device enters ALARM or WARNING state.

The check is specific to a scope.

Parameters

Scope - the DHCP scope to check (for example, 192.168.1.0).

Free Lease Warning - the number of remaining leases at which the device enters WARNING state.

Free Lease Alarm - the number of free leases remaining at which the device enters ALARM state.

Free Lease Critical - the number of free leases remaining at which the device enters CRITICAL state.

View the DHCP scope table - click to view a list of available scopes, along with information about in-use lease, free lease, and pending offers.

Filename: `com.dartware.snmp.dhcpcheck.txt`
Version: 0.4

Microsoft > NT Services

This probe monitors the state of one or more services on a Microsoft Windows-based machine, Microsoft Windows NT 4.0 and newer. Intermapper uses the Service Control Manager (SCM) to retrieve the information about the specified services. This probe works only if the Intermapper server is running on a Windows computer.

Parameters

Services to Monitor - the list of services to be monitored. In the status window, services with green icons are currently running; those with red icons are stopped.

Intermapper monitors services whose boxes are checked. For a single machine, choose from all the services on the machine. For multiple machines, choose from those services common to all of the machines.

Username - the name of an administrative user on the machine being probed. Intermapper uses this username to log into the target machine to query the Service Control Manager.

Password - the password for the specified user.

If Username and Password are blank, the user credentials under which Intermapper is running will be used.

NOTE: For this probe to operate, Intermapper must be running as an administrative user or you must supply an administrator username and password for in the NT Services panel in Server Settings. This allows Intermapper to elevate its privileges temporarily.

Filename: `com.dartware.ntsvcs.std`
Version: 1.9

Microsoft > SQL Server Query

This probe establishes an ADO (ActiveX Data Object) connection to a Microsoft SQL Server running on the target host. It issues the specified query and displays the returned fields. If no records are returned, the device status is set to Critical.

Parameters

Query - the SQL query to send. It should be enclosed in double-quotes. Using the TOP keyword in your query improve the response to the query. You can specify specific columns in your query and include a WHERE or an ORDER BY clause.

Rows and **Columns** - the number of columns and the number of rows of records in the query you want to view.

Instance - the SQL server instance on the target host the query is sent to. To query the default server instance, leave this field blank.

Database - the database on the target instance to query.

User - can be an SQL Server user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank to use integrated authentication. The specified user must have dbreader privileges to the database.

Timeout (sec) - allows you to override the device's specified timeout.

Intermapper invokes the sql_query.vbs script, included with this probe.

Filename: `com.dartware.cmd.sql_query.txt`
Version: 1.4

Nagios NRPE

The NRPE (Nagios Remote Plugin Executor) protocol defines a way to execute Nagios plugins on remote machines. After you install a Nagios NRPE daemon and one or more Nagios plugins on a remote machine, Intermapper does the following to retrieve the status of that machine:

- Establishes an encrypted SSL/TLS connection to the remote NRPE daemon.
- Requests that a specific Nagios plugin be executed.
- Receives the response from the plugin.
- Parses the response and display the state of that machine.]

The NRPE daemon uses a configuration file (nrpe.cfg) that has command definition entries in the following format:

```
command[check_swap]=/usr/local/nagios/libexec/check_
swap -w 20% -c 10%
```

When the NRPE daemon receives a request to run the check_swap plugin, it issues the command above.

Parameters

Nagios Plugin - tells which plugin to execute. It must match one of the command definitions in the nrpe.cfg file (the text within square brackets [...]). To test the connection from Intermapper to the NRPE daemon, set **Nagios Plugin** to **_NRPE_CHECK**.

For information on installing an NRPE daemon, see the [NRPE Documentation](http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf) (at <http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf>), especially the section on Remote Host Configuration. Nagios and the Nagios logo are registered trademarks of Ethan Galstad. For more information, see <http://www.nagios.org>.

Filename: com.dartware.tcp.nrpe.txt
Version: 1.2

Miscellaneous

Demo Probe

Builds a demo map and generates random data for the traffic on all its links. All data is chartable, and can be used to demonstrate strip charts or data collection.

This probe also toggles the device state between UP/OK and Down when you manually reprobe the device. This makes it easy to see what happens when a device goes down, especially for manual dependencies.

For simple maps, the parameters can be set to 0. To create complicated, heavily-interconnected demonstration maps, try setting the Link Count and Loop % parameters to 10 and 50, respectively.

Parameters

Link Count - sets the number of interfaces to create when adding the device to the map.

Loop % - sets the percentage of links that connect themselves to subnets already present on the map.

Filename: `com.dartware.demo`
Version: `1.7`

Legacy > Basic OID (v2c)

This is a legacy probe, provided for compatibility with Intermapper Traditional and older versions of Intermapper (< 4.4). Use the Basic OID probe, setting the SNMP version to SNMP v2.

This probe allows you to monitor a single, user-defined MIB variable. It uses SNMPv2c.

Parameters

Object Name - (optional) the name of the value that you want to monitor. It is displayed in the Status window and in a chart legend.

Object ID - the object identifier (OID) of the value that you want to monitor. To retrieve the value of a MIB variable that is not in a table, the OID must end with .0 (for example, 1.3.6.1.2.1.1.1.0).

Filename: `com.dartware.snmpv2c.basic`
Version: `1.6`

Legacy > Cisco (v2c)

This is a legacy probe, provided for compatibility with Intermapper Traditional and older versions of Intermapper (< 4.4). Use the Cisco - Process and Memory Pool probe instead and set the probe's SNMP version to SNMP v2 in the Probe Info window.

This probe monitors the CPU and Memory utilization of a Cisco router using SNMPv2c.

Parameters

CPU Busy - Alarm - specifies the Alarm threshold for CPU utilization as a percentage. If the average CPU usage over a 1 minute interval exceeds this threshold, the device is set to Alarm state.

CPU Busy - Warning - specifies the Warning threshold for CPU utilization. If the average CPU usage over a 1 minute interval exceeds this threshold, the device is set to Warning state.

Low Memory - Alarm - specifies the Alarm threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device is set to Alarm state.

Low Memory - Warning - specifies the Warning threshold for the amount of free memory remaining (in bytes). If the free memory drops below this threshold, the device is set to Warning state.

Filename: `com.dartware.snmpv2c.cisco`
Version: `1.11`

Legacy > SNMP v2c

This is a legacy probe, provided for compatibility with Intermapper Traditional and older versions of Intermapper (< 4.4). Use the SNMP MIB-II probe, setting the SNMP version to SNMP v2.

The SNMP v2c probe retrieves MIB-II information from the device. This includes sysLocation, sysContact, and sysUptime from the system group, and traffic (bytes/second, packets/second, and errors/minute) for each interface.

It uses the 64-bit counters for interface traffic statistics. This provides accurate information (without rollover) on very high speed links.

Parameters

None

Filename: `com.dartware.snmpv2c`
Version: `1.7`

Nagios > Nagios Plugin

This probe allows you to specify a Nagios plugin. Intermapper invokes the plugin and uses the exit value to set the condition of the device. It uses the performance data returned by the plugin to create a nice display of chartable data.

Parameter

Plugin - the same command line (including arguments) you use to manually test the plugin.

NOTE:

`${ADDRESS}` is replaced with the device's IP address. `${PORT}` is replaced by the port specified for the probe.

This probe expects the plugin to be located in the InterMapper Settings/Tools directory.

Nagios and the Nagios logo are registered trademarks of Ethan Galstad. For more information, see <http://www.nagios.org>

Parameter

Plugin - the Nagios command string. You can use ``${ADDRESS}` and ``${PORT}`.

Filename: `com.dartware.nagios.template`

Version: 1.8

Non-Polling Probe

This probe does not invoke any action. It can be used as a placeholder for a device; it does not count against the InterMapper device count.

Filename: `com.dartware.nonpolling`

Version: 1.5

Prototype SNMP Probe

This probe demonstrates an InterMapper SNMP probe (how to retrieve SNMP values from a device by specifying their OIDs, how to display those values in the device's Status window, and provides thresholds that set the device into Alarm or Warning state). Many of these features are described in Creating Your Own Probes, in the Developer Guide. If you have questions about this probe, [contact Fortra](#).

This probe is not very useful for production work. However, it provides examples of techniques available in custom SNMP probes.

In the example, the device goes into Alarm or Warning state if it has been rebooted recently (controlled by the RebootAlarm and RebootWarn parameters which are two and three minutes, by default) or if there are not as many interfaces in the ifTable as specified (in the ExpectedInterfaces parameter).

This probe also demonstrates the following:

- **CALCULATION variables** - converts centi-seconds (hundredths of a second) into seconds.
- **Status window formatting** - in the `<snmp-device-display>` section.
- IMML allows you to create a link to a URL, using the `\U2=http://xxxx\` notation shown in the `<snmp-device-display>` section.

Parameters

RebootAlarm - sets the device to Alarm if the sysUptime is less than the specified value in minutes.

RebootWarn - sets the device to Warning if the sysUptime is less than the specified value in minutes.

ExpectedInterfaces - sets the device to Warning if the ifNumber is greater than or equal to this value.

Filename: `com.dartware.snmp.prototype.txt`

Version: 1.4

TCP Check

This probe generates an alarm if the count of TCP connections exceeds a specified number. It can be used to detect people telnetting into a system that should not have connections, such as a router that might be attacked from outside your network.

It retrieves the device's tcpCurrEstab variable and compares it. If the number of established TCP connections exceeds the value specified in Allowed TCP Connections, the device is set to the Alarm state.

Parameter

Allowed TCP Connections - the maximum number of TCP connections allowed.

Filename: `com.dartware.snmp.tcpcheck`
Version: 1.6

Wireless

Alvarion > Alvarion B-14 & B-28 (BU)

This probe monitors an [Alvarion](#) B-14 or B-28 base unit (BU). It retrieves and displays the radio band, operating frequency, and slave association. It will go into an alarm when no slave is associated, and when the operating frequency doesn't match the configured frequency. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, we recommend using the "Display unnumbered interfaces" behavior.)

Parameters

None

Filename: `com.dartware.wrls.alvarion.b14.master.txt`
Version: 0.5

Alvarion > Alvarion B-14 & B-28 (RB)

This probe monitors an [Alvarion](#) B-14 or B-28 remote bridge (RB) unit. It retrieves and displays the radio band, operating frequency, average received signal to noise ratio, and the MAC address of the associated base unit (BU). It will go into alarm or warning states based on user-defined parameters for a low signal to noise ratio or high traffic on a specified interface.

Parameters

Avg Receive SNR too low alarm, Avg Receive SNR low warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

High Traffic Interface Number - the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarion.b14.slave.txt`
Version: 0.5

Alvarion > BreezeACCESS (AU)

This probe monitors a BreezeCom or [Alvarion](#) BreezeACCESS 2.4 Ghz or 900 MHz access unit (AU). It retrieves and displays the operating radio band of the unit, and the number of client associations since the last reset. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, Fortra recommends using the "Display unnumbered interfaces" behavior.)

Parameters

Retransmitted Fragments too high alarm, Retransmitted Fragments high warning,

Dropped Frames too high alarm, Dropped Frames high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

High Traffic Interface Number - the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarionbaau.txt`
Version: 1.7

Alvarion > BreezeACCESS (SU)

This probe monitors a BreezeCom or [Alvarion](#) BreezeACCESS 2.4 Ghz or 900 MHz subscriber unit (SU). It retrieves and displays the radio band, average power (in dBm or RSSI), and the MAC address of the associated AU. For a 900 MHz unit, it will also display the radio frequency. The probe will go into alarm or warning states based on user-definable parameters for low signal power or high incoming traffic on a specified interface.

Parameters

Average Power too low alarm, Average Power low warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

High Traffic Interface Number - the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarionbasu.txt`
Version: 1.7

Alvarion > BreezeACCESS LB

This probe is meant to probe an [Alvarion](#) BreezeACCESS LB radio, acting as either AP or an SU. It retrieves and displays a number traffic and radio related variables. It will go into alarm or warning states based on user-defined parameters.

Parameters

Expected Operating Frequency - the frequency.

SNR too low alarm, SNR low warning - the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.alvarionbalb.txt`
Version: 0.16

Alvarion > BreezeACCESS VL (AU)

This probe monitors an [Alvarion](#) BreezeACCESS VL access unit (AU). It retrieves and displays the radio band, operating frequency, and number of clients. It will go into an alarm or warning based on user defined parameters for high and low numbers of clients (SUs), and when the operating frequency doesn't match the configured frequency. Traffic information is available for the ethernet and radio interfaces. (To show the ethernet interface, we recommend using the "Display unnumbered interfaces" behavior.)

Parameters

Current SU Count too high alarm, Current SU Count high warning,

Current SU Count too low alarm, Current SU Count low warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.alvarionbavlaui.txt`

Version: 1.7

Alvarion > BreezeACCESS VL (SU)

This probe monitors an [Alvarion](#) BreezeACCESS VL subscriber unit (SU). It retrieves and displays the radio band, operating frequency, average received signal to noise ratio, and the MAC address of the associated access unit (AU). It will go into alarm or warning states based on user-defined parameters for a low signal to noise ratio or high traffic on a specified interface.

Parameters

Avg Receive SNR too low alarm, Avg Receive SNR low warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

High Traffic Interface Number - the number of the interface for which you want to monitor traffic.

Filename: `com.dartware.wrls.alvarionbavlsu.txt`

Version: 1.7

Atmel > Atmel AT76C510

This probe monitors devices based on the Atmel AT76C510 chip. Please refer to your device's technical specification to find out the chip type.

Sample devices based on AT76C510 chip are as follows: Belkin F5D6130, D-Link DWL 900AP (rev. 1), Netgear ME102, and Linksys WAP11 (ver < 2).

It retrieves and displays information from the AT76C510 MIB using SNMP v1. Depending on the bridge's operating mode this probe will display different information.

If device is operating as a wireless client or a wireless repeater, the probe will display information about the connection to the parent access point (ESSID, SSID, channel, RSSI, link quality).

If the device is operating as a wireless bridge (either point-to-point or point-to-multipoint), the probe will display the list of authorized MAC addresses.

If the operating mode is a wireless repeater or access point, the probe will monitor the number of clients and list each one with its RSSI/link quality.

It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address, firmware revision).

This probe may not return complete information to SNMPv1 clients using the community string "public". To fully utilize this probe, you must set the community string to the one with the correct permissions.

Parameters

Number of clients warning, Maximum number of clients,

Too many failed packets/sec, Too many retry packets/sec

- the thresholds for Warning and Alarm.

Link to Device Management Tool - the URL to the web manager for this device.

Filename: `com.dartware.wrls.AT76C510.txt`

Version: 1.5

Basic > IEEE 802.11

This probe monitors 802.11 counters from a wireless device that supports the IEEE802dot11-MIB.

Parameters

Interface index - the interface for the wireless device.

Tx Failed frames/sec, Tx Retry frames/sec, Rx FCS err fragments/sec, and ACK failures/sec - the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.80211counters.txt`

Version: 0.2

Basic > SNMP for Wireless

(Previously titled "Wireless - Generic (SNMP MIB-II)")

This is a general probe for monitoring wireless gear for which there is no specific Intermapper probe, but that supports SNMP MIB-2. This probe will gather general traffic information, network connections, etc. It also adds an alarm when traffic on a user-selected interface reaches specified levels.

Parameters

Wireless interface number - the interface number of the device.

High Traffic Bytes alarm, High Traffic Bytes warning - the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.generic.txt`

Version: 1.4

Canopy > Canopy (AP)

This probe monitors a Canopy wireless access point (AP), including basic information, traffic information, and the number of clients associated. It places the device into alarm or warning when the number of clients exceeds the user-defined thresholds.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

Too many clients alarm, Many clients warning,

Too few clients alarm, Few clients warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.canopyap.txt`

Version: 1.9

Canopy > Canopy (SM)

This probe monitors a Canopy wireless service module (SM).

This probe retrieves and displays a number of variables. It will place the device in alarm or warning states based on user-defined thresholds for high

re-registration count, low RSSI, high Jitter, long Round Trip delay, and low Power Level, and give an alarm if the unit is not registered.

Note that the 2x jitter thresholds will only be used when the SM is operating in 2x/2x mode.

To disable any of the thresholds, set their values to 0.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

RSSI too low alarm, RSSI low warning,

Jitter too high alarm, Jitter high warning,

Jitter (2x) too high alarm, Jitter (2x) high warning,

Round Trip too long alarm, Round Trip long warning,

Power Level too low alarm, Power Level low warning,

Session count alarm, Session count warning,

Reg count alarm, Reg count warning,

Re-reg count alarm, Re-reg count warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.canopysm.builtin.txt`

Version: 1.6

Canopy > Canopy Backhaul (45 Mbps/FW 5830)

This probe monitors a Canopy 45Mbps Backhaul radio with firmware 5830 or older, acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation and speed mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning

states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning,

SNR too low alarm, SNR low warning

- the thresholds for **Warning** and **Alarm**.

Filename: `com.dartware.wr1s.canopy.backhaul45old.txt`

Version: 1.7

Canopy > Canopy Backhaul (60 Mbps/FW 5840)

This probe monitors a Canopy 60Mbps Backhaul radio with firmware 5840 or later, acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation and speed mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.canopy.backhaul45.txt`

Version: 1.9

Canopy > Canopy Backhaul (Master)

This probe monitors a Canopy wireless backhaul master unit, including wireless network and link information. It will give a warning if no slave is associated.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

None

Filename: `com.dartware.wrls.canopybhm.txt`

Version: 1.4

Canopy > Canopy Backhaul (Slave)

This probe monitors a Canopy wireless backhaul slave unit. It retrieves and displays a number of variables. It will place the device in alarm or warning states based on user-defined thresholds for low RSSI, high Jitter, long Round Trip delay, and low Power Level, and give an alarm if the unit is not registered.

The default poll interval for this probe is 5 minutes. The default poll interval is an automatic safeguard; polling more frequently has been shown to adversely affect the device.

Parameters

RSSI too low alarm, RSSI low warning,

Jitter too high alarm, Jitter high warning,

Round Trip too long alarm, Round Trip long warning,

Power Level too low alarm, Power Level low warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.canopybhs.txt`
Version: 1.4

Canopy > Canopy CMM-Micro

This probe monitors a Canopy CMM-Micro. The device only supports basic SNMP v2c MIBs, no device-specific enterprise information is available.

Parameters

None

Filename: `com.dartware.wrls.canopy.cmmmicro.txt`
Version: 0.5

CB3 > CB3 Bridge

This TCP probe queries a CB3 wireless bridge via a HTTP GET request.

Parameters

User - the username to use when logging in.

Password - the password for the User specified above.

Port - the CB3's web interface HTTP port.

Quality Warning, Quality Alarm - the thresholds (in percent) for Warning and Alarm.

Filename: `com.dartware.wrls.cb3.old.txt`
Version: 1.2

CB3 > CB3 Deluxe Bridge

This TCP probe queries a CB3 Deluxe wireless bridge via a HTTP GET request.

Parameters

User - the username to use when logging in.

Password - the password for the User specified above.

Port - the CB3's web interface HTTP port.

Quality Warning - the value (as a percentage) that the communications quality must fall below for the device to go into the WARN state.

Quality Alarm - the value (as a percentage) that the communications quality must fall below for the device to go into the ALARM state.

Filename: `com.dartware.wrls.cb3.txt`

Version: 1.5

Inscape Data > AirEther AB54 Series AP (AP Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Access Point Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Port - the Web interface's HTTP port.

RSSI Warning <, RSSI Alarm <,

Too Many Stations Warning >, Too Many Stations Alarm >,

Too Few Stations Warning <, Too Few Stations Alarm <

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.inscape.ab54.ap.txt`

Version: 1.1

Inscape Data > AirEther AB54 Series AP (Bridge Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Point to Point or Point to Multipoint Bridge Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Port - the Web interface's HTTP port.

RSSI Warning <, RSSI Alarm < - the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.inscape.ab54.bridge.txt`
Version: 1.1

Inscape Data > AirEther AB54 Series AP (Client Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, and AB54E Pro Multifunctional AP in Client Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Signal Strength Warning - the warning threshold for low signal strength %.

Signal Strength Alarm - the alarm threshold for low signal strength %.

Link Quality Warning - the warning threshold for low link quality %.

Link Quality Alarm - the alarm threshold for low link quality %.

Expected BSSID - the expected BSSID. This value will be ignored if blank.

Port - the Web interface's HTTP port.

Filename: `com.dartware.wrls.inscape.ab54.client.txt`
Version: 1.1

Inscape Data > AirEther AB54 Series AP (Repeater Mode)

This probe monitors [Inscape Data](#)'s AB54, AB54E, AB54E Pro Multifunctional AP in Repeater Mode.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

RSSI Warning <, RSSI Alarm <,

Too Many Stations Warning >, Too Many Stations Alarm >,

Too Few Stations Warning <, Too Few Stations Alarm <

- the thresholds for Warning and Alarm.

Port - the Web interface's HTTP port.

Filename: `com.dartware.wrls.inscape.ab54.repeater.txt`
Version: 1.1

Inscape Data > AirEther CB54 Series Client

This probe monitors [Inscape Data](#)'s CB54, CB54E, and CB5418 wireless client device.

Parameters

User - the name of the administrator.

Password - the password for the administrator.

Signal Strength Warning - the warning threshold for low signal strength %.

Signal Strength Alarm - the alarm threshold for low signal strength %.

Link Quality Warning - the warning threshold for low link quality %.

Link Quality Alarm - the alarm threshold for low link quality %.

Expected BSSID - the expected BSSID. This value will be ignored if blank.

Port - the Web interface's HTTP port.

Filename: `com.dartware.wrls.inscape.cb54.client.txt`
Version: 1.1

MikroTik > MT Radio Uplink

This probe monitors a MikroTik router and its radio uplink interface. For the AP it monitors general SNMP interface and traffic information, as well as device utilization (CPU, Disk, Memory loads). For the radio uplink interface it monitors name & ssid, frequency, tx/rx rates, strength, and BSSID.

You must manually specify the OID index of the wireless uplink interface. Using Telnet: 1) Login, 2) Enter "interface wireless print oid", 3) The interface index is the last digit of the OIDs, 4) Type this number into the "Wireless Interface" field below.

This probe raises an alarm in the following situations:

- **High Use** - for CPU, Disk, or Memory loads exceeds 90% (default setting of parameter).

This probe is part of the Intermapper Wireless Probe Bundle, and requires Intermapper 4.2.1 or later.

Parameters

High Use Threshold - Percentage of use to trigger alarm

Wireless Interface - OID of the wireless uplink interface

Filename: `com.dartware.wrls.mt-1radio.txt`

Version: 1.14

MikroTik > MT Routerboard

This probe monitors a MikroTik Routerboard (wireless access point). It monitors the general SNMP interface and traffic information, device utilization (CPU Load, Disk use, and Memory use in percent), and the device's "health" (internal voltages and temperatures).

This probe will raise an alarm in the following situations:

- **High Use** - CPU Load, Disk use, or Memory use exceeding 90%.
- **Unsafe Temperatures** - Safe ranges of -20°C to 50°C for Board & Sensor temps., -20°C to 70°C for CPU temp.
- **Unsafe Voltages** - Safe deviation of +/- 5% for 12V & 5V, +/- 3% for 3.3V and Core Voltage (either 1.8V or 2.0V).

This probe is part of the Intermapper Wireless Probe Bundle, and requires Intermapper 4.2.1 or later.

Parameters

High Use Threshold - the percentage of use to trigger alarm

High and Low Temperature thresholds - the temperature values (C) to trigger alarms, or keep the default values.

High & Low voltage thresholds - the voltage values to trigger alarms, or keep the default values.

Filename: `com.dartware.wrls.mt-routerboard.txt`
Version: 1.6

MikroTik > MT Software Only

This probe monitors any device that uses MikroTik software (a wireless access point), but does not monitor its wireless interfaces. It monitors general SNMP interface and traffic information and device utilization: CPU Load, Disk use, and Memory use (in percent).

This probe raises an alarm in the following situations:

- **High Use** - CPU Load, Disk use, or Memory use exceeds 90%.

This probe is part of the Intermapper Wireless Probe Bundle, and requires Intermapper 4.2.1 or later.

Parameter

High Use Threshold - the percentage of use to trigger alarm.

Filename: `com.dartware.wrls.mt-0radio.txt`
Version: 1.5

MikroTik > WDS Bridge

This probe monitors a MikroTik router in WDS Bridge mode. The probe monitors the Ethernet traffic information, as well as device utilization (CPU, Disk, Memory loads). The probe also displays the signal strength and tx/rx rates of the wireless link.

You must specify both the MAC address of the other AP, as well as the ifIndex of the wireless interface. The MAC address must be entered as six decimal numbers separated by "."

To determine the ifIndex of the wireless interface, Telnet to the radio, then:

1. Log into the router
2. Enter `interface wireless print oid`
3. The interface index is the last digit of the OIDs
4. Type this number into the Wireless Interface field below.

This probe will raise an alarm if the CPU, Disk, or Memory loads exceeds the High Use Threshold.

Parameters

Associated AP MAC Adrs - the MAC address of Access Point to which the router is connected.

Wireless Interface - the index of the interface

High Use Threshold (%) - the usage threshold to trigger Alarm.

Filename: `com.dartware.wrls.mikrotik-wds.txt`

Version: 1.3

Motorola > PTP 400 Series Bridge

This probe monitors a Motorola PTP400 point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- the modes and thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.motorola.ptp400.txt`

Version: 1.2

Motorola > PTP 600 Series Bridge

This probe monitors a Motorola PTP600 point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- the modes and thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.motorola.ptp600.txt`

Version: 0.8

Orthogon > Gemini

This probe monitors an Orthogon Systems Gemini point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, and link loss. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, and link loss.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrsl.orthogon.gemini.txt`

Version: 1.8

Orthogon > Spectra

This probe monitors an Orthogon Systems Spectra point-to-point (P2P) Wireless Ethernet Bridge acting as a master or slave.

It monitors and displays a variety of information, including mode and association, range, active channels, transmit and receive modulation mode, current and maximum transmit power, receive power, vector error, link loss, and signal-to-noise ratio. It will go into alarm and warning states based on user-specified levels for the modulation/speed mode, received power, vector error, link loss, and signal-to-noise ratio.

Parameters

Tx Modulation Mode Alarm, Tx Modulation Mode Warning,

Rx Modulation Mode Alarm, Rx Modulation Mode Warning,

Rx Power too low alarm, Rx Power low warning,

Vector Error too high alarm, Vector Error high warning,

Link Loss too high alarm, Link Loss high warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.orthogon.spectra.txt`
Version: 0.8

Other > HTTP

This probe tests an HTTP server by downloading a specific web page and scanning it for a specific string of HTML.

Parameters

URL Path - the full path of the desired file on the web server (for example, `/index.html`). The first character must be a `'/'`.

String to verify - a string to verify in the server's response. For example, if you are retrieving a web page, you might search for `<HTML>` or `<P>` to verify that the data is HTML, or look for a unique string that is present only in the specified page.

User ID - the user name you would type into the web browser's authentication dialog. It is blank by default. Set this parameter to test a web page that requires authentication.

Password - the password you would type into the web browser's authentication dialog. It is blank by default. Set this parameter to test a web page that requires authentication.

Filename: `com.dartware.wrls.http.txt`
Version: 1.5

Proxim > Proxim AP-600

This probe monitors [Proxim](#) AP-600 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set *Show station statistics* to **true**.

NOTE:

Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- the thresholds for Warning and Alarm.

Show wireless if settings - specifies whether to show wireless interface settings.

Show security settings - specifies whether to show security settings.

Show station statistics - specifies whether to show statistics.

Filename: `com.dartware.wrls.proximap600.txt`
Version: 1.3

Proxim > Proxim AP-700

This probe monitors [Proxim](#) AP-700 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set *Show station statistics* to **true**.

NOTE:

Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- the thresholds for Warning and Alarm.

Show wireless if settings - specifies whether to show wireless interface settings.

Show security settings - specifies whether to show security settings.

Show station statistics - specifies whether to show statistics.

Filename: `com.dartware.wrls.proximap700.txt`

Version: 1.4

Proxim > Proxim AP-2000

This probe monitors [Proxim](#) AP-2000 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set *Show station statistics* to **true**.

NOTE:

Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- the thresholds for Warning and Alarm.

Show wireless if settings - specifies whether to show wireless interface settings.

Show security settings - specifies whether to show security settings.

Show station statistics - specifies whether to show statistics.

Filename: `com.dartware.wrls.proximap2000.txt`
Version: 1.4

Proxim > Proxim AP-4000

This probe monitors [Proxim](#) AP-4000 access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set *Show station statistics* to **true**.

NOTE: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

- the thresholds for Warning and Alarm.

Show wireless if settings - specifies whether to show wireless interface settings.

Show security settings - specifies whether to show security settings.

Show station statistics - specifies whether to show statistics.

Filename: `com.dartware.wrls.proximap4000.txt`
Version: 1.4

Proxim > Proxim LAN Access Point

This probe monitors [Proxim](#) LAN access points.

The probe displays the device's general settings, wireless interface RF parameters, security information, and wireless clients. To show the wireless client list, set *Show station statistics* to **true**.

NOTE: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many clients warning, Too many clients alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm,

Show wireless if settings[true,false], Show security settings[true,false]

- the thresholds for Warning and Alarm.

Show station statistics - specifies whether to show statistics for this device.

Filename: `com.dartware.wrls.proximap.txt`

Version: 1.4

Proxim > Tsunami GX

This probe monitors a Proxim Tsunami GX (GX 32 and GX 90).

This probe sets the device to **Alarm** if the status of either of the device's external inputs is in alarm. It also monitors the device's RFU status, IDU and RFU temperatures, RFU cable status, IDU fan status, IDU synthesizer status, RFU power status, RFU summary/minor relay status, AIS injection status, link status, and the number of errors/sec.

The temperature warning and alarm threshold are used only if the *Use custom temperature threshold* checkbox is selected.

Parameters

Use custom temperature threshold - sets your own temperature thresholds.

Temperature warning, Temperature alarm,

Errors/sec warning, Errors/sec alarm, Severe errors/sec alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.proxim4.txt`

Version: 0.4

Proxim > Tsunami MP.11 BSU

This probe monitors [Proxim](#) Tsunami MP.11 Base Station Unit (BSU). This probe can be used to monitor all MP.11 models, including 2411, 2454-R, 5054, and 5054-R.

NOTE:

Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Many subscribers warning, Too many subscribers alarm,

Signal dBm too low alarm, Signal dBm low warning,

Noise dBm too high alarm, Noise dBm high warning,

Send retries pct high warning, Send retries pct too high alarm,

Send failures pct high warning, Send failures pct too high alarm,

Receive retries pct high warning, Receive retries pct too high alarm,

Receive failures pct high warning, Receive failures pct too high alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm

- the thresholds for Warning and Alarm.

Show wireless if settings - shows interface settings.

Show SU statistics - shows Subscriber Unit statistics.

Filename: `com.dartware.wrls.proximtmpbsu.txt`

Version: 1.2

Proxim > Tsunami MP.11 SU

This probe monitors [Proxim](#) Tsunami MP.11 Subscriber Unit (SU/RSU).
This probe can be used to monitor all MP.11 models, including 2411, 2454-R, 5054, and 5054-R.

NOTE: Some of the alarms/warnings of this probe will not function unless the Proxim device is set to send traps to the Intermapper server.

Parameters

Signal dBm too low alarm, Signal dBm low warning,

Noise dBm too high alarm, Noise dBm high warning,

Send retries pct high warning, Send retries pct too high alarm,

Send failures pct high warning, Send failures pct too high alarm,

Receive retries pct high warning, Receive retries pct too high alarm,

Receive failures pct high warning, Receive failures pct too high alarm,

FCS errors/sec high warning, FCS errors/sec too high alarm,

Failures/sec high warning, Failures/sec too high alarm,

Retries/sec high warning, Retries/sec too high alarm

- the thresholds for Warning and Alarm.

Show wireless if settings - select to show interface settings.

Filename: `com.dartware.wrls.proximtmprsu.txt`

Version: 1.3

Redline > AN50

This probe is meant to probe a [Redline](#) AN50 point-to-point radio, acting as either a master or slave. It retrieves and displays a number of critical statistics for the radio, and gives alarms if it goes out of user-specified thresholds. The probe retrieves:

Average RF Rx signal strength, Average RF SNR, Signaling Burst Rate, Operating frequency, Radio Link Status and compares them to the thresholds below.

Parameters

Avg. Rx Signal strength too low alarm, Avg. Rx Signal strength low warning,

Avg. SNR too low alarm, Avg. SNR low warning,

Expected Uncoded Burst Rate, Expected Operating Frequency,

Active Links too high alarm, Active Links high warning,

Active Links too low alarm, Active Links low warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.redlinean50.txt`

Version: 1.3

smartBridges > airBridge

This probe monitors a [smartBridges](#) airBridge device. It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address).

NOTE: Install Intermapper on a machine where you don't plan to run smartBridges simpleMonitor. To run both Intermapper and smartBridges' simpleMonitor on the same machine, disable trap processing in Intermapper.

Parameters

RSSI % low warning, RSSI % too low alarm,

Too many failed packets/sec, Too many retry packets/sec

- the thresholds for Warning and Alarm.

Link to Device Management Tool - the URL for the device's web manager.

Filename: `com.dartware.wrls.airbridge.txt`
Version: 1.5

smartBridges > airClient Nexus

This probe monitors a [smartBridges](#) airClient Nexus device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm

Tx retries (%) high warning, Tx retries (%) too high alarm

Tx failed (%) high warning, Tx failed (%) too high alarm

Frame errors (%) high warning, Frame errors (%) too high alarm

ACK failures/min high warning, ACK failures/min too high alarm

Aborted frames/min high warning, Aborted frames/min too high alarm

RTS errors (%) high warning, RTS errors (%) too high alarm:

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airclientnexus.txt`
Version: 0.5

smartBridges > airClient Nexus PRO total

This probe monitors a [smartBridges](#) airClient Nexus PRO total device. It retrieves and displays general device information, remote device information,

wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm

Tx retries (%) high warning Tx retries (%) too high alarm

Tx failed (%) high warning, Tx failed (%) too high alarm

Frame errors (%) high warning, Frame errors (%) too high alarm

ACK failures/min high warning, ACK failures/min too high alarm

Aborted frames/min high warning, Aborted frames/min too high alarm

RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airclientnexuspro.txt`

Version: 0.5

smartBridges > airHaul2 Nexus PRO

This probe monitors a [smartBridges](#) airHaul2 Nexus PRO device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Radio to monitor - the radio interface to monitor.

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airhaul2nexuspro.txt`
Version: 0.5

smartBridges > airHaul Nexus

This probe monitors a [smartBridges](#) airHaul Nexus device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airhaulnexus.txt`
Version: 0.5

smartBridges > airHaul Nexus PRO total

This probe monitors a [smartBridges](#) airHaul Nexus PRO total device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airhaulnexuspro.txt`

Version: 0.5

smartBridges > airPoint

This probe monitors a [smartBridges](#) airPoint device. It retrieves and displays information from the AT76C510 MIB using SNMP v1. Depending on the bridge's operating mode this probe will display different information.

If device is operating as a wireless client or a wireless repeater, the probe will display information about the connection to the parent access point (ESSID, SSID, channel, RSSI, link quality).

If the device is operating as a wireless bridge (either point-to-point or point-to-multipoint), the probe will display the list of authorized MAC addresses.

If the operating mode is a wireless repeater or access point, the probe will monitor the number of clients and list each one with its RSSI/link quality.

It retrieves and displays a number of traffic (bytes received/transmitted) and physical variables (name, MAC address, firmware revision).

This probe may not return complete information to SNMPv1 clients using the community string "public". To fully utilize this probe, you must set the community string to the one with the correct permissions.

NOTE: Install Intermapper on a machine where you don't plan to run smartBridges simpleMonitor. To run both Intermapper and smartBridges' simpleMonitor on the same machine, disable trap processing in Intermapper.

Parameters

Number of clients warning, Maximum number of clients,

Too many failed packets/sec, Too many retry packets/sec

- the thresholds for Warning and Alarm.

Link to Device Management Tool - the URL to the web manager for this device.

Filename: `com.dartware.wrls.airpoint.txt`

Version: 1.5

smartBridges > airPoint2 Nexus PRO

This probe monitors a [smartBridges](#) airPoint2 Nexus PRO device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Radio to monitor - the radio interface to monitor.

Many clients warning, Too many clients alarm,

Many WDS clients warning, Too many WDS clients alarm,

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm,

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airpoint2nexuspro.txt`

Version: 0.5

smartBridges > airPoint Nexus

This probe monitors a [smartBridges](#) airPoint Nexus device. It retrieves and displays general device information, remote device information,

wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Many clients warning, Too many clients alarm,

Many WDS clients warning, Too many WDS clients alarm,

RSSI (dBm) low warning, RSSI (dBm) too low alarm,

Tx retries (%) high warning, Tx retries (%) too high alarm,

Tx failed (%) high warning, Tx failed (%) too high alarm,

Frame errors (%) high warning, Frame errors (%) too high alarm,

ACK failures/min high warning, ACK failures/min too high alarm,

Aborted frames/min high warning, Aborted frames/min too high alarm,

RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airpointnexus.txt`

Version: 0.5

smartBridges > airPoint Nexus PRO total

This probe monitors a [smartBridges](#) airPoint Nexus PRO total device. It retrieves and displays general device information, remote device information, wireless statistics information and bridge information (when the device is operating as a bridge).

Parameters

Many clients warning, Too many clients alarm,

Many WDS clients warning, Too many WDS clients alarm,
RSSI (dBm) low warning, RSSI (dBm) too low alarm,
Tx retries (%) high warning, Tx retries (%) too high alarm,
Tx failed (%) high warning, Tx failed (%) too high alarm,
Frame errors (%) high warning, Frame errors (%) too high alarm,
ACK failures/min high warning, ACK failures/min too high alarm,
Aborted frames/min high warning, Aborted frames/min too high alarm,
RTS errors (%) high warning, RTS errors (%) too high alarm

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.airpointnexuspro.txt`
Version: 0.5

Trango > Trango M900S (AP)

This probe monitors a [Trango](#) M900S access point (AP). It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected antenna mode, and expected channel. (This probe calculates counters without using `sysUpTime`, which isn't available. MIB-2 traffic and interface information is also unavailable.)

Parameters

Tx power too low alarm, Tx power low warning - the thresholds for Warning and Alarm.

Expected Channel - the expected channel number.

Expected Antenna - the antenna mode.

Filename: `com.dartware.wrls.trango900.txt`
Version: 1.4

Trango > Trango M2400S (AP)

This probe monitors a [Trango](#) M2400S access point (AP). It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected antenna mode, and expected channel. (This probe calculates counters without using sysUpTime, which isn't available. MIB-2 traffic and interface information is also unavailable.)

Parameters

Tx power too low alarm, Tx power low warning - the thresholds for Warning and Alarm.

Expected Channel - the expected channel number.

Expected Antenna - the antenna mode.

Filename: `com.dartware.wrls.trango2400.txt`

Version: 1.1

Trango > Trango M5800S

This probe monitors a [Trango](#) 5800S access point, 5800-AP-60, or 5830-AP-60.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, number of subscriber unit clients, channel number, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

Too many client alarm, Many client warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

High Traffic Bytes alarm, High Traffic Bytes warning,

- the thresholds for Warning and Alarm.

Expected Channel - the expected channel number.

Filename: `com.dartware.wrls.trango10.txt`
Version: 1.4

Trango > Trango M5830S

This probe monitors a [Trango](#) M5830S access point.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, number of subscriber unit clients, channel number, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

Too many client alarm, Many client warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

High Traffic Bytes alarm, High Traffic Bytes warning,

- the thresholds for Warning and Alarm.

Expected Channel - the expected channel number.

Filename: `com.dartware.wrls.trango20.txt`
Version: 1.4

Trango > Trango M5830S (SU)

This probe monitors a [Trango M5830S SU](#) Subscriber Unit.

You must enter the password for the subscriber unit to retrieve the information.

NOTE: Occasionally, this Subscriber Unit reports extremely high data rates. These rates - in the range of millions of kbps - are seen both by this probe and in the Web interface. To keep the strip charts accurate, we recommend you turn off the Auto-adjust feature for the chart.

Parameter

Password - the password for the Subscriber Unit.

Filename: `com.dartware.wrls.trango.M5830SSU.txt`

Version: 1.2

Trango > Trango P5830S (master)

This probe monitors a [Trango](#) P5830S master unit.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, expected active channel number, and temperature. (This probe calculates counters without using sysUpTime, which is not available.)

Tx power too low alarm, Tx power low warning,

RSSI too low alarm, RSSI low warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

RF High Traffic Bytes alarm, RF High Traffic Bytes warning,

Eth High Traffic Bytes alarm, Eth High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Expected Channel - the expected channel number.

Filename: `com.dartware.wrls.trangoP5830SMU.txt`

Version: 1.5

Trango > Trango P5830S (remote)

This probe monitors a [Trango](#) P5830S remote unit with firmware version 1.11 (040930) or later.

It retrieves and displays a number of traffic, physical, and radio status variables. It can go into alarm or warning based on user-defined parameters for transmit power, incoming traffic on the radio interface, and temperature. (This probe calculates counters without using sysUpTime, which isn't available.)

Parameters

Tx power too low alarm, Tx power low warning,

RSSI too low alarm, RSSI low warning,

Too Hot alarm, Hot warning,

Too Cold alarm, Cold warning,

RF High Traffic Bytes alarm, RF High Traffic Bytes warning,

Eth High Traffic Bytes alarm, Eth High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.trangoP5830SRU.txt`

Version: 1.7

Tranzeo > Sixth Generation AP

This probe monitors the sixth generation Access Point (AP) from [Tranzeo](#). This series includes AP for the following models: 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus.

This probe is part of the Intermapper Wireless Probe Bundle, and requires Intermapper 4.3 or later. Tranzeo is a trademark of Tranzeo Wireless Technologies, Inc.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.gen6ap.txt`
Version: 1.0

Tranzeo > Sixth Generation CPE

This probe monitors the sixth generation Customer Premise Equipment (CPE) from [Tranzeo](#). This series includes models 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus, running firmware version 2.0.11 or later.

The probe monitors the received signal strength and compares it to the warning and alarm thresholds below.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - the thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.gen6cpe.txt`
Version: 1.2

Tranzeo > Sixth Generation PxP

This probe monitors the sixth generation point-to-point (PxP) equipment from [Tranzeo](#). This series includes models 5A, 5Aplus, 6600, 6500, 6000, 4900, CPQ, CPQplus, running firmware version 2.0.11 or later.

The probe monitors the received signal strength and compares it to the warning and alarm thresholds below.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - the thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.gen6pxp.txt`
Version: 1.1

Tranzeo > Tranzeo 58XX Series Backhaul

This probe is meant to monitor a [Tranzeo](#) 58XX Series Backhaul.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.58xx.backhaul.txt`

Version: 1.5

Tranzeo > Tranzeo (AP)

This probe monitors a [Tranzeo](#) 1000, 2000, 3000, 400, or 4000-series all in one device used as an Access Point (AP).

It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, and gives an alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Expected Channel - the number of the expected channel.

Filename: `com.dartware.wrls.tranzeoap.txt`

Version: 1.3

Tranzeo > Tranzeo (PXP)

This probe is meant to probe a [Tranzeo](#) 1000, 2000, 3000, 400, and 4000-series all in one device used as a PXP (bridge), or as an SAI (station) in router mode.

The probe retrieves and displays a number of variables for basic, ethernet, wireless, and bridge information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, as well as into alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Expected Channel - the number of the expected channel.

Filename: `com.dartware.wrls.tranzeopxp.txt`
Version: 1.3

Tranzeo > Tranzeo (SAI)

This probe is meant to probe a [Tranzeo](#) 1000, 2000, 3000, 400, and 4000-series all in one device used as an SAI (station).

The probe retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for Received Signal level, Expected versus actual Station Channel, and incoming traffic on the radio interface, as well as into alarm when the wireless or ethernet links are reported down.

Supported Models: TR-410, TR-420, TR-430, TR-440, TR-450, TR-4115, TR-4215, TR-4315, TR-4415, TR-4118, TR-4218, TR-4318, TR-4418, TR-4500, and TR-4519. This probe will also support TR-1000, TR-1100, TR-1200, TR-1300, TR-2015, TR-2115, TR-2215, TR-2315, TR-3015, TR-3115, TR-3215, TR-3315, TR-2018, TR-2118, TR-2218, and TR-2318 model radios with firmware version 3.4.31.

Parameters

Received Signal Level too low alarm, Received Signal Level low warning,

No Buffer Packets too high alarm, No Buffer Packets high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Expected Channel - the number of the expected channel.

Filename: `com.dartware.wrls.tranzeosai.txt`

Version: 1.3

Tranzeo > Tranzeo AP-5A

This probe is meant to monitor a [Tranzeo](#) TR-AP.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.ap.5A.txt`

Version: 1.4

Tranzeo > Tranzeo AP-5A (44R)

This probe is meant to monitor a [Tranzeo](#) TR-AP.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Filename: `com.dartware.wrls.tranzeo.ap.5A.44r.txt`
Version: 1.4

Tranzeo > Tranzeo Classic

This probe is meant to monitor a [Tranzeo](#) Classic.

Parameter

Password - the administrative password.

Filename: `com.dartware.wrls.tranzeo.classic.txt`
Version: 1.4

Tranzeo > Tranzeo CPE-5A

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - the thresholds for signal strength.

Filename: `com.dartware.wrls.tranzeo.cpe.5A.txt`
Version: 1.4

Tranzeo > Tranzeo CPE-5A (44R)

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - the thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.cpe.5A.44r.txt`
Version: 1.5

Tranzeo > Tranzeo CPE-200

This probe monitors a [Tranzeo](#) TR-CPE 200. It has thresholds for alarms and warnings if the signal level gets too low.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Warning Threshold, Alarm Threshold - the thresholds for signal strength

Filename: `com.dartware.wrls.tranzeo.cpe.200.txt`

Version: 1.7

Tranzeo > Tranzeo CPE-200 (1.77.R)

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

Quality Warning, Quality Alarm,

Signal Warning, Signal Alarm

- the thresholds for Warning and Alarm for Quality and Signal Strength.

Filename: `com.dartware.wrls.tranzeo.cpe.200.177R.txt`

Version: 1.4

Tranzeo > Tranzeo TR-CPE

This probe is meant to monitor a [Tranzeo](#) TR-CPE.

It will give a warning at a user-definable threshold for low signal, and an alarm when signal strength is "poor". You will need to enter as parameters

your web admin username and password, as well as the SSID of the connection you want information on.

Parameters

User - the device's administrative user name.

Password - the administrator's password.

SSID - the SSID of the connection you want to view.

Warning Threshold - the threshold for Signal Strength.

Filename: `com.dartware.wrls.tranzeocpe.txt`

Version: 1.3

WaveRider > CCU

This probe monitors a WaveRider CCU (access point). It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for radio frequency, percentage of payloads not needing a retry, percentage of payloads sent as broadcast, percentage of payloads discarded, percentage of payloads "Rx PER", percentage of payloads with HCRC errors, "Rx No-Match" errors, and high traffic incoming on the wireless interface. It will also go into an alarm based on the global status indicator.

Parameters

Expected Frequency - the expected frequency

No Retry percentage too low alarm, No Retry percentage low warning,

Broadcast percentage too high alarm, Broadcast percentage high warning,

Discard percentage too high alarm, Discard percentage high warning,

Rx PER percentage too high alarm, Rx PER percentage high warning,

HCRC percentage too high alarm, HCRC percentage high warning,

Rx No-Match too high alarm, Rx No-Match high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the Warning and Alarm thresholds.

Filename: `com.dartware.wrls.waveriderccu.txt`

Version: 1.1

WaveRider > EUM

This probe monitors a WaveRider EUM (subscriber unit). It retrieves and displays a number of variables for basic, traffic, and wireless information. It will go into alarm and warning states based on user-defined parameters for radio frequency, percentage of payloads not needing a retry, percentage of payloads discarded, RSSI value, signal strength rating, and high traffic incoming on the wireless interface. It will also go into an alarm based on the global status indicator.

Parameters

RSSI too low alarm, RSSI low warning,

Signal rating too high alarm, Signal rating high warning,

SNR too low alarm, SNR low warning,

No Retry percentage too low alarm, No Retry percentage low warning,

Tx Discard percentage too high alarm, Tx Discard percentage high warning,

High Traffic Bytes alarm, High Traffic Bytes warning

- the thresholds for Warning and Alarm.

Filename: `com.dartware.wrls.waveridereum.txt`

Version: 1.2

Experimental

AWS-EC2

This probe collects AWS metrics from AWS EC2 Instances.

Instance ID - The Instance ID, which must be from the ones listed in the Server Settings > 'AWS EC2' tab.

Poll Interval (seconds) - The time interval between the metrics being collected from AWS CloudWatch

Flow Exporter Status

This probe monitors a Flow Exporter and reports statistics about Flow activity. It does this by retrieving information from the Intermapper Flows server.

The normal state of the device is UP/OKAY. There are two error conditions:

- If the monitored device does not appear to be a Flow Exporter (it is not listed by Intermapper Flows), the status of the device is set to CRITICAL.
- If the Intermapper Flows server has received no flow records during a poll interval, the status of the device is set to DOWN.

Parameters

None

Filename: `com.dartware.flow.exporter.txt`

Version: 1.3

Intermapper

This probe monitors the status of the Intermapper polling engine. With the default setting, this probe displays the results of 500 loops through the polling engine. To measure activity at a finer-grain, decrease the value of the *Loops* parameter. A value of '1' updates the statistics on every pass through the main run loop.

The "Main Loop" frequency is the number of times that Intermapper performs the main loop each second. The theoretical maximum loop frequency is 66.667 loops per second, based on the current yield value of 15 msec. If it falls below 10 or even 5 loops per second, Intermapper may report false outages.

This probe also reports polling rate as a percentage of the maximum loops per second. This is a measure of how much additional processing occurs per loop. This percentage will never be 100%. It should, however, level out and remain steady over time.

Intermapper tracks the number of bytes sent out the main UDP polling socket. Bytes/Loop is the average bytes sent per loop, averaged over the last batch of N loops. Bytes Peak is the maximum number of bytes sent in a *single* polling loop. (In the current implementation, the peak bytes is checked on every loop, but only resets to 0 when you change the # loops parameter; ie peak bytes is not the peak bytes of the last batch of N loops.)

Parameter

Loops - the number of loops to perform before updating statistics.

Filename: `com.dartware.tcp.Intermapper.txt`
Version: 0.11

sFlow v1.2

This probe's Status Window shows the sFlow version, address, and address type of the sFlow exporter. It uses the [sFlow MIB version 1.2](#), with the Enterprise Number 4300 to retrieve statistics for sFlow versions 2 and 4.

It also shows the sFlowTable, as an on-demand table. It lists all devices receiving the sFlow records. (To view this on-demand table, you must import [the SFLOW-MIB version 1.2](#).)

Parameter

Version_HiWarn - the expected sFlow version. If the exporter version does not match this version, the device is set to a Warning state.

Filename: `com.dartware.sflowv1.2.txt`
Version: 1.2

sFlow Vers. 1.3

This probe's Status Window shows the sFlow version, address, and address type of the sFlow exporter. It uses the [sFlow MIB version 1.3](#), with the Enterprise Number 14706 for sFlow version 5.

It also shows the sFlow Receiver Table as an on-demand table. It lists all devices receiving the sFlow records. (To view this on-demand table, you must import [the SFLOW-MIB version 1.3](#).)

Parameter

sFlow version - the version of sFlow to use.

Filename: `com.dartware.sflow.v1.3.txt`
Version: 1.3

PowerShell

Disk Space

This probe uses PowerShell to retrieve the disk space available on a drive on the target host. It uses WMI's ability to retrieve information from a remote host instead of PowerShell's remoting capability. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning, Alarm and Critical parameters specified by you.

Parameters

Drive - set to All to list all local hard drives on the host. Enter a list of comma-separated drive letters with colons (:).

Drives can be listed regardless of whether they are local or not. Zero-sized drives, such as empty cd-roms, are not listed. The first drive failing the warning or critical criteria test is cited as the reason.

Warning, Alarm, Critical, Down (%) - enter a threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - can be a local user on the target host or take the form of domain\user for a domain login. Leave this field blank if authentication is not required, such as when the target is the localhost.

Password - the password of the specified user.

Timeout (sec) - the number of seconds to wait for a response from the target host.

PowerShell Version - the version of PowerShell running on the Intermapper server's host.

NOTE:

Powershell Version is not the target device's host.

Intermapper invokes the WindowsWmiFreeDiskSpace.ps1 companion script in the Tools folder of the InterMapper Settings folder when probe is loaded. It uses the exit value to set the condition of the device and the performance data returned by the script to create a display of chartable data.

Filename: `com.helpsystems.powershell.wmi.diskspace.txt`
Version: 1.0

Remoting > Disk Space

This probe uses PowerShell to determine how much disk space is available on a drive on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning and Critical parameters set by you. The target host must be running PowerShell with Remoting enabled.

Parameters

Drive - set to All to list all local hard drives on the host. Use a list of comma-separated drive letters with colons (:).

Drives can be listed regardless of whether they are local or not. Zero-sized drives (for example, an empty cd-rom) are not listed. The first drive failing the warning or critical criteria test is cited as the reason.

Warning, Alarm, Critical, Down (%) - the threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - can be a local user on the target host or take the form of domain\user for a domain login. Leave this field blank if authentication is not required, such as when the target is the localhost.

Password - the password of the specified user.

Timeout (sec) - the number of seconds to wait for a response from the target host.

PowerShell Version - the version of PowerShell running on the Intermapper server's host.

NOTE:

PowerShell Version is not the target device's host.

Intermapper invokes the WindowsRemotingFreeDiskSpace.ps1 companion script in the Tools folder of the InterMapper Settings folder when probe is loaded. It uses the exit value to set the condition of the device and the performance data returned by the script to create a display of chartable data.

Filename: `com.helpsystems.powershell.remote.diskspace.txt`
Version: 1.0

Remoting > Disk Space (Signed)

NOTE:

This probe requires a companion script that must be signed and placed in the \Intermapper Setting\Tools folder before it can be run.

This probe uses PowerShell to determine the disk space available on a drive on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the Warning and Critical parameters you set. The target host must be running PowerShell with Remoting enabled.

Parameters

Drive - set to All to list all Local hard drives on the host. Use a list of comma-separated drive letters with colons (:).

Drives can be listed regardless of whether they are local or not. Zero-sized drives (for example, an empty cd-rom) are not listed. The first drive failing the warning or critical criteria test is cited as the reason.

Warning, Alarm, Critical, Down (%) - the threshold for the percentage of disk space that changes the device's state to the specified alarm level.

User - can be a local user on the target host or take the form of domain\user for a domain login. Leave this field blank if authentication is not required, such as when the target is the localhost.

Password - the password of the specified user.

Timeout (sec) - the number of seconds to wait for a response from the target host.

PowerShell Version - the version of PowerShell running on the Intermapper server's host.

NOTE:

PowerShell Version is not the target device's host.

Intermapper attempts to invoke the WindowsRemotingFreeDiskSpace.signed.ps1 companion script after setting ExecutionPolicy to AllSigned. If Intermapper is installed in the default location, this script is available in the C:\Program Files\Intermapper\docs\samples\powershell folder. It must be copied to the Tools folder and signed before it can run. It uses the exit value to set the condition of the device and the performance data returned by the script to create a display of the results.

Filename:

`com.helpsystems.powershell.remote.diskspace.sign.txt`

Version: 1.0

Remoting > Installed Software

This probe uses PowerShell to provide a listing of installed software, installed updates, or both. This probe requires that **PowerShell 2.0** or later be installed and that PowerShell remoting is enabled and configured to use this probe. This probe uses the registry, not WMI objects.

Parameters

Software - specify whether to list installed software, software updates, or both.

User - can be a local user on the target host or take the form of domain\user for a domain login. Leave this field blank if authentication is not required, such as when the target is the localhost.

Password - the password of the specified user.

Authentication - the type of authentication you want PowerShell when connecting to the target host.

Timeout (sec) - the number of seconds to wait for a response from the target host.

PowerShell Version - the version of PowerShell running on the Intermapper server's host.

NOTE:

PowerShell Version is not the target device's host.

Intermapper invokes the included ApplicationList.ps1 companion script in InterMapper Settings/Tools.

Filename:

`com.helpsystems.powershell.remote.installedSoftware.txt`

Version: 1.0

Remoting > Process Count

This probe uses PowerShell's remoting capabilities and Get-Process object to retrieve the number of instances of a given process currently executing on the target host.

Parameters

ProcessName - the name of the process you want to monitor.

User - may be a local user on the target host, or may take the form of "domain\user" for a domain login. Leave it blank if authentication is not required, such as when the target is the localhost.

Password - the password of the specified user.

Timeout (sec) - the number of seconds to wait for a response from the target host.

PowerShell Version - the version of PowerShell running on the Intermapper server's host.

NOTE:

PowerShell Version is not the target device's host.

Intermapper invokes the ProcessCount.ps1 companion script in the Tools folder of the InterMapper Settings folder when probe is loaded.

Filename:

`com.helpsystems.powershell.remote.processcount.txt`

Version: 1.0

Probe Groups

Probe Group

This probe creates an empty probe group. After you create a device using this probe, you can select the new probe group device and other devices and click Insert > Group to place those devices into the single probe group. For more information on probe groups, see the User Guide at <http://Intermapper.com/go.php?to=Intermapper.probegroups>.

Parameters

None

Filename: `com.dartware.probegroup.txt`
Version: 0.4

Splunk

Layer 2 Output

This probe scans InterMapper's Layer 2 database for information collected from switch devices, and writes it into a CSV file. The InterMapper App for Splunk , then retrieves this data for its display.

If the process fails for any reason, the device is set to Warning.

Default poll interval is 10 minutes. You should decrease this (Set Info > Set Poll interval) only if your Layer 2 discovery runs more frequently.

NOTE: You should create only one device that uses this probe on an InterMapper server. Having multiple instances consumes server resources with no benefit.

Parameters

None

WMI

WMI CPU Utilization

This probe uses WMI to retrieve the percentage of time that a processor uses to execute a non-idle thread on the target host. Specifically, it queries the PercentProcessorTime property of the Win32_PerfFormattedData_PerfOS_Processor class and compares it against the Warning and Critical parameters you set.

The target host must be running Windows XP or Windows Server 2003 or later.

Parameters

Single Warning, Single Critical, Total Warning, and Total Critical - the device's condition is set by comparing each processor against the specified Single percentages, and the total CPU utilization against the specified Total percentages. You can leave any of these values blank.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost), leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `cpu_util.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.cpu_utilization.txt`
Version: 1.13

WMI Disk Available

This probe uses WMI to determine the disk space available on the specified drive(s) on the target host. Specifically, it queries the Size and FreeSpace properties of the Win32_LogicalDisk class, computes percentage free space, and compares it against the specified values. The target host must be running Windows 2000 or later.

Parameters

Drive - May be set to "All" to check disk space on all of the host machine's local hard drives. Enter a list of comma-separated drive names (including the colon). These drives will be listed regardless of whether they are local

hard drives. Zero-sized drives, such as an empty cd-rom, are not listed. The first drive with space that is less than the specified values is cited in the reason.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Intermapper invokes the `disk_avail.vbs` companion script included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.disk_available.txt`
Version: 1.12

WMI Disk Fragmentation Analysis

This probe uses WMI to analyze disk fragmentation on a drive on the target host. Specifically, it calls the `DefragAnalysis` method of the `Win32_Volume` class and reports pertinent statistics from the analysis. If the drive needs to be defragmented, the device is set to **Warning**. The target host must be running Windows Vista, Windows Server 2003 or later.

Parameters

Drive - the drive letter assigned to the local disk to be analyzed, including the colon but without backslashes.

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `defrag_analysis.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.defrag_analysis.txt`
Version: 1.12

WMI Event Log

This probe uses WMI to retrieve entries from the Event Logs on the target host. Specifically, it queries the Win32_NTLogEvent class, limiting the search with the parameters you set. If matching events are found, a critical status is returned. The target host must be running Windows 2000 or later.

Parameters

Log File - contains a comma-separated list of the logs to be searched. At least one Log File is required.

Event Codes - a comma-separated list of event codes to search. To select all codes, leave this parameter blank.

Event Types - a comma-separated list; can include event type names or corresponding numerical values. Names and values can be intermixed. Limits the selection to events of the specified types.

Hours, Minutes, and Seconds - combine to define how far back in the event log to search. The specified values are subtracted from the current time and used to select events, based on when they were written to the log.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `event_log.vbs` companion script included with this probe.

Filename: `com.dartware.wmi.event_log.txt`
Version: 1.14

WMI File Check

This probe uses WMI to retrieve information about files on the target host. Specifically, it queries the CIM_DataFile class, limiting the search with the parameters you set. The target host must be running Windows 2000 or later.

Parameters

Path - the location of the files to be checked. Include the drive, and enclose the path in double-quotes if it contains spaces.

File - the filename and extension of the file you wish to check. The path is prepended to filename during the final query. To check all files that met the specified Size or time criteria, leave this parameter blank. You may also use a list of comma-separated filenames.

Wildcards (* ?) can be used in the filename. When using wildcards, be sure to specify the Path parameter. Otherwise, the query could take an inordinate amount of time. At least one of *File* or *Path* must be set.

Size - the minimum filesize in bytes. Any file larger than this value is listed.

Hours, Minutes, and Seconds - specify how recently the file was changed in order to be listed, based on the file's LastModified value. At least one of these parameters must be set.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `file_chk.vbs` companion script, included with the probe. It lists the files which meet the specified criteria, and uses the exit value to set the condition of the device.

Filename: `com.dartware.wmi.file_check.txt`
Version: 1.12

WMI Folder Check

This probe uses WMI to retrieve information about a folder on the target host. Specifically, it queries the Win32_Directory and CIM_DataFile classes to walk the directory tree, accumulating file and folder counts and the total of file sizes. It also notes the most recently modified file in the tree. The target host must be running Windows 2000 or later.

Parameters

Path - specifies the folder at the top of the tree you want to check. It should include the drive, and should be enclosed in double-quotes if it contains spaces.

Warning and **Critical** - set thresholds for the number of folders, the number of files, and the total of the file sizes.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `folder_chk.vbs` companion script, included with the probe. The script compares the number of files, folders, and the total size against your criteria to set the condition of the device.

Filename: `com.dartware.wmi.folder_check.txt`
Version: 1.14

WMI Free Memory

This probe uses WMI to retrieve the amount of physical memory available to processes running on the target host, in megabytes. Specifically, it queries the `TotalPhysicalMemory` property of the `Win32_ComputerSystem` class. It also queries the `FreePhysicalMemory` property of the `Win32_OperatingSystem` class and compares it against specified thresholds. The target host must be running Windows 2000 or later.

Parameters

Warning and **Critical** - specify thresholds in megabytes for which the device condition is set to the specified state.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `free_mem.vbs` companion script, included with the probe. The script uses the `exit` value to set the condition of the device. It

uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.free_memory.txt`
Version: 1.11

WMI Installed Software

This probe uses WMI to retrieve information about software installed on the target host. Specifically, it queries the Win32_Product class for information about products installed using Windows Installer. It also queries Win32_OperatingSystem and displays the operating system name, version and service pack level.

The target host must be running Windows XP, Windows Server 2003 or later. On Windows Server 2003, the Win32_Product class isn't always installed by default. You can install the "WMI Windows Installer Provider" component under "Management and Monitoring Tools" in "Add/Remove Windows Components".

Parameters

User - may be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `installed_software.vbs` companion script included with this probe.

Filename: `com.dartware.wmi.installed_software.txt`
Version: 1.8

WMI Logged-on Users

This probe uses WMI to retrieve information about users logged on to the target host. Specifically, it queries the LogonType and StartTime properties of the Win32_LogonSession class, limiting the selection to those in the comma-separated list of numeric Logon Types you set in the Type parameter. It queries instances of the Win32_LoggedOnUser class, matches the LogonID and extracts the user's name and domain from the

path of the Win32_Account. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `log_users.vbs` companion script, included with this probe.

Filename: `com.dartware.wmi.logged-on_users.txt`
Version: 1.14

WMI MExchange 2007 Hub Transport Server

This probe uses WMI to retrieve performance information about the delivery queues on a MS Exchange 2007 Hub Transport Server. Specifically, it queries the `Win32_PerfFormattedData_MExchangeTransportQueues_MExchangeTransportQueues` class to collect a variety of queue statistics and then compares them to the criteria you set. The default criteria for warning and critical conditions are taken from the Microsoft TechNet article [Monitoring Hub Transport Servers](#).

Parameters

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `ex07_transport.vbs` companion script included with this probe. It uses the exit value to set the condition of the device.

Filename: `com.dartware.wmi.ex07_transport_server.txt`
Version: 1.7

WMI MExchange 2007 Mailbox Server

This probe uses WMI to retrieve performance information about the delivery queues on a MS Exchange 2007 Mailbox Server. Specifically, it queries the Win32_PerfFormattedData_MSExchangeIS_MSExchangeIS, Win32_PerfFormattedData_MSExchangeIS_MSExchangeISMailbox, Win32_PerfFormattedData_MSExchangeIS_MSExchangeISPublic, Win32_PerfFormattedData_MSExchangeSearchIndices_MSExchangeSearchIndices classes to collect a variety of statistics and then compares them to the criteria you set. The default criteria for warning and critical conditions are taken from the Microsoft TechNet article [Monitoring Mailbox Servers](#).

Parameters

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `ex07_mailbox.vbs` companion script included with this probe. It uses the script's exit value to set the condition of the device.

Filename: `com.dartware.wmi.ex07_mailbox_server.txt`
Version: 1.7

WMI Network Utilization

This probe uses WMI to retrieve the network utilization on an interface on the target host. Specifically, it queries the BytesTotalPersec, CurrentBandwidth, OutputQueueLength and PacketsReceivedErrors properties of the Win32_PerfFormattedData_Tcpip_NetworkInterface class. It compares OutputQueueLength against the Warning and Critical parameters you set. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

The interface may be selected by IP Address, MAC Address, or Index. When specifying a MAC address, use colons, hyphens or no separators. The interface name is queried from the Win32_NetworkAdapterConfiguration class and used to query data from the Win32_PerfFormattedData_Tcpip_NetworkInterface class.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `net_util.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.net_utilization.txt`
Version: 1.13

WMI Process Monitor

This probe uses WMI to retrieve information about processes running on the target host. Specifically, it queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfProc_Process` class and compares it against the specified parameters. Any of the specified processes not found are listed, and the status is set to Critical. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

Process - a comma-separated list of process names to check. Extensions are not included in the process names. Names containing spaces or other special characters should be enclosed in quotes. If more than one process matches the name, all matching processes are listed.

Warning and Critical - the thresholds (in percent) for which the device condition is set to the specified state.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `proc_mon.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the device. It

also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.process_monitor.txt`
Version: 1.14

WMI Service Monitor

This probe uses WMI to retrieve the state of services running on the target host by querying the Win32_Service class. Any specified services not found are listed, and the status is set to Critical. The target host must be running Windows 2000 or later.

Parameters

Service - a comma-separated list of service names to be checked.

NOTE: Service names should not be confused with the service's Display Name, shown in the Services tool. Check the Properties for the service to find the actual service name. Names containing spaces or other special characters should be enclosed in quotes.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `serv_mon.vbs` companion script, included with the probe. The script's exit value is used to set the condition of the device.

Filename: `com.dartware.wmi.service_monitor.txt`
Version: 1.15

WMI SQL Server 2008 Service Monitor

This probe uses WMI to retrieve the state of Microsoft SQL Server 2008 services running on the target host by querying the Win32_Service class. The states of the selected services are listed, and if any are not running, the status of the device is set to Critical. The target host must be running Windows 2000 or later.

Parameters

Services - select or clear checkboxes to select the services which you want to monitor.

Instance - the SQL Server instance you wish to monitor on the target host. To monitor the default instance, leave this parameter blank.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `sql2k8_serv_mon.vbs` companion script, included with this probe. It uses the script's exit value to set the condition of the device.

Filename: `com.dartware.wmi.sql2k8_service_monitor.txt`
Version: 1.7

WMI System Accessibility

This probe uses WMI to test accessibility of a target device from the monitored host. Specifically, it uses the `Win32_PingStatus` class to test the connectivity and returns a chartable response time. If the target cannot be pinged, the status is set to critical and a discontinuity is inserted in the chart data. The target host must be running Windows XP, Windows Server 2003 or later.

Additional information about the monitored host is queried from the `Win32_NetworkAdapterConfiguration` and `Win32_NTDomain` classes and displayed in the status window.

Parameters

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `sys_access.vbs` companion script, included with the probe. It uses the script's exit value to set the condition of the

device. It also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.system_accessibility.txt`
Version: 1.12

WMI System Information

This probe uses WMI to collect a variety of information about the monitored host including hardware and operating system details. The target host must be running Windows 2000 or later.

Parameters

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `system_info.vbs` companion script, included with the probe.

Filename: `com.dartware.wmi.system_infomation.txt`
Version: 1.11

WMI Top Processes

This probe uses WMI to retrieve information about CPU utilization and processes running on the target host. Specifically, it queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfOS_Processor` class and compares it against the specified thresholds. It queries the `PercentProcessorTime` property of the `Win32_PerfFormattedData_PerfProc_Process` class and lists up to five processes using the most CPU time. Because there is a time lapse between collecting the CPU data and the process data, the reported values do not add up exactly. The target host must be running Windows XP, Windows Server 2003 or later.

Parameters

Warning and **Critical** - set a value in percent to use as the threshold to set the device to this condition.

User - can be a local user on the target host, or can take the form `domain\user` for a domain login. If authentication is not required (such as when the target is localhost,) leave this parameter blank.

Timeout (sec) - the number of seconds to wait before assuming the host is not available.

Intermapper invokes the `top_cpu.vbs` companion script, included with the probe. The probe uses script's the exit value to set the condition of the device. It also uses the performance data returned by the script to create a nice display of chartable data.

Filename: `com.dartware.wmi.top_process.txt`
Version: 1.13

Packet-Based Probes

Packet-Based Test Procedure

Whenever Intermapper tests a packet-based device, it uses the following procedure:

1. Intermapper sends the appropriate probe packet (ping, SNMP get-request, DNS query, and so on).
2. Intermapper waits the timeout interval specified for the particular device.
3. If a response arrives, Intermapper examines its contents and sets the device status based on that response.
4. However, if no response arrives, Intermapper sends another probe packet
5. The above procedure is repeated until a response arrives or the specified number of probes has been sent.
6. If no response has arrived after the final timeout, Intermapper sets the device status to Down.
7. In any event, the device is scheduled to be tested again at a time set by the map's (or the device's) poll interval.

The default timeout is three seconds, with a default probe count of three seconds. Consequently, Intermapper will take nine seconds to declare a device is down (three probes, waiting three seconds each). Both the timeout and the number of probes can be set for each device.

This often gives rise to 21 second or 51 second outages. What's happening here is that the device fails to respond to one set of probes (for example, after nine seconds), but

responds immediately at the next poll 30 or 60 seconds later. This gives an outage duration to be $(30-9=21)$ seconds or $(60-9=51)$ seconds.

Shared Polling in Ping/Echo and SNMP Probes

For Ping/Echo and SNMP probes (built-in or custom), Intermapper polls a device only once if it is considered to be the same device, and shares the response among all the maps that poll that device.

This happens automatically, and there are no user-controllable parameters.

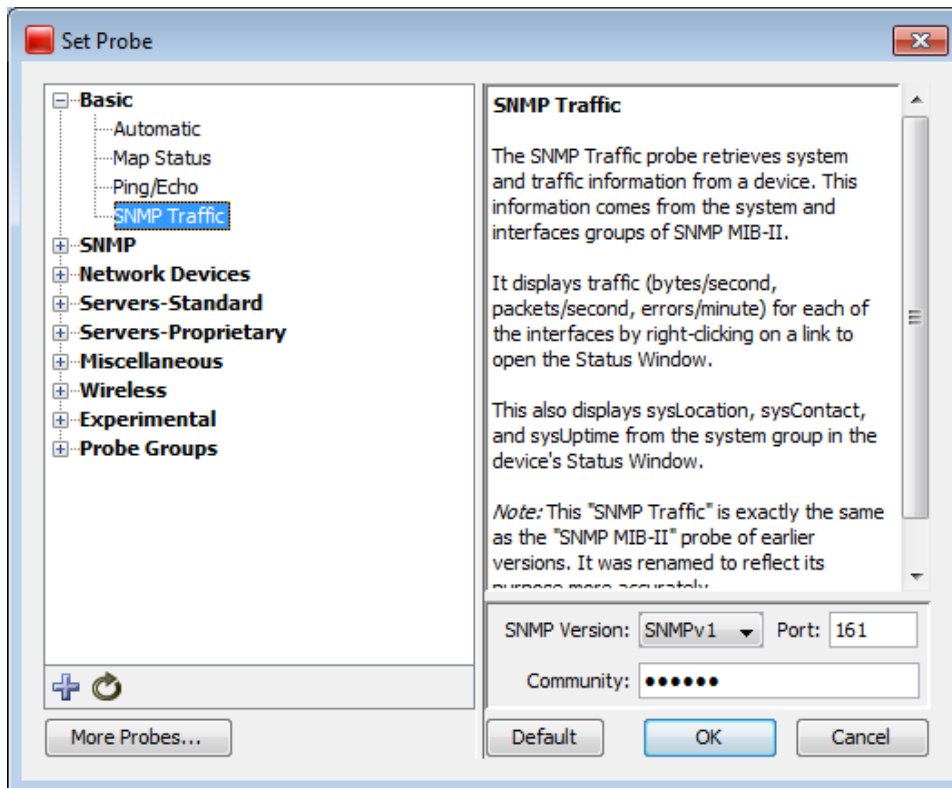
In order for two mapped devices to be considered the same and share the results of a single probe, the following characteristics of the mapped device must be identical:

- Probe Type
- Address
- Port
- Poll Interval
- Timeout
- Max tries
- Display Unnumbered Interfaces, Ignore Discards, Ignore Errors, Allow Periodic Reprobe
- SNMP Version and read-only community string
- Number, name, and value of probe parameters
- SNMPv3 authentication information

For SNMP probes, the following flags in the probe file must be identical. (this is nearly always the case, as it is implied by the probe type, but is still checked explicitly):

- MINIMAL
- NOLINKS
- LINKCRITICAL

SNMP Versions

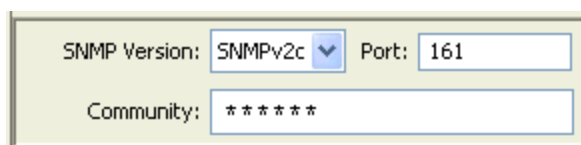


Using SNMP Version 1, 2c, and 3 in Probes

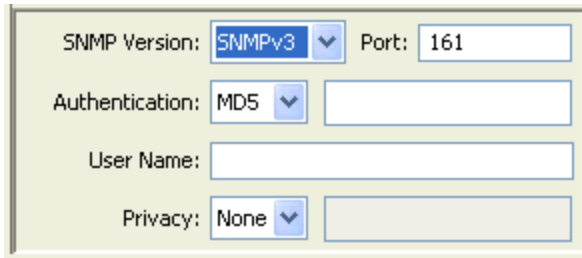
All SNMP-based probes can use one of version 1, 2c, or 3, at the user's choice. The Probe Configuration window allows you to specify the SNMP version at the same time you set all the other parameters for the probe.

The lower part of the Probe Configuration window displays the SNMP version information. Select the version from the SNMP Version menu.

- Selecting SNMPv1 or SNMPv2c will show a field to enter the SNMP Read-only community string.



- Selecting SNMPv3 changes the lower half of the probe configuration window to let you specify all the authentication and privacy parameters. The initial settings show the default settings taken from the Server Settings > SNMP pane. See the [SNMP Preferences \(Pg. 228\)](#) page for more details.



The screenshot shows a configuration window for SNMP. It contains the following fields and controls:

- SNMP Version:** A dropdown menu currently set to "SNMPv3".
- Port:** A text input field containing the value "161".
- Authentication:** A dropdown menu set to "MD5", followed by an empty text input field.
- User Name:** An empty text input field.
- Privacy:** A dropdown menu set to "None", followed by an empty text input field.

NOTE: Certain equipment requires SNMPv2 or SNMPv3, and probes can be built to force that selection. If you try to set the SNMP version lower than the probe can support, you receive an error message.

Command Line Probes

Command line probes execute a command as a command-line on supported platforms. They usually call custom executables on the target machine.

Use the Command Line probe to execute a user-written program or script to test a device. The result code returned from the program sets the device's condition. When you create a custom command line probe, you usually start with the Nagios Plugin probe.

For more information, see Command Line Probes in the Developer Guide.

Monitoring NT Services with the Microsoft Windows NT Services Probe

Intermapper can monitor and send notifications for NT Services running on another system. Intermapper uses the Service Control Manager facilities of the underlying Microsoft Windows host to communicate with a remote computer to track the state of its services.

NOTE: This NT Services monitoring is only available if the Intermapper server is running on a Microsoft Windows XP or 2003 system. You cannot use this facility if you use a macOS or Linux system to host the Intermapper server.

The **NT Services** configuration window displays the full list of services that are running on a remote host. You can select one or more services to monitor; Intermapper and receive an alert if any of them fails. The following are the probe parameters:

- A list of **NT services** on the target machine. This list displays red and green icons to indicate if the service is currently running. To receive an alert when a system fails, select the service.
- The **Username** and **Password** required to log into the target machine.

Authentication for NT Services Probe

The NT Services probe opens the Service Control Manager (SCM) on the target machine; hence, some authentication is required before this can happen. There are several ways to do this.

1. **Using built-in username and password:** Intermapper has the built-in ability to solicit from you a username and password for authentication. When you choose the NT Services probe, it will prompt you for a username and password before attempting to connect to the target machine. If you have not used one of the methods below, fill in a username and password at that point and click OK. This will be all you need to do for authentication; the username and password will be saved.

NOTE: For this to work, Intermapper must be running as an administrator, as only administrators are empowered to make the required network connections. You can do this in one of two ways:

NT Services Preferences Panel

- The first way is by adjusting the account under which Intermapper is run. Intermapper is normally installed under the LocalSystem account, which does not have administrator privileges. To change the account under which it runs, go to the **SCM** and stop the **Intermapper service** if it is running. Right-click and select **Properties**. Select the **Log On** tab. Under **Log On As**, click the radio button next to **This account** and click **Browse** to list the accounts; choose an account with administrator privileges. Fill in the password for the account in **Password** and **Confirm Password**. Click **OK**.
- The second way is to allow Intermapper to be an administrator when it needs to be by supplying it with an administrator's username and password, so that it can elevate its privileges when it needs to. You can do this using the NT Services item in the Server Settings list.

NOTE: In either scheme, the administrator you supply must have been given the "Logon as a service" right in the local security policy of the machine you are monitoring.

2. **The NET USE command.** Another way to authenticate is to use the NET USE command to create a connection between the host machine and the target. For instance, to monitor the services on a host at 192.168.1.140, enter the following:

```
NET USE \\192.168.1.140\ipc$ /USER:Administrator
```

You will be prompted for the password, and the connection will be made. (If you have done this, when prompted for a username and password for NT Services by Intermapper, you can leave them blank and click OK.)

NOTE: You must use the IP address and not the network name for the machine. That is important, as the Windows OS will not see the DNS name or the domain name as being the same as 192.168.1.140 when checking the connections, and will not recognize that there is a connection when Intermapper tries to query the services by IP address, returning an "access denied" error instead.

3. **Synchronizing Users:** A third way to authenticate is to make sure that the user and password under which the Intermapper service is running exists on the target machine as well.

When Intermapper is first installed, it is installed running under the user "LocalSystem", as most services are. It is necessary to create a new user on your machine; let's name it "Intermapper"> and give it a password. Make sure it is a member of Administrators. (If you already have a username and password that exist on all machines that are to be targeted by the NT Services probe as

well as the Intermapper host and which has Administrator permissions everywhere, you can skip the previous step and substitute it for *Intermapper* in the following.)

Go to the **SCM** and stop the **Intermapper service** if it is running. Right-click and select **Properties**. Select the **Log On** tab. Under **Log On As**, click the radio button next to **This account** and click **Browse** to list the accounts. Select *Intermapper*. Fill in the password for the account in **Password** and **Confirm Password**. Click **OK**.

On the target machine, create a new user, also named *Intermapper*, with the same password and a member of Administrators.

Start Intermapper from the SCM on the original machine. You can now use NT Services probes. (When prompted for a username and password for NT Services by Intermapper, you can leave them blank and click **OK**.)

Error Messages

Intermapper may encounter authentication errors when attempting to connect. Here is a list of the messages and ways you might work around them:

- **Error attempting to elevate privileges.** Intermapper is not running as an administrator, and thus needs to elevate its privileges in order to be able to execute the NT Services probe. It could not do so. Make sure a correct username and password for the Intermapper host machine have been supplied in the NT Services panel of the Server Settings dialog. Make sure the user given has the right to log on as a service in your Local Security Policy. If host machine is Microsoft Windows Server 2003 or newer, make sure the user has the right to impersonate another user.
- **Could not establish Microsoft Windows Networking connection to probe target.** When a username and password have been supplied for the target machine, Intermapper attempts to use them to create a connection between the host and the probe target. This attempt failed for some reason. Will be followed by more specific error information. See below.
- **Could not open SCM on probe target.** Intermapper could not open the Service Control Manager on the target machine. Is followed by more specific error information. See below.

The following errors might be appended to the messages above:

- **Access is denied.** Make sure Intermapper is running as an administrator, or that an administrator username and password have been provided in the NT Services panel in the Server Settings dialog. Make sure a valid administrator username and password have been supplied for the probe target. If the probe

target is running Microsoft Windows XP, make sure that "Simple Networking" is turned off.

- **The network name cannot be found.** and **The network path was not found.** The device you have specified does not appear to exist on the network. If you are sure that it does, make sure it is a Microsoft Windows machine with File and Print Sharing turned on, and that any firewall has exceptions for File and Print Sharing.
- **An extended error has occurred.** A network-specific error has occurred. It should be followed by more information about the nature of the error. You might need to consult your network administrator.
- **The specified network password is incorrect.** The password you supplied doesn't match the username.
- **No network provider accepted the given network path.** and **The network is not present or not started.** No network is present, or a component of the network is not started. Consult your network administrator.
- **The RPC server is unavailable.** Make sure that probe target is a Microsoft Windows machine with File and Print Sharing turned on, and that any firewall has exceptions for File and Print Sharing.

Cisco IP SLA Probe

IP SLA uses active traffic monitoring - the generation of traffic in a continuous, reliable, and predictable manner - for measuring network performance edge-to-edge over a network. The traffic generated simulates network applications like VoIP and video conferencing, and collects network performance information in real time. The information collected includes data about jitter (interpacket delay variance), latency, and packet loss.

Cisco IP SLA is supported on most IOS-based Cisco routers and switches. IP SLA was previously known as Service Assurance Agent (SAA).

You can easily configure your Cisco routers and switches to be IP SLA agents or IP SLA responders. An agent initiates IP SLA tests to a remote responder. A particular agent can have multiple IP SLA tests running to many remote responders. A particular router or switch can be both an agent and a responder. For each IP SLA test that has been configured the agent collects edge-to-edge network performance information and stores it in the Cisco RTTMON MIB.

The Intermapper IP SLA Probe


```

Jitter Test UBC<->UNBC
Device Status
  Name: Jitter Test UBC<->UNBC
  DNS Name: (Unknown)
  SysName: LFSC01-97
  Address: 10.10.2.29
  Status: UP
  Protocol: SNMP - Cisco SRA Jitter Probe (port 161)
  Up Time: 13 days, 17 hours, 45 minutes
  Contact: netadmins@example.com
  Availability: 100 % (of 3 days, 20 hours, 9 minutes)
  Packet Loss: 0.14 % (of 11079 total attempts) [Reset]
  Recent Loss: 1 pkts at Oct 31, 20:43:06
  Round-trip time: 7 msec
Cisco IP SLA Jitter Test Information
Probe version: Feb.1, 2007 IP SLA Agent 1min Avg CPU Busy:1%
Alarm and Warning Thresholds:
  Latency Alarm:150ms, Latency Warning:100ms
  Jitter Alarm:30ms, Jitter Warning:20ms
  Packet Loss Alarm:1%
Jitter Test Parameters:
  Send 50 1024-byte packets spaced 20ms apart every 60 seconds
  SNMP index:59
Latest Round Trip Test Results:
  Number of Round Trips:50, Min:15ms, Max:16ms, Sum:776ms, Avg:16ms
  SD Packets Lost:0, DS Packets Lost:0
  Out of Sequence:0, Late Arrival:0
  % Packet Loss:0%, Total Packets Lost:0
Latest Jitter Test Results:
  SD +Jitter Values #:2, Min:1ms, Max:1ms, Sum:2ms, Avg:1ms
  SD -Jitter Values #:2, Min:1ms, Max:1ms, Sum:2ms, Avg:1ms
  DS +Jitter Values #:4, Min:1ms, Max:1ms, Sum:4ms, Avg:1ms
  DS -Jitter Values #:3, Min:1ms, Max:1ms, Sum:3ms, Avg:1ms
  Average Jitter Value:0ms, Total Jitter:11ms, Max Jitter:1ms
Latest Latency Test Results:
  SD Packets Sent #:50, Min:8ms, Max:9ms, Sum:403ms, Avg:8ms
  DS Packets Rcvd #:50, Min:7ms, Max:8ms, Sum:373ms, Avg:7ms
  Average Latency:8ms, Max Latency:9ms
60min Accumulated Test Results:
  60min Max Round Trip Time:17ms
  60min Total SD Packets Lost:0, Total DS Packets Lost:0
  60min Max SD +Jitter Value:1ms, -Jitter, Value:1ms
  60min Max DS +Jitter Value:2ms, -Jitter, Value:2ms
Last updated Nov 01, 09:58:41; interval: 1 minute, 0 seconds

```

The Intermapper Cisco IP SLA Jitter probe uses SNMP to collect the information from the RTTMON MIB in the agent, allowing you to alarm jitter, latency, and packet loss, and to chart these values. You can [download a .zip](#) of the probe.

The Intermapper Cisco IP SLA Probe is particularly useful for monitoring and measuring QoS for VoIP and video conferencing applications. However, it is useful in many other contexts including:

- Service level agreement monitoring, measurement, and verification.
- IP network health assessment
- Troubleshooting of network operation

Documentation

An [IP SLA Probe User Guide](#) describes how to set up the IP SLA testing between two Cisco routers/switches and how to configure the Intermapper probe to monitor the values.

This page shows a sample Status Window for the probe. You can also see a [screenshot with several graphs from a live installation](#).

Extensive documentation about IP SLA and how to configure IP SLA is available on the [Cisco website](#).

Big Brother Probes

Intermapper can act as a Big Brother server. Big Brother has been a popular network monitoring tool that allows you to create scripts ("clients") that run on remote systems and send status reports back to the Big Brother server. This allows a network manager to test additional kinds of network devices, either by writing scripts or by using some of the many scripts that are already available.

NOTE: Big Brother was created by two developers who later joined Quest Software, continuing to work on the product. In 2012, Quest Software was purchased by Dell. (Source: [Wikipedia](#).)

All available support information about Big Brother provided by Dell can be found at Dell's [Big Brother page](#). Dell does not appear to provide client binaries, but you may be able to find them at one of the software distribution sites. A lot of additional information, including potential sources of binaries and source code, is at the Wikipedia link above.

Using the Big Brother Probe

When you specify a device to be tested with a Big Brother probe, Intermapper's built-in Big Brother server listens for messages coming from a Big Brother client on the corresponding machine.

To configure Big Brother probe, you need to set the following parameters:

- **Port** - the default port is 1984, but you may choose a different port. If you choose a different port, make sure that the Big Brother client on the corresponding machine is also configured for the same port.

- **Purple Time** - the number of minutes to wait without a report before indicating a problem. In an actual Big Brother server, this is thirty minutes; Big Brother shows a device as purple if it goes this long without reports from the device. Intermapper shows it as DOWN (blinking red).

In order for Intermapper to receive Big Brother messages from the remote client, it must be configured correctly. In particular, the client must be configured so that its BBDISPLAY is set to the IP address of the machine where Intermapper is running.

The Big Brother states will be mapped to Intermapper states as shown in the table below:

Big Brother State	Intermapper Status
Okay (green)	Okay (green)
Attention (yellow)	Warning (yellow)
Trouble (red)	Critical (red)

At the moment, the only messages that Intermapper processes and represents are status and combo messages.

NOTE: The Big Brother server for a given port does not start until at least one device has been configured for that port. Similarly, once the last device for that port has been removed, the server for that port shuts down.

Troubleshooting Network and Server Probes

How do I change the protocol that Intermapper polls with?

1. Select the device you want to change.
2. From the **Monitor** menu, select **Info Window**.
3. From the **Probe Type** menu, select a new probe type. If parameters are required, a parameters window is displayed for the selected probe type.
4. Enter parameters as needed and click **OK**. The device is polled using the new probe type.

For more information, see [Status Windows](#).

What MIB variables does Intermapper poll?

Anytime Intermapper displays traffic for a link, (using the [SNMP Traffic Probe](#), for example) it polls the following variables:

SNMPv1

When you set the SNMP Version to SNMPv1, the following variables are queried:

MIB Variable	OID	SNMP Version
ifInOctets	1.3.6.1.2.1.2.2.1.10	SNMPv1
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	SNMPv1
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	SNMPv1
ifOutOctets	1.3.6.1.2.1.2.2.1.16	SNMPv1
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	SNMPv1
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	SNMPv1

Intermapper examines these two variables to decide whether an interface is up or down:

MIB Variable	OID	SNMP Version
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1

Intermapper examines these variables to detect error conditions:

MIB Variable	OID	SNMP Version
ifInDiscards	1.3.6.1.2.1.2.2.1.13	SNMPv1
ifInErrors	1.3.6.1.2.1.2.2.1.14	SNMPv1
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	SNMPv1
ifOutErrors	1.3.6.1.2.1.2.2.1.20	SNMPv1

SNMPv2c

When you set the SNMP Version to SNMPv2c, the following variables are queried:

This variable set is used on an initial scan of the device.

MIB Variable	OID	SNMP Version
ifDescr	1.3.6.1.2.1.2.2.1.2	SNMPv1
ifType	1.3.6.1.2.1.2.2.1.3	SNMPv1
ifMTU	1.3.6.1.2.1.2.2.1.4	SNMPv1
ifSpeed	1.3.6.1.2.1.2.2.1.5	SNMPv1
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	SNMPv1
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1
ifName	1.3.6.1.2.1.31.1.1.1.1	SNMPv2c
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15	SNMPv2c
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16	SNMPv2c
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17	SNMPv2c
ifAlias	1.3.6.1.2.1.31.1.1.1.18	SNMPv2c

This variable set is polled to display statistics for the device's operation.

MIB Variable	OID	SNMP Version
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	SNMPv1
ifOperStatus	1.3.6.1.2.1.2.2.1.8	SNMPv1
ifLastChange	1.3.6.1.2.1.2.2.1.9	SNMPv1
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	SNMPv1
ifInErrors	1.3.6.1.2.1.2.2.1.14	SNMPv1
ifInDiscards	1.3.6.1.2.1.2.2.1.13	SNMPv1
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	SNMPv1
ifOutErrors	1.3.6.1.2.1.2.2.1.20	SNMPv1
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	SNMPv1
sysUpTime	1.3.6.1.2.1.1.3	SNMPv1
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	SNMPv2c

ifHCOctets	1.3.6.1.2.1.31.1.1.1.10	SNMPv2c
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2	SNMPv2c
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	SNMPv2c
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	SNMPv2c
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5	SNMPv2c

NOTE: In the SNMPv2c, the input and output MulticastPkts and BroadcastPkts MIB variables replace NUCastPkts variables of the SNMPv1 probe, which are deprecated. HCOctets replace the regular Octets counters. Pkts and errors still use the MIB-II 32 bit counters.

How does Intermapper compute traffic statistics?

Intermapper uses `ifInOctets` and `ifOutOctets` to compute the Receive and Transmit bytes/second values, respectively.

The Receive and Transmit packets/second numbers are computed using the sum of the (`ifInUcastPkts` + `ifInNUcastPkts`) and (`ifOutUcastPkts` + `ifOutNUcastPkts`) respectively.

How does Intermapper compute Utilization for a link?

Intermapper queries a device at specified intervals, and requests a number of SNMP MIB variables. To compute utilization, Intermapper does the following:

1. It queries `ifInOctets` (and `ifOutOctets`) and the `sysUpTime` and `ifSpeed` variables.
2. It subtracts the octet counts from successive samples, and divides by the difference in the `sysUpTime` samples to compute a byte/second rate.
3. It divides the result by the `ifSpeed` variable to compute a percentage of the link's capacity/bandwidth. (If the user has overridden the `ifSpeed` variable, Intermapper uses the user-entered value.)
4. If a network is using a shared baseband link (such as Ethernet, wireless, etc.) Intermapper compares the sum of the transmitted and received bytes/second against the link speed to get the utilization.
If it's a full-duplex link (such as a frame relay, T-1 or T3, ATM, etc.) then Intermapper compares the higher of the transmitted or received data rate against the link speed.

How does Intermapper compute errors for a link?

Q:

"I see the Received Discards/Minute and Percent Err values for an ATM AAL5 interface are non-zero and I would like to know which variables were used, and what calculation was used to arrive at these numbers.

"We are also graphing the Percent Err: value. This figure is showing errors and my Cisco support folks wanted to know which MIB variables go into the calculation of this percentage and how they are combined to create this number."

A: The Percent Err values are computed as follows:

The one-way percent errors under the Receive section are computed by totalling { ifInUcastPkts, ifInNUcastPkts, ifInErrors, ifInDiscards } as follows:

```
PERCENT ERROR = totalErrors / totalPkts;
```

where:

```
totalErrors = dErrs + dDis and
totalPkts = dUcast + dNUcast + totalErrors
```

and:

```
dUcast = ifCurrStats.inUcastPkts - ifPrevStats.inUcastPkts
dNUcast = ifCurrStats.inNUcastPkts - ifPrevStats.inNUcastPkts
dErrs = ifCurrStats.inErrors - ifPrevStats.inErrors
dDis = ifCurrStats.inDiscards - ifPrevStats.inDiscards
```

NOTE: You can force the dErrs or dDis values to zero if you have IgnoreInterface Errors or Ignore Interface Discards selected.

The one-way percent errors for outgoing traffic are similarly computed from the { ifOutUcastPkts, ifOutNUcastPkts, ifOutErrors, ifOutDiscards } statistics.

The two-way Percent error number (just below Utilization on the Interface information menu) is the probability given both one-way error percentages that a packet will be lost making the round-trip across the link and back. If the probability of successful transmission is T and the probability of successful receipt is R (and assuming the act of transmission and receive are relatively independent), then the probability of a successful round-trip is $T * R$. The probability of error is $(1 - T * R)$.

T and R are computed from the complement of the one-way percent errors above.

Why can't I get a DHCP probe on OSX to work?

When running Intermapper on macOS, disable DHCP and PPP and assign a manually assigned static address to the computer running Intermapper.

To disable DHCP and PPP for all interfaces:

1. Open the **Network** settings in the **System Preferences** application.
2. From the **Show** menu, select **Network Port Configurations**.
3. Disable any ports that have been configured to use DHCP or PPP, even if nothing is plugged into them and they aren't currently being used.
4. If DHCP or PPP is enabled on any interface of your machine, the process "configd" will open UDP port 68, and prevent Intermapper from using it. You can use the Terminal application to test if configd has port 68 open. Type `'sudo lsof -i | grep bootpc'` and press return. If configd is listed, you still have DHCP running.
5. If Intermapper still marks the device as down after making these changes, you may need to use a DHCP Message Type of "DHCP-Discover" instead of the default "DHCP-Inform". This setting can be toggled in the DHCP/Bootp probe parameters dialog.

If I look at the traffic on a link, wait five seconds, and look again, the traffic rates are the same. Shouldn't these numbers be updated?

The traffic statistics are samples: the numbers do not change until after Intermapper probes the device again.

How does Intermapper compute byte and packet rates?

SNMP only supplies counts of bytes, packets, or errors, etc. that have passed through or occurred in an interface. These counts increment "forever" (or until the counter rolls over to zero like a car's odometer).

During each poll, Intermapper collects the total traffic and computes the difference with the total traffic from the previous poll. It then divides by the amount of time that has passed to compute the rate (per second or per minute).

Technical note: Even when a counter rolls over (e.g., from 999 to 000), Intermapper will compute the traffic rates accurately. Let's say the two successive samples are 995 and 003. Intermapper subtracts the previous count (995) from the new count (003), assumes that the "003" is actually "1003", and gets the proper difference of 8. Although the counters in the SNMP MIB variable are binary numbers, the same arithmetic principles hold. Thus Intermapper can compute these rates accurately.

How does Intermapper compute time intervals?

To compute the elapsed time accurately, Intermapper uses the `sysUpTime` variable of the device as a timestamp to calculate the time that has elapsed between subsequent two polls. The time elapsed should roughly correspond to the poll interval; however, it is possible for polls to be delayed occasionally so using the change in `sysUpTime` to measure the elapsed time is more accurate.

Configuring Intermapper DataCenter

Intermapper DataCenter is installed automatically when you install Intermapper.

NOTE:

Unless you want to do one of the following, you do not to take any of the steps described in this topic,

- To install and run Intermapper DataCenter from another machine.
- To specify an outgoing email server for error and bug reporting.
- To change the logging setup.

To open the Intermapper DataCenter web UI:

- From the **Reports Server** pane of Intermapper's **Server Settings** window, click **Configure**
- Navigate to the following URL:

<https://127.0.0.1:8182/>

NOTE:

If this is a fresh installation, Intermapper DataCenter automatically generates an SSL certificate, used to encrypt communication with your browser and the Intermapper server. Because a new certificate is generated for every installation, the certificate cannot be signed by a recognized certificate authority. As a result, your browser may display a message alerting you to an invalid certificate. To avoid seeing the message in the future, choose the option to continue, and tell your browser to add the certificate to its list of trusted certificates. In some browsers, including Firefox, you may need to click a link on the warning page and use a separate pane to add an exception for the certificate.

You can replace the generated certificate with one of your own by visiting the Services List. Click the Change Settings link for the Intermapper DataCenter Daemon, once initial setup is complete.

Setting the Password for the Admin Account

Before you can use Intermapper DataCenter from another machine, you must set the password for the Intermapper DataCenter admin account.

To set the password for the Intermapper DataCenter admin account:

1. Click the **Settings** tab.
2. In the **Username** text box, type a username. The default username is admin.
3. In the **Password** text box, type a password.
4. In the **Confirm Password** text box, re-enter the password.
5. Click **Save Settings** at the bottom of the page.

NOTE:

By default, you can log in to Intermapper DataCenter from the machine it is installed on without any authentication. You can force authentication even on the local machine by clearing the Skip authentication for local connections check box and creating a password as described above.

If you are planning to use an existing database, you are now ready to [configure it \(Pg. 607\)](#). If you are planning to use [Intermapper Authentication Server \(Pg. 613\)](#), you are also ready to configure it now.

Setting Up Intermapper DataCenter Logging and Event Collection

Intermapper DataCenter can log status information, connection attempts by Intermapper servers, and error information obtained when connecting to directory services. Intermapper DataCenter logs to a file called *log/imdc.log* within the IMDC install folder. For the location of the log file for your platform, see [Intermapper Files and Folders](#).

To set the logging level:

1. Click **Log** in the upper-left corner of the page. The Log Viewer is displayed.
2. From the **Logging Level** menu, select the level you want to use.
3. Click **Save**. The Intermapper DataCenter installation is complete.

Setting up Intermapper DataCenter's Error Reporting

Intermapper DataCenter can report problems and send bug reports to Intermapper Support. To do this, you need to specify one or more SMTP hosts and user information.

To set up error reporting:

1. In the Intermapper **DataCenter** section of the Intermapper **DataCenter home page**, click the **Settings** tab. The DataCenter Settings page is displayed.
2. In the **Primary SMTP** section of the **Error Reporting** section, enter a **Host** and **Port** (if different from the default), a valid **Username** and **Password** for the email account you want to use to send messages, and a **From** address for the messages. Enter (optional) SMTP settings for a secondary SMTP host.
3. To send an E-mail notification when an error occurs in Intermapper DataCenter, select the **On errors, send E-mail to** check box.
4. To send an email notification to Fortra when an error occurs, click to select the **Automatically E-mail bug reports to Help/Systems** check box.
5. To test your SMTP connection, click **Send Test E-mail**. A test email message is sent to the specified address.

Using an Existing Database

Intermapper makes it easy to install and run Intermapper Reports Server using the built-in PostgreSQL database. The database is installed, configured, and registered automatically. To use Intermapper Reports Server, you need only to start the server so that Intermapper reports to it.

If you prefer, you can use another instance of a PostgreSQL database, running on the same machine or on another machine. See [Configuring the Database](#) below.

Configuring the Database

Use this section only if you want to use an existing PostgreSQL database, regardless of whether it is running on the same machine as Intermapper or on a different machine.



InterMapper Database

Status: **not yet configured**

Click **Configure** to set up the connection to the database.

[Configure](#)

Use the Intermapper Database section of the Intermapper DataCenter Administration Panel to configure the Intermapper Database used by the Reports Server.

Configuring a New Installation

When configuring a new installation, follow these steps.

1. Configure database to connect to, or use the default Built-in database.
2. Register your Intermapper Server with the Intermapper Reports server.

Step 1: Database Configuration

1. Specify whether to use the Built-in database, or to connect to an existing external (PostgreSQL) database.
2. If you use the **Built-in** database, an *Intermapper* account is created automatically for Intermapper to use, so you can click **Continue** without adding any additional accounts. You have the option to create one or more user accounts when the database is installed.

You will need an additional user account if you want to use pgAdmin, Perl, PHP, Crystal Reports, or some other method to retrieve information from Intermapper Reports Server. If you want, you can add them later.

3. If you choose to use an existing database, enter a **Host**, **Port**, **Database Name**, **Database Username**, and **Database Password** in the appropriate boxes and click **Continue**. You are finished with Step 1.

NOTE:

The user you specify must have, at minimum, CREATE, TEMPORARY, and CONNECT privileges in order for Intermapper to log data to the database.

4. Click **Add** to add a user. An unnamed user is displayed in the User List at left.
5. In the **Username** text box, type a user name.
6. In the **Password** and **Confirm Password** text boxes, type the password.

7. Select or clear the **Write Access** check box to specify whether a user can make changes to tables (as through pgAdmin).
8. By default, users can access the database only from the same host as it is running on. Select or clear the **Remote Login** check box to choose whether to grant a user access from any machine on the network.
9. To create more users, repeat steps 4 through 8.

Step 2: Register your Intermapper Server with the Intermapper Database server

1. If Intermapper Reports detects an Intermapper server running on the same machine, you are given the option to register that server to export data to the Intermapper Reports Server.
 - a. Click **Register Server**. The existing server is registered with Intermapper Reports Server, and you are presented with the option of registering additional servers.
 - b. Click **Instructions**, and follow the instructions for each Intermapper server you want to register.
 - c. Click **Finish**. The Intermapper DataCenter home page appears, showing that the Intermapper Reports Server is running.

If Intermapper Reports Server is installed on a different machine, you'll need to register your Intermapper server(s) manually. Click **Register Server Manually**.

2. In Intermapper, view the Server Configuration > Reports Server pane of the Server Settings panel, click **Start**. Intermapper begins sending data to Intermapper DataCenter.

Changing Settings After Installation

Intermapper DataCenter is installed automatically when you install Intermapper. Once you have configured Intermapper Database, you can change settings as needed from the Intermapper DataCenter Administration Panel.

To change the settings in the Intermapper Database:

From the Intermapper DataCenter's Home page, click **Change Settings** in the Intermapper Database box. The Intermapper Database Settings Page appears.

To view the Intermapper Database log:

In the Intermapper Database section of the DataCenter Administration Panel, click the **Log** tab. The Intermapper Database log page appears.

Retention Policies

You can use data retention policies to average raw data, reducing the amount of data stored. Data retention policies control how often and how much data is averaged, and reduced.

A data retention policy can be applied to a specific map, to one or more devices or interfaces on a map, to an individual dataset, or to all maps on an Intermapper Server. Policies also affect the way Intermapper stores chart data.

Using Data Retention Policies

Use the Retention Policies pane of the Server Preferences section of the Server Settings window to create and edit retention policies that can be used to specify how data is stored for a particular device or map. For more information, see [Retention Policies](#).

Configuring Intermapper Database Logging Preferences

Use the Intermapper DataCenter's Log tab to view recent log entries, to set the level of logging you want to the Intermapper Database to use, and to set preferences for the Log tab.

To change the settings of the Service Log File page:

Make the changes you want, and click **Save Settings**.

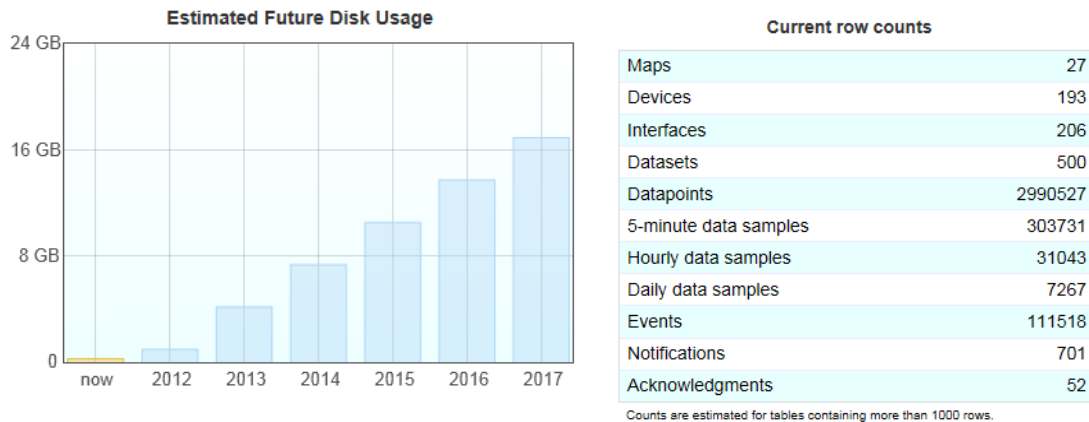
Log Levels

From the Logging Level menu, choose the logging level you want to use, as follows:

- **Full Debug** - logs minor details such as values read from configuration files and chunks of data arriving as part of directory responses.
- **Connections** (default) - logs authentication attempts, connections by the Intermapper server, and outgoing data.
- **Information** -logs web admin panel logins, changes to configuration and scheduled server tasks.
- **Errors Only** - logs only serious errors, indications of future errors, and possible security problems.

Reviewing Database Disk Usage

You can view disk usage statistics from the Intermapper Database's Overview page. The following statistics are available:



How Statistics are Calculated

- Estimated future disk usage is calculated based on the number of devices, datasets, and how retention policies are configured.
- With the exception of **Datapoints**, each row count corresponds to a specific database table, and indicates the number of records in that table. For tables with more than 1000 rows, the value is estimated.
- **Datapoints** is an estimated value.

To view database disk usage statistics:

From the Intermapper DataCenter's **Home** tab, click **Overview**. The Overview page is displayed, showing disk usage statistics.

Configuring Automatic Database Backups

Intermapper Database can automatically create back-ups of its built-in database. Please keep in mind that creating a backup can consume a lot of disk space, and takes time to complete.

To set up automatic backups:

1. From the Intermapper **Database Settings** page, click **Automatic Backups**. The Automatic Database Backups page appears.
2. Set the period you want to use for backing up. You can do backups daily or weekly.

3. For daily backups, set the time you want the backup to start. For weekly backups, set the day and time.
4. Specify the maximum number of backups you want to store. After this number of backups is reached, the oldest backup is deleted each time a new one is created.
5. Click **Save Settings**. The backup settings are saved, and backups are created according to the specified schedule.

Creating an Unscheduled Backup

You can create a backup at any time.

To create a backup:

Click **Create Backup**. A new backup file is created immediately. The backup starts immediately. When finished, the backup file is listed in the **Available Backups** list.

Restoring a Previous Backup

You can restore a previous backup.

To restore a previous backup:

1. From the **Available Backups** list, click the backup file you want to restore.
2. Click **Restore**. Data from the selected backup is restored to the Intermapper database.

Viewing Backup Progress and Canceling Backups

When a backup is underway, you can view its progress from the Automatic Database Backups page. You can also cancel a backup while it is under way.

To view backup progress or cancel a backup:

- While the backup is under way, go to the **Automatic Database Backups** page. The progress bar is displayed.
- Click **Abort** to cancel the current backup.

Performing Maintenance Tasks

You can use the Maintenance Tasks page to perform these maintenance tasks.

- **Pause Operations** - Sometimes it can be useful to pause import, without stopping the database entirely. This allows you to manually re-cluster or re-index tables, or avoid errors when the Intermapper Server goes down for maintenance. Specify the interval for which you want to pause, then click **Pause Operations**. A Resume Operations button and countdown clock appear. To resume operations at any time, click **Resume Operations**.
- **Data to Delete** - Data retention policies are the recommended way to free disk space on a per-dataset basis. You can also delete data or events across all devices, or you can delete data for deleted devices and interfaces. Please be aware that this operation is permanent and cannot be undone. Specify which data you want to delete (raw data, data samples, events, or data from deleted devices), and a time period over which you want to delete them, then click **Delete**.
- **Apply Retention Policies and Reclaim Disk Space**- Retention policies are applied daily, and a maintenance task runs once each week to reclaim unused disk space. You can run both of these tasks manually using these buttons. Both operations can take from a few minutes to a few hours to complete, depending on the size of your database. See [About Automatic Maintenance Tasks](#) below for more information.

Two tasks run automatically to clear out data that is beyond its retention policy expiration, and to reclaim unused disk space.

- **Daily task** - runs at 1AM local time each day. It applies retention policies, then uses the PostgreSQL VACUUM command to mark free space for re-use by the database. This is a relatively low-impact process, and does not pause database operations. It does not release disk space for reuse by the operating system.
- **Weekly task** - runs at 1AM local time each Sunday. It uses the PostgreSQL CLUSTER command, and pauses database operations while it runs. This task frees up unused database space, making it available to the operating system.

After you run one of these tasks, the Disk Usage table shows the freed disk space as available.

Using the Intermapper Authentication Server

Use the Intermapper Authentication Server to authenticate Intermapper users through an external authentication directory.

The Intermapper Authentication Server (IMAuth) is a component of the Intermapper DataCenter (IMDC) add-on package. It lets an Intermapper server authenticate users

against an external authentication directory. IMAuth supports LDAP, RADIUS, ActiveDirectory, IAS, and Kerberos directories.

IMAuth acts as an intermediary between an Intermapper server and the directory. If an authentication request comes in from a user whose password is not in Intermapper's local user database, the Intermapper server forwards that request to IMAuth. IMAuth translates and passes the request to the directory server, and forwards any responses it receives back to the Intermapper server. In addition, a new user entry is created in the local database, configured for external authentication and assigned to a default group you will have specified for users created this way.

IMAuth is not a replacement for Intermapper's local user database. You may continue to keep some user passwords in Intermapper's local user database for local authentication while requiring others to be authenticated via IMAuth. For each user, you must choose one method or the other.

Select the "Use External Authentication" check box in the **Edit User** or **Create User** dialog to indicate that the user should be authenticated via IMAuth, in which case you should not supply a password. For more information on creating and editing users, see [Users and Groups \(Pg. 272\)](#).

Installing the Authentication Server

Intermapper Authentication Server runs as a component of Intermapper DataCenter and is installed automatically when you install Intermapper.

Configuring and Connecting to Your Directory

You need to configure the Intermapper Authentication Server to talk to your directory server. This is done from Intermapper DataCenter's web administration page. To do this, start IMAuth Server as described above, then open a web browser and navigate to: <https://localhost:8182>. You can also click Configure in the Reports Server pane of the Server Settings window.

1. Configure the connection to your authentication directory (LDAP, Radius, ActiveDirectory, Microsoft IAS, or Kerberos v5).
2. Configure the connection that an Intermapper server uses to connect to IMAuth.
3. Configure Intermapper to connect to IMAuth.

Tips and Hints for Various Authentication/Directory Servers

RADIUS/IAS

IMAuth acts as a RADIUS client, and so it must be added to the clients section of your RADIUS configuration file or, for Microsoft IAS, the clients section of the IAS configuration pane. You are asked to specify a *secret*, and must then enter exactly the same secret in the IMAuth RADIUS settings.

LDAP

You can authenticate with LDAP using port 389 with or without SSL. To connect with LDAP on port 389 with a plaintext connection, leave the *Use SSL* checkbox unchecked. To connect with LDAP on port 389 with an encrypted connection, select the *Use SSL* checkbox.

You can authenticate with LDAP on port 636, which is an encrypted connection by default. This means the *Use SSL* checkbox has no effect when using port 636.

NOTE: In a future version of Intermapper, the *Use SSL* checkbox will be disabled when port 636 is being used for LDAP authentication.

If you encounter any problems, first try clearing the *Use SSL* checkbox, or choose *Whenever Necessary* for the *Use Plaintext* option in the IMAuth LDAP settings. If this works, it means your server wasn't built to include SSL or SASL DIGEST-MD5 password encryption. You'll need to either stay with the lower IMAuth security settings, or upgrade your LDAP server.

Another thing to look at is the LDAP Base DN specified in the IMAuth LDAP settings. This tells IMAuth where in your LDAP directory the user entries are located. This depends on how your directory was set up, but usually takes the form:

`ou=people,dc=example,dc=com`, where *example* and *com* correspond to the domain name your directory was set up with. IMAuth takes the Base DN and attaches the user's name; for example,
`cn=Jane,cn=Smith,ou=people,dc=example,dc=com`.

ActiveDirectory

ActiveDirectory is based on LDAP, but differs slightly in its default configuration. If you are encountering problems with these ActiveDirectory versions, try clearing the *Use SSL* checkbox or choosing *Whenever Necessary* for the *Use Plaintext* option in the IMAuth LDAP settings. The Base DN for an ActiveDirectory server will almost always be: `cn=Users,dc=example,dc=com` where *example* and *com* are replaced by the name of the Windows Domain that ActiveDirectory is serving.

Since ActiveDirectory is built around the idea of domains rather than single servers, the username you use to authenticate must have your domain name attached to it. For example, if your normal Windows logon name is *jan smith* and your domain is

example.com, the username you give when accessing a map with Intermapper or Intermapper Remote Access is janesmith@example.com.

Almost all ActiveDirectory versions support SSL. If you have provided your own certificate, choosing the *Whenever Necessary* option for the Use Plaintext field in the IMAuth LDAP settings doesn't have much impact on your security. If you really do need the additional encryption, you must perform these steps:

1. Log in to your server as an administrator, and start the **Active Directory Users and Computers** panel.
2. Open the properties for each user who needs to authenticate, and switch to the **Account** tab.
3. Under **Account options**, select the **Store password using reversible encryption** check box.

NOTE: Microsoft Windows cannot apply the change immediately, so you must get that user to log on to the Windows domain as normal (by signing on to their machine, for example) before the change becomes active.

In this case you might again need to use a different username. Instead of the usual login name, you may need to use the user's full name. For example, instead of janesmith you would use Jane M. Smith.

When setting up IMAuth, it's a good idea to try the normal login name, the login name with your domain attached, and the user's full name, to see which login your ActiveDirectory server accepts.

Kerberos

For a good introduction to Kerberos, see the following Knowledgebase article:

- [Using Kerberos with Intermapper](#)
- [Supported Kerberos encryption modes](#)

Problems encountered when using Kerberos are usually caused by misconfiguring the Intermapper Authentication Server, or by the values used when creating the `imauth` service account.

- **Kerberos Domain** - The name, of the Kerberos authentication realm. It is typically all uppercase (Example: `Intermapper.COM`). On Windows, it is almost always the same as the ActiveDirectory domain's name, but upper-cased.

- **KeyServer Address** - The full domain name of the Kerberos key server. On Windows, even on complex networks with multiple ActiveDirectory nodes, only one acts as the Key Distribution Center. The KeyServer Address value must match the machine's name *exactly*. For example, if the machine is registered on the network as `ad.Intermapper.com`, the **KeyServer Address** must be `'ad.Intermapper.com'`; entering the IP address of the machine, or just `'ad'`, causes authentication failures.
- **Service Principal** - The service principal name associated with IMAuth on the domain. This is typically the service name (`imauth`) followed by a forward slash and then the Kerberos key server's full domain name. For example, on Windows, assuming you follow the instructions in the Knowledgebase link above, and created an ActiveDirectory service account called `'imauth'`, the Service Principal value would be `'imauth/ad.Intermapper.com'`. This user account *must also be active* in ActiveDirectory; disabling the account is a common mistake that causes authentication failures.

Data Collecting and Reporting

You can use the Intermapper Reports Server to collect data you can use for analysis and to create custom reports.

Intermapper Reports Server is a module of Intermapper DataCenter. [Intermapper DataCenter \(Pg. 605\)](#) is installed automatically when you install Intermapper Server on Microsoft Windows and macOS. It is a separate download on other platforms.

Use the Reports Server panel, available from the Server Configuration section of the Server Settings panel, to start and stop collecting data. You can also configure Intermapper to connect to a remote database server, and specify the intervals at which data is stored. For more information, see [Reports Server \(Pg. 255\)](#).

Collecting Data for a Device or Interface

You can collect data for any device in any map. Use the Set Data Retention command, available from the Monitor menu or the device or interface's **Set Info** context menu to specify how long the data from the device or interface is retained, and at what resolution.

The default server-wide Data Retention Policy is 24 Hours (except for devices and interfaces associated with charts created in 4.6 or earlier). You can also create and select a different retention policy as the server-wide default policy:

- For all maps, select **Inherit** to use the specified server-wide default policy, as set in the Server Settings window. You can also specify a default Data Retention policy for a map that is different from the server's default policy.

- For all devices, select **Inherit** to use the specified map-wide default policy, as set in the Map Settings window. You can also specify a default Data Retention policy for a device that is different from the map's default policy.
- For all interfaces, select **Inherit** to use the specified device policy, as set in the Device Info window. You can also specify a default Data Retention policy for an interface that is different from the device's policy.
- For devices and interfaces associated with charts created in 4.6, the default Data Retention policy is **IM46Charts**.
- If you do none of the above, the default server-wide policy is applied automatically.

NOTE:

Data Retention Policies are applied individually, not in sequence. For example, specifying an hourly data expiration of two days now causes hourly samples to be deleted after two days, instead of two days plus the raw and custom expirations.

Retention Policies in Status and Info Windows

A device or interface's current Retention Policy is shown in the Status and Info windows. In the Status window, the information appears as follows:

Retention Policy: PolicyName, [Not] Exportable

- **Policy** - the policy name as created in Intermapper Reports server.
- **Exportable/Not Exportable**
 - **Exportable** is displayed if the parameters of the policy are such that they cause data to be exported to the database.
 - **Not Exportable** is displayed if the parameters of the policy are such that they will not cause data to be exported to the database (the None policy, for instance).

Getting Data From the Database

The Reports Server is the easiest way to get data from the Reports Server database, but you can use your own method for retrieving data from the Intermapper Database using SQL queries. There are several example reports written for Crystal Reports and OpenRPT, as well as several perl scripts available. For more information, see *Retrieving Data From the Intermapper Reports Server* in the Developer Guide.

Intermapper Files and Folders

Intermapper saves its files in specific folders. In particular, the following file and folders have special locations:

- **The Intermapper application folder** - If applicable, it contains the actual Intermapper Application.
- **The Intermapper Remote Access application folder** - If applicable, it contains the actual Intermapper Application.
- **The Intermapper Settings folder** - Contains all Intermapper server settings file as well as several folders containing various information used by Intermapper. For detailed information its contents, see [Intermapper Settings \(Pg. 622\)](#).
- **The Intermapper DataCenter folder** - contains the data storage for all installed components of Intermapper DataCenter, as well as a number of other files. For detailed information on the contents of the Intermapper DataCenter folder, see [Intermapper DataCenter Folder](#).
- **The Intermapper Flows folder** - contains data storage for Flows data as well as a number of other files.

File Locations

The locations of these files and folders differ slightly between operating systems as described below.

Intermapper Application Folder

OS	Location of Intermapper Application files
Windows 32 & 64-bit	C:\Program Files\Intermapper or specified location.
macOS	Binary files (Intermapperd, Intermapperauthd) are placed in /usr/local/bin, unless a different location was chosen at installation.
Linux	Binary files (Intermapperd, Intermapperauthd) are placed in /usr/local/bin, unless a different location was chosen at installation.

Intermapper Settings Folder

For detailed information on the contents of the Intermapper Settings folder, see [Intermapper Settings](#).

OS	Location of Intermapper Settings files
Windows	C:\ProgramData\Intermapper\InterMapper Settings or specified location.
macOS	As specified in /etc/Intermapperd.conf (Usually /Library/Application Support/InterMapper Settings/)
Linux	As specified in Intermapperd.conf (Usually /var/opt/helpsystems/intermapper/InterMapper_Settings)

Intermapper Remote Access Application Folder

OS	Location of Intermapper Remote Access files
Windows 32-bit	C:\Program Files\Intermapper RemoteAccess
Windows 64-bit	C:\Program Files (x86)\Intermapper RemoteAccess
macOS	Drag and drop to location of your choice.
Linux	Installed at location where .bin file is run.

Intermapper DataCenter Folder

For detailed information on the contents of the Intermapper DataCenter folder, see [Intermapper DataCenter Folder](#).

OS	Location of Intermapper DataCenter files
Windows 32 and 64-bit	C:\Program Files\Intermapper\dwf
macOS and Linux	/usr/local/imdc

Intermapper Flows Folder

OS	Location of Intermapper Flows files
Windows 32 & 64 bit	<ul style="list-style-type: none"> (Flows files) C:\Program Files\Intermapper\flows (Database) C:\ProgramData\Intermapper\InterMapper Settings\Flows\SESSIONDB

macOS	<ul style="list-style-type: none"> • (Flows configuration files) /Library/Application Support/InterMapper Settings/Flows • (Database) /Library/Application Support/InterMapper Settings/Flows/SESSIONDB • (Logs) /Library/Application Support/Intermapper Logs/flows-stderr.txt, flows-stdout.txt, flows.log
Linux	<ul style="list-style-type: none"> • (Flows files) /var/local/Intermapper_Settings/Flows • (Database) /var/local/Intermapper_Settings/Flows/SESSIONDB/

Creating Backups

Intermapper saves its state the in Intermapper Settings folder.

As described in [Intermapper Files and Folders](#), the Intermapper Settings folder is in different locations, depending on whether it is installed in Microsoft Windows, Linux, or macOS.

To backup Intermapper on any of these systems:

Back up the **Intermapper Settings** folder.

Note: When making backups of the Intermapper Settings folder on Microsoft Windows installations, it is important to stop the Intermapper Server before making a backup, or make sure that your backup mechanism allows files to be accessible by Intermapper simultaneously. Opening certain types of chart or log files can cause them to be inaccessible to Intermapper, causing the Intermapper Server to stop abruptly.

Retaining Copies of Maps in Older Formats

A new version of Intermapper can use a file data structure which is different from previous versions. To preserve the ability to "go back" to an earlier version, Intermapper creates a copy of the current maps when you install a new version of Intermapper, named with the new version number. This becomes the copy that contains active maps.

The old maps are moved to a folder named with the previous version number. If you need to revert to an earlier version of Intermapper, you can get your original maps from the folder whose name corresponds with the version you want to run. In subsequent releases, the folder that corresponds to the current version is used automatically.

Intermapper Settings Folder

The Intermapper Settings folder contains all the settings, preferences, and configuration of Intermapper. The location of this folder varies, depending on your platform. For more information, see [Files and Folders \(Pg. 618\)](#).

The Intermapper Settings folder contains the following items:

- **Certificates folder** - Contains certificates used by secure servers to verify that they are the Intermapper servers they claim to be. Also contains key files and pending certificate signing requests.
- **Chart Data folder** - Contains the saved data of charts. When Intermapper starts up, it reads the data from these files to restore the charts' history.
- **Custom Icons folder** - Contains custom icons you add to maps to enhance Intermapper's built-in icon set. See [Custom Icons \(Pg. 81\)](#) for details about making and adding custom icons.
- **Intermapper Logs folder** - Contains text files that log events that Intermapper has detected.
- **Intermapper Prefs file** - Contains the current settings of all Intermapper preferences.
- **Maps folder** - Contains maps saved from Intermapper. All maps in this folder are opened automatically when you start Intermapper.
 - **[Version Number] folder** - For each version of Intermapper that has been installed, (starting with 5.4) a new folder is created for each version. Maps from a previous version are copied into the new folder, which becomes the active maps folder. The folder for each new version contains a Disabled folder and a Deleted folder.

- **Enabled folder** - Contains maps that have been disabled by removing the check mark in the Map Files panel of the Server Settings window.
- **Disabled folder** - Contains maps that have been disabled by removing the check mark in the Map Files panel of the Server Settings window.
- **Deleted folder** - Contains maps that have been removed using the Map Files panel of the Server Settings window.
- **Backups folder** - Contains backups created using the Backup command.
- **MIB Files folder** - Contains SNMP MIB files that ship with the product, or have been added using the **Import > MIB...** command. Intermapper parses the MIB files in this folder and uses the information to convert between variable names and OIDs.
- **Probes folder** - Contains built-in and custom probes. Probes are text files that add functionality to Intermapper so that it can test new devices. See Customizing Intermapper's Probes for details about creating and customizing probes.

NOTE:

Built-in probes are stored in a ZIP archive named BuiltinProbes.zip. To view or modify a built-in probe, you'll need to unzip the archive. Intermapper scans the archive as well as the unzipped contents of the folder. If a built-in probe's filename matches an unzipped version, the probe's version number, then the last-modified date, is used to determine which probe is the most recent. If you are developing or modifying a built-in probe, be sure to advance the version number to be sure that Intermapper uses the modified version.

- **Sounds folder** - Add .aiff, .wav, and other sound files to this folder to make them available for Intermapper notifications. For more information on sounds and how to use them, see [Configuring a Sound Notifier \(Pg. 120\)](#)
- **Web Pages folder** - Contains the template and target files that describe the web pages that the Intermapper server displays. See Customizing Web Pages for details about customizing these pages.
- **Intermapper User List folder** - Previous versions of Intermapper kept the user list in a separate file. Now, these user and group settings have been incorporated into the Intermapper Prefs file. You may leave this file in place without affecting Intermapper's operation.
- **Tools folder** - Contains executable files (or aliases/links/shortcuts to them) that will be used as command-line probes or notifiers.
- **Fonts folder** - (optional) Contains TrueType fonts used by the web server.

Note: On Microsoft Windows machines, the Microsoft Windows font directory is

also available, giving access to all available TrueType fonts installed on the machine. On macOS, Intermapper looks in /Library/Fonts and /System/Library/Fonts, as well as in the /InterMapper Settings/Fonts folder.

- **Temporary folder** - When files are uploaded, they are initially uploaded and saved into this directory until the upload is complete. At that point, they are moved into a more appropriate directory. If something goes wrong, and an upload is interrupted, a file may remain in the Temporary directory.

When you exit Intermapper, it leaves the files in the Temporary directory alone, so debugging information can be collected. When Intermapper starts up, it checks the Temporary directory, and deletes all files in it. Therefore, Intermapper users should not rely on the contents of the Temporary directory remaining long, and should not park files there.

- **ssl.conf.example file**

This is a text file that serves as a template for the Intermapper administrator to write a local SSL configuration file under the name of `ssl.conf`. In this file, blank lines are ignored. Lines where the first non-space character is a number sign (#) are comments and are also ignored.

The distributed (template) file `ssl.conf.example` consists of blank lines and comments that document the defaults.

To configure the SSL service with non-default settings values, copy the `ssl.conf.example` file to `ssl.conf` and add (or uncomment and modify) lines beginning with one of the following keywords respectively:

- protocols
- ciphers
- options

After creating or modifying the `ssl.conf` file, restart the Intermapper service processes for the change to take effect.

Intermapper DataCenter Folder

The Intermapper DataCenter folder, named `dwc` on Windows systems and `imdc` on macOS and Linux systems, contains a number of folders related to Intermapper DataCenter and its components. The folder location depends on the operating system. For more information, see [Intermapper Files and Folders](#).

Folders Common to All Platforms

All platforms contain the following folders:

- **config** - the database storage, including configuration information for Intermapper DataCenter and its components.
- **core** - the Intermapper-distributed versions of PostgreSQL and Python, as well as license information about used or distributed third-party products.
- **imauth** - Python objects, HTML, text, and so on, for the Intermapper Auth Server component.
- **imdatabase** - Python objects, HTML, text, and so on, for the Intermapper Database component.
- **imdc** - Python objects, HTML, text, and so on, common to all IMDC components and for the Intermapper DataCenter setup, configuration, and so on.
- **imreports** - Python objects, HTML, text, and so on, for the Intermapper Reports component.
- **log** - the logs for all Intermapper DataCenter components.

Platform-Specific Folders

macOS

The Mac platform also contains the following:

sbin - This contains a script used by `launchctl` to start and stop the Intermapper DataCenter daemon.

Linux

The Linux platform also contains the following:

sbin - This contains a script used by the platform's load daemon to start and stop the Intermapper DataCenter daemon, as well as assorted other scripts.

Importing and Exporting

Use Intermapper's import and export features when you need to manage, create or update maps, devices, users. Intermapper includes a rich set of features for controlling both [import](#) and [export](#) of data.

You can automate imports and exports through Intermapper's command-line interface, and you can even create data layers for maps that [use geographic coordinates](#) suitable for [viewing in Google Earth](#).

Importing and Exporting Maps

Exporting Data From Maps

Exporting, Servers, and Clients

When you use the Export commands to retrieve information, you are exporting from the Intermapper Server, and saving it using the Intermapper client. The client is either running on the same machine as the server, or you are using Intermapper Remote Access to connect to an Intermapper Server and retrieve the data.

Intermapper exports data about the devices on its maps.

Why Export?

The two Export commands are intended for different purposes:

- **Export Map** - creates a file containing a visual representation of the map. This includes Intermapper's native **.MAP** format, which includes all data associated with the devices on the map, which you can import to another Intermapper server.
- **Export Data** - creates a text-based file you can use for database-related activities. It contains data from fields you choose from selected tables associated with the selected maps, as well as tables that contain data not specific to maps or devices.

Export a map to retrieve a visual representation you can use for your purposes. You can do the following:

- Transfer a map to a different server in native **.MAP** format.
- Use a **PNG**, **SVG**, or **Visio** file in a presentation, marketing piece, or other use.

NOTE:

- SVG is supported on all platforms if you have a paid license versus a free or trial license.
- Visio files are supported if the client is on a Microsoft Windows system. To export maps to Visio, you must have the full version of Visio 2013 or higher installed.

- Send an image of a map to illustrate a problem you are troubleshooting.

Export data for use in database-related applications. For example,

- To review the map's configuration to check for consistency
- To edit the map data using some external tool, and then re-import it (using the [Import Command \(Pg. 631\)](#)) back into the map, updating the affected devices.
- To use the configuration in some down-stream application

NOTE: You can automate the exporting of map data by sending commands to Intermapper Remote Access through its command-line interface or through the HTTP API. This allows you to interact with Intermapper through your own scripts. For more information, see [Command-line options for Remote Access](#).

Exporting Maps

You can export maps in a number of formats, each intended to provide a visual representation of the map. When you export a map in native .MAP format, all the data associated with that map is saved. In all other formats, a visual representation of the map is created.

To export a map:

1. From the Export submenu, choose **Export Map**

This command is available as follows:

- From the **File** menu, when a map is selected in the Map List window.

NOTE:

Fortra recommends that you do not export too many maps to Visio at a time.

- From the **File** menu in any Map window.
- From a context menu when you right-click a map from the Map List or Device List window,

A standard File Save dialog appears.

2. From the **Files of type** menu, select one of the following file formats and click **Save**:

Type	Extension	Description
Map	.map	saves a copy of the map from the server on which it's running to a file on a local computer running Intermapper or IntermapperRemote Access.

PNG	.png	PNG - saves a PNG image of the current map. A standard File Save dialog appears.
SVG	.svg	SVG - creates a standard SVG (Scalable Vector Graphics) file (XML). For Linux systems, Fortra recommends that you do not use fonts that are larger than 20 pts because some font types are not rendered correctly in SVG files.
Visio	.vsdx	Visio - creates a file with a .VSDX extension that can be opened in Visio. NOTE: Visio files can be created only on Microsoft Windows systems with the full Visio 2013 or higher version installed. Exporting to Visio is not available if you are using a free or a trial license key.

Exporting Data

Save a text file containing information about a map, devices, interfaces, notifiers, or users, intended for use in database-related applications.

To export data:

1. From the File menu's Export submenu, select **Export Data**. A standard file dialog appears.
2. Choose a file name, location, and file output format as described in the table below. The Export Data window appears (also shown below).

From the **Table** menu, select **devices** (device attributes), **vertices** (appearance attributes), **maps**, **notifiers**, **notifierrules**, **users**, or **schema** (output file attributes).

NOTE: The schema file contains attributes of all the tables as described in the attribute topics listed above. As with the other export tables, you can specify the columns you want to export, as well as the order of the columns, as described in the following steps.

3. From the **Fields** area, click to choose the fields you want to export. *Shift-click* to select a contiguous series, or *Ctrl-click* to choose non-contiguous fields.
4. Click **Add**. The selected fields appear in the **Field Export Order** box. If you want to export all fields, click **Add All**.

5. In the **Field Export Order** box, drag the field names up or down to set the order you want the fields to appear in the export file.
6. Select **Export data from all maps** or **Export this map**.
7. If you want to export data only for the selected items on the map, click **Export selected items**.
8. From the **Output format** drop-down menu, choose one of the formats as described below.
9. Click **Export**. A standard File Save dialog is displayed.
10. Select a name and location for the export file and click **Save**. The export file is saved in the specified location.

Export the data in one of these formats:

Type	Extension	Description
TAB	TAB	Tab-delimited - creates a text file with all field data separated by tab characters.
XML	XML	XML - creates a text file containing field data in XML format.
HTML	HTML	HTML - creates a text file containing field data in HTML tables.
CSV	CSV	CSV - creates a text file with all field data separated by commas.
JSON	JSON	JSON - creates a text file containing field data in JSON (Javascript Object Notation)

Export Data from Selected Maps (2)

Table: devices

Fields:

- MapName
- MapPath
- Address
- Id
- Name
- Probe
- Comment
- Community

Field Export Order:

Buttons: Add >>, << Remove, Add All, Remove All

Export to: C:\HELP\SYS\MyExport.tab

☐ Export from all maps
☒ Export from selected maps (2)

Export Cancel

The following table shows the Intermapper tables you can export to data files in the selected format.

The Source column indicates whether the table contains information specific to the map or information specific to the server.

Table	Source	Description
Devices	Server	<p>Contains information about devices and their Device Attributes on page 649.</p> <p>If the ProbeXML field is included in the export, the ProbeXML D-Set for the specified notifier is included for each device on a selected map, as described in About D-Sets on page 674.</p>
Vertices	Map	<p>Contains information about the locations of devices on maps as described in Vertex Attributes on page 660</p> <p>Available only when a map is selected, either from the Map List window or from the Map Window.</p>
Interfaces	Map	<p>Contains information about Interfaces, as described in Interface Attributes on page 662</p> <p>Available only from the Map window.</p>
Maps	Server	Contains information about the maps on your server, as described in Map Attributes on page 667
Notifiers	Server	<p>Contains information about the Notifiers defined on your server, as described in Notifier Attributes on page 669.</p> <p>If the NotifierXML field is included in the export, the NotifierXML D-Set for the specified notifier is included for each notifier for each active notifier on a map, as described in About D-Sets on page 674.</p>
Notifier Rules	Server	Contains the rules for each notifier as described in Notifier Rules Attributes on page 670 .
Users	Server	Contains a list of users defined on your server as described in User Attributes on page 672 .
Schema	Server	Contains the information for each Attributes table described above.
Retention Policies	Server	Contains information about the retention policies defined on your system as described in Retention Policy Attributes on page 673 .

Importing Data

Intermapper can import data from a text file to update information about devices on a map, or information about Users or Groups. Some reasons you might want to import data:

- you want to import the devices/probe types from another monitoring system (or information that's already present in a spreadsheet or other format) into Intermapper.
- You make frequent updates to existing devices on maps.
- You frequently add new devices to maps. For example, you might want to enter information about new customers to a database, then export the new device information to a file that can be bulk-imported into Intermapper.
- You want to make systematic changes to your maps. You can export the Intermapper map as tab-delimited data, edit columns in a spreadsheet or database, then re-import, letting Intermapper merge the new information onto the existing devices. This is useful for wholesale label changes, switching IP addresses, etc.
- You want to import a list of users from another source for authentication purposes.

To import data:

1. Create an import file as described in [Creating an Import File \(Pg. 632\)](#).
2. In the Map List window, click to select the server to which you want to import map data, or open a map on that server.

NOTE: The import file contains the name of the map. If the map does not exist, it is created automatically.

3. From the File menu's **Imports** submenu, select **Data File**. A standard file dialog is displayed.
4. Select the file you want to import and click **Open**. If the map data is valid, devices are added or updated on the specified maps as appropriate. If the specified map does not exist, one is created automatically.

NOTE: You can automate the importing of map data by sending commands to Intermapper RemoteAccess through its command-line interface or through the HTTP API. This allows you to interact with Intermapper through your own scripts. For more information, see [Command-line options for Remote Access](#).

When importing data in Tab/CSV/XML formats, foreign characters must be presented in the same way as the output of the **Export** command:

- Characters with values less than 255 can be directly imported.
- Character values greater than 255 must be escaped using the standard XML format (`&#[character code]`).

Creating an Import File

Since a missing tab can cause errors in an import by causing data to be imported into the wrong fields, creating a file from scratch in a text editor is relatively error-prone. The following methods are recommended for creating import files quickly and accurately:

- [Export a map \(Pg. 625\)](#), then edit the file.
- [Use a spreadsheet application \(Pg. 633\)](#) such as Excel to create a tab-delimited file.
- Generate a file algorithmically from a database. This may be useful if you plan to update maps regularly.

An import file is text file, formatted as follows:

- **The first line of the file specifies the format of the following lines** - specifies the file format (tab in the example below), the table to be filled ("devices") and the order of the fields. Three fields must be specified: MapName, Address, and Probe; the remaining fields are optional.
- **Remaining lines contain the data for the devices you want to import** - each device occupies a single line, and the data columns are separated by tabs (a "tab-delimited" file.) Each column corresponds to a field in the **fields** specification of Line 1.

Line 1 - Specifying the Import File Data Format

The first line of the file determines the method you are going to use for importing, and can provide you with a significant amount of control over how devices are imported. There are two different methods you can use for importing; each uses a different format for the first line of the file:

- **Spreadsheet-style import** - This technique is used only for adding new devices to a map. The first line of the file contains the column names associated with the data in the remaining lines. This is the recommended method. Once you have created this file, it is easy to change the first line to a Directive line.
- **Directive line** - This method gives you a large amount of control over the import process. In addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them. This technique is documented in [Advanced Data Importing \(Pg. 643\)](#) in the References section.

NOTE:

- For either style of importing, data is set only in those fields whose Access value is specified as READ-WRITE in the Device Attributes and Vertex Attributes topics, found in the in [Advanced Data Importing \(Pg. 643\)](#) in the References section.
- Text files should be encoded in UTF8 format.
- Characters with values less than 255 can be imported directly.
- Character values greater than 255 must be escaped using the standard XML format (&#[character code]).

Spreadsheet-Style Import File

The recommended format for creating an import file is a spreadsheet style format, in which the first line contains tab-separated column names that correspond to the remaining rows:

```
LabelTemplate MapName Address
Machine1 Map1 192.0.0.1
Machine2 Map1 192.0.0.2
```

This is the equivalent of the following directive line, as explained below:

```
# format=tab table=devices fields=LabelTemplate,MapName,Address
insert=LabelTemplate,MapName,Address
Machine1 Map1 192.0.0.1
Machine2 Map1 192.0.0.2
```

NOTE:

- If you created a spreadsheet-style import file, you can easily change it to a *Directive line-based* file for updating the map.
- You can include columns in your import file from both the Device and Vertices tables. Intermapper automatically applies the Vertex attributes appropriately.

The columns are imported in the order specified. The last value specified takes precedence over previous values in the same line. Because of this, Help/Systems recommends that you use only one the following columns when importing. If more than one of these is specified, and there are conflicts, the last column's values are used:

- **Address**
- **DNSName**
- **IMProbe**

For a complete list of device attributes and corresponding field names, see Device Attributes in Advanced Data Importing [\(Pg. 643\)](#) in the References section.

Directive-Line

Using the Directive Line technique, in addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them. This technique is documented in [Advanced Data Importing \(Pg. 643\)](#) in the References section.

Using Geographic Coordinates

You can use geographic Latitude and Longitude coordinates to place devices on your map. This can be useful if you have many devices at different locations. The procedure is relatively simple:

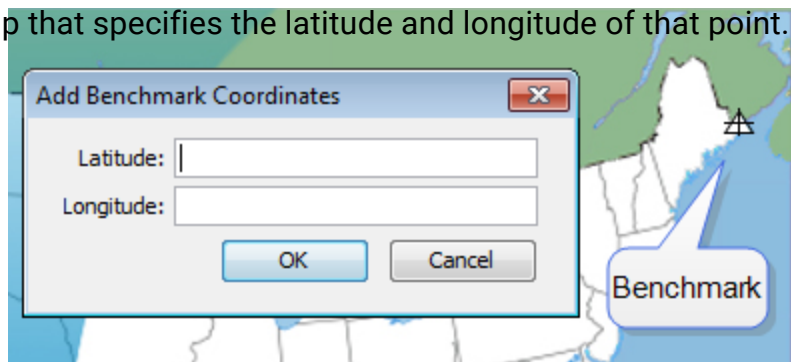
1. Create a new map on which you want to place the devices.
2. Obtain a map image you want to use as the background for the map. You can scan your own map to create the image, or get one from one of the sites listed below. Intermapper can import image files in PNG, JPEG, or GIF format.
3. Set the image as the background for your map as described in [Background Images \(Pg. 84\)](#).
4. Set *benchmarks* in the map as described below. This sets the relationship between your map image and real geographic coordinates.
5. Create a text file containing a list of your devices with their IP addresses and Latitude and Longitude coordinates. You can specify many other parameters for each device within this file as well. For more information, see [Importing Data Into Maps \(Pg. 631\)](#). A sample data file is shown below, containing geographic coordinates.
6. Import the text file. The devices appear at the correct location on the map.

Setting Benchmarks in Your Map

A benchmark is an icon on a map that specifies the latitude and longitude of that point. Intermapper uses the benchmarks to determine the proper location for icons on the map.

To place a benchmark on a map:

1. Right-click (CTRL-click) a known location (on for which you know the actual latitude and longitude) in the map's background image and choose **Add benchmark**. The Add Benchmark Coordinates window appears.
2. Enter the latitude and longitude for the point. A small triangular icon appears to represent the benchmark. Intermapper supports multiple formats for latitude and longitude. (See below)
3. Follow steps 1 and 2 to enter a second benchmark to complete the geographic information. Your map is now ready for you to import devices with specified geographic coordinates.



To remove a benchmark on a map:

- Right-click (CTRL-click) an existing benchmark, choose **Remove benchmark**. The benchmark disappears from the map.

To remove both benchmarks from a map:

- Right-click (CTRL-click) anywhere in the map's background image and choose **Clear benchmarks**. Both benchmarks are removed from the map.

Accepted Geographic Coordinate Formats

Intermapper supports a wide variety of formats for entering geographic coordinates. Any coordinate can be entered as follows:

- Decimal degrees: 43.692 or 72.272
- Degrees, minutes, seconds: 43:16:34.56
- Degrees with decimal minutes: 43:23.341
- Use W and S suffixes as alternatives to negative values.

Sample accepted formats:

- [+|-]dd.dd:mm.mm:ss.ss
- [+|-]dd.dd:mm.mm
- [+|-]dd.dd
- [+|-]dd.dd mm.mm ss.ss
- [+|-]dd.dd mm.mm

Allowable suffixes:

- s
- n
- e
- w
- S
- N
- E
- W

Acceptable Data Elements (in order)

- an optional negative sign
- a real number
- anything except letters, digits, -, or .
- a real number
- anything except letters, digits, -, or .
- a real number
- an optional ending directional notation (N, S, E, W, n, s, e, w (depends on the field)) or (in the case of 43° 16' 23)

Importing Devices with Geographic Coordinates

You can create a tab-delimited file with information about the devices to be added to the map. This information can include any of following fields: Name, IP Address, DNS name, port, type of device, SNMP community string, latitude, longitude, and many other fields. Fields left unspecified are filled with default values. For more information, see [Importing Data Into Maps \(Pg. 631\)](#).

An import file is formatted as follows:

- **Line 1 specifies the format of the following lines** - it specifies the file format (tab in the example below), the table to be filled (devices) and the order of the fields. MapName, Address, and Probe must be specified; the remainder are optional.
- **Remaining lines contain the data for the devices you want to import** - Each device occupies a single line, and the data columns are separated by tabs (a tab-delimited file.) Each column corresponds to a field in the **fields** specification of Line 1.

In this example import file, there are five fields to import. Intermapper places these items on the map named MapA, using the address specified to create HTTP probes. They are placed at the indicated latitude and longitude.

```
# format=tab table=devices
fields=MapName,Address,Probe,Latitude,Longitude
MapA    192.168.2.100    http    43.3    -72.0
MapA    192.168.2.101    http    43.9    -72.3
MapA    192.168.2.102    http    43.8    -72.8
MapA    192.168.2.103    http    43.0    -72.4
MapA    192.168.2.104    http    43.2    -72.3
MapA    192.168.2.105    http    43.6    -72.2
```

Map Sources

The following mapping services are available through the web:

Web-based Service	Description
<u>Google Image Search</u>	http://www.Google.com/imghp?hl=en&tab=wi&ie=UTF-8&q= Search their Images section for the word "map" plus the name of the country, province, state, etc. you need. Free.
<u>Maporama</u>	http://www.maporama.com Attractive street maps with different styles and coloring that are good for backgrounds. Large maps available. Free.
<u>Mapblast</u>	http://www.mapblast.com Another site showing street maps suitable for backgrounds. Large maps available. Free.
<u>National Atlas</u>	http://www.nationalatlas.gov A source of national and state maps. Free.
<u>terraserver.com</u>	http://www.terraserver.com Aerial photographs. Clever interactive latitude and longitude indicator using mouse rollover. 1 m/px resolution.
<u>Microsoft Research Maps</u>	http://msrmaps.com/ USGS Aerial photos, and topo maps to 1 m resolution. Clicking shows latitude and longitude of the clicked point. Also allows large, medium, and small maps. Free.
<u>US Census Bureau</u>	http://www.census.gov/geo/www/maps Construct a map from Census data as well as street, political, river/water data. Free.
<u>Yahoo! Listing of Map Resources</u>	http://dir.yahoo.com/Science/Geography/Cartography/Maps/Interactive/ Yahoo! Search for interactive maps. Lists many interesting mapping sites. Free.
<u>dmoz Open Directory</u>	http://dmoz.org/Science/Social_Sciences/Geography/Geographic_Information_Systems/ Links to many Geographic Information Systems sites. Free.
<u>Geocode.com</u>	http://www.geocode.com/ An inexpensive geocoding service that converts street addresses to latitude and longitude.
<u>Radio Mobile</u>	http://www.cplus.org/rmw/english1.html Software that predicts the performance of a radio system based on topographic maps. Free.

Exporting Information to Google Earth

Intermapper exports the following information so that Google Earth can place devices in the proper location. This information is exported as a .KML file compatible with Google Earth.

Each Intermapper map appears as a place in the left pane of Google earth. Items are shown as follows:

- **Devices** are represented by their status badges (green, yellow, orange, red circle icons)
- **Network ovals** are shown as small circles.
- **Links** between devices are shown as lines connecting the icons.
- **A Status window** for each of the above items displayed when you click the item.

To be displayed in Google Earth, a device must have geographic information; devices that do not have geographic information are not displayed at all.

Geographic coordinates can be set in the following ways:

- **Explicitly** - by using **Set Latitude and Longitude** for each device. You can set latitude and longitude values for many devices at once by [importing a text file containing the correct information \(Pg. 637\)](#).
- **Implicitly** - When benchmarks are placed on a map, the device's latitude and longitude are inferred from the x/y position on the map, relative to the established benchmarks. Use the Insert menu's [Map Benchmark... \(Pg. 635\)](#) to add benchmarks. Use of benchmarks is inherently less precise than using explicit coordinates.

In the case where both explicitly set coordinates and benchmarks are used, Intermapper uses the explicit coordinates and ignores the benchmarks.

How it Works

- **Google Earth requests information from the Intermapper server using HTTP.** Consequently, the Intermapper web server interface must be enabled in the Server Settings.
- **The Google Earth connection uses the same authentication method as the web interface;** you must have appropriate web access permissions for any map you wish to view in Google Earth. (Google Earth will prompt you for the username and password.)
- **Google Earth does not need to be installed on the Intermapper server,** though its machine must have appropriate access permissions established in the Intermapper web server firewall.

- **Google Earth uses a "Network Link"** with a URL that Google Earth uses to request information from Intermapper.

How to Use it

The easiest way to get the URL is through the Intermapper web interface.

1. Download and install Google Earth.
2. From the Server Configuration section of the Server Settings window, click **Web Server**. The Web Server settings pane appears in the right pane.
3. Make sure the web server is running, then click the URL to launch a browser with the Intermapper Web interface.
4. In the Intermapper web interface, click **Map List**. A list of maps on your server appears.
5. Click the link to a map that contains latitude/longitude information, either implicitly or explicitly. The map appears in the browser.
6. At the bottom of the map, click **View this map in Google Earth**. This is a link to the map's .KML file, a data file used by Google Earth. Assuming Google Earth has been installed properly, your browser offers to use Google Earth to open the file.

If everything is set up properly, the status badges for your devices hover over the surface of the Earth in appropriate locations.

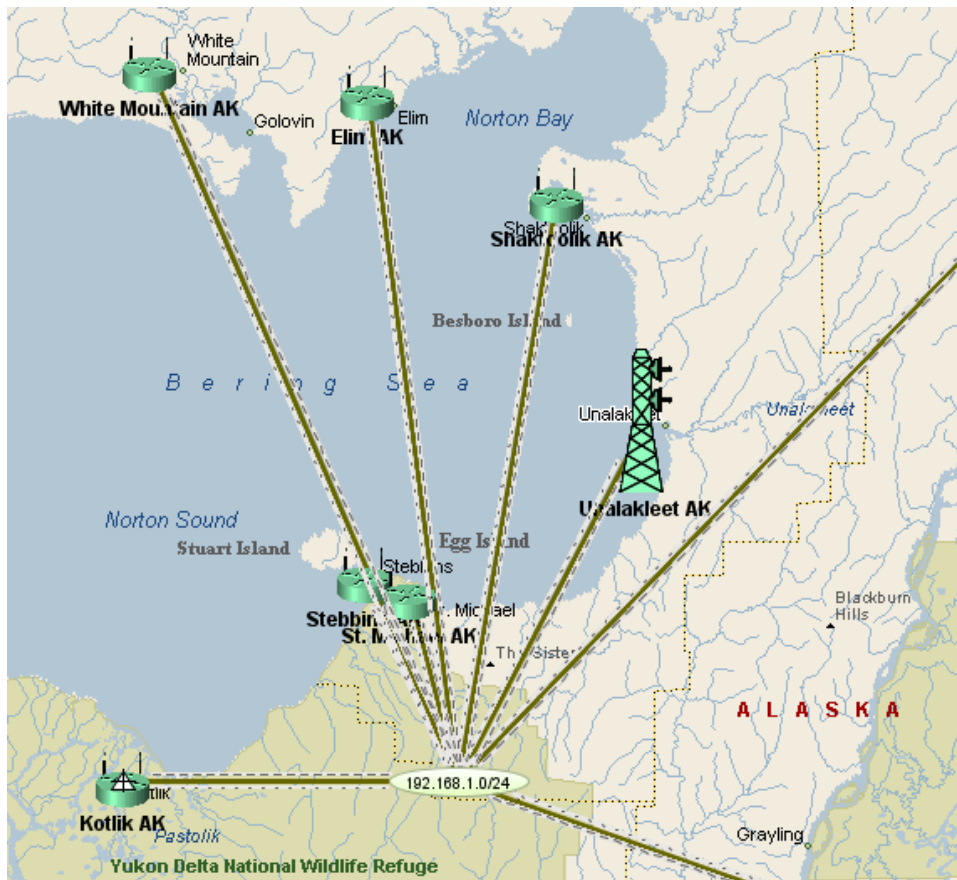
To view a device's status window:

Click the device's badge. The device's Status window is displayed in the Google Earth window.

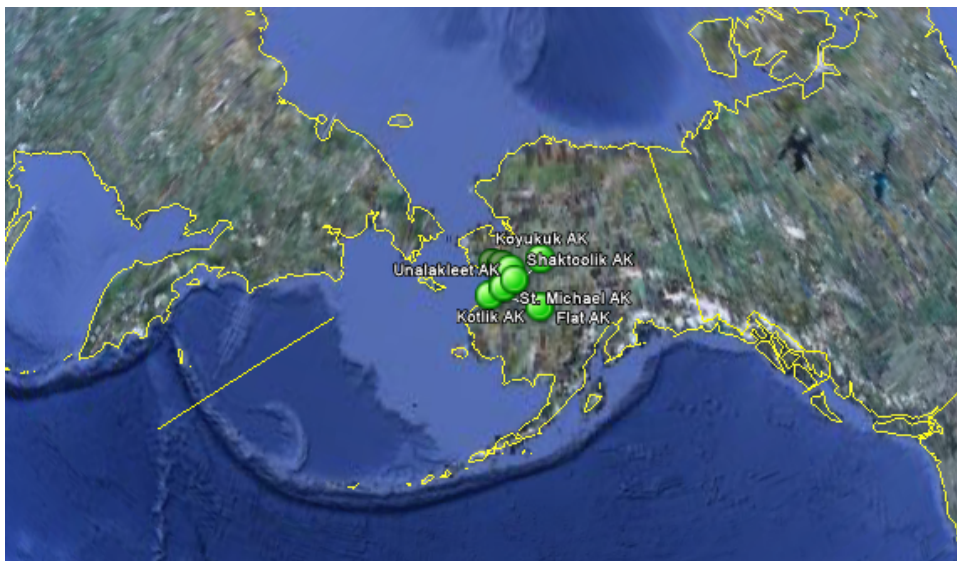
The map refreshes automatically every 5 minutes.

What You See

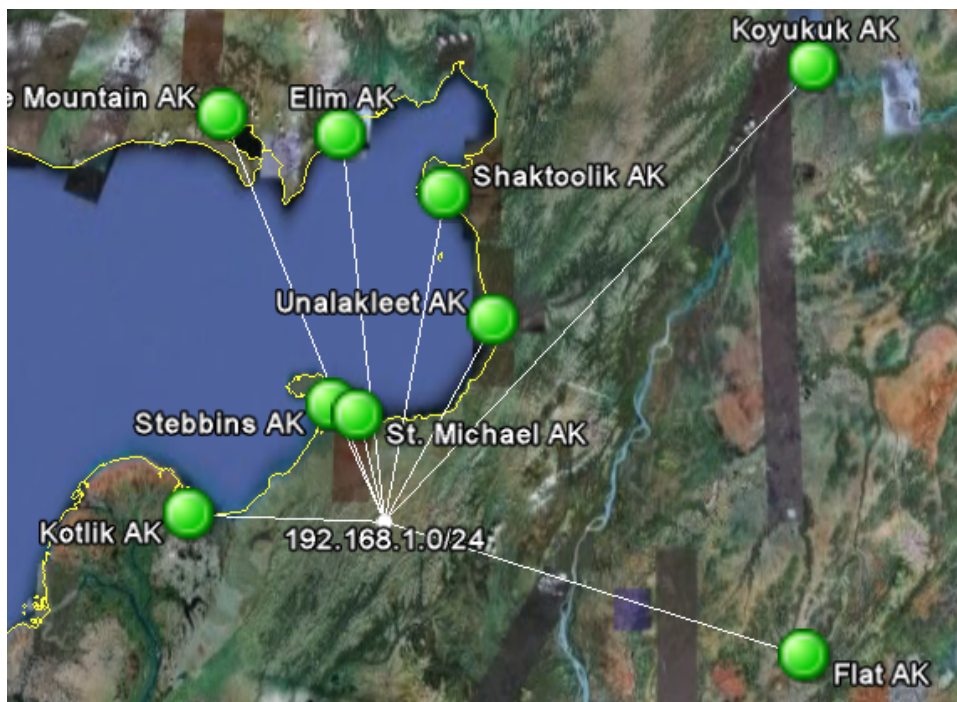
The images below show the original map, the mapped devices displayed from two different zoom levels, and the status window for one of the devices.



Original map in Intermapper



Wide view in Google Earth



Closer view in Google Earth



Status window in Google Earth

Advanced Data Importing

Introduction - Directive Line

If you need more control over the import process, you can use the Directive line technique instead of a spreadsheet-style import file. In addition to inserting new devices, you can update specific attributes of existing devices, change their appearance or location, and delete them.

NOTE: You can automate the importing of map data by sending commands to Intermapper Remote Access through its command-line interface. This allows you to interact with Intermapper through your own scripts. For more information, see [Using the Command Line Interface](#).

The first line, known as the directive line, is formatted as follows:

```
# format=tab table=devices fields=id,name,address modify=address
match=id
```

Each of the following elements are separated by a tab:

- The first line must begin with pound sign (#).
- The table=devices parameter specifies which table the data should be imported into.

Valid choices are detailed in [Data types \(Pg. 648\)](#).

- You can generate a list of fields and descriptions for any data type by exporting the **Schema** table. For more information, see [Exporting Data From Maps \(Pg. 625\)](#).
- You can include columns in your import file from both the Device and Vertices tables. Intermapper automatically applies the Vertex attributes appropriately to the vertex linked to the indicated device.
- The fields=id,name,address parameter identifies the order of the data in the columns. In this example, there are three columns for the device's ID, name, and address.
- The modify and matchparameters combine to specify which device attributes to change, and which device attributes to use to verify that the correct device has been found.

Directive Parameter	Format/Options
---------------------	----------------

<i>Format</i>	<p>Supported file formats:</p> <ul style="list-style-type: none"> • tab - tab-delimited • csv - comma-separated • xml - XML format (see an exported file for the format) <p>Example:</p> <pre>format=tab</pre>
<i>Table</i>	<p>Available values for the <code>table</code> directive are listed in Data types (Pg. 648), below.</p> <p>Examples:</p> <pre>table=devices table=vertices</pre>
<i>Modify</i>	<p>Comma-separated list of field names. Use this parameter to specify which of the columns you want to update. You can combine this with the optional Match parameter.</p> <p>Note: If there is no Match parameter, the ID field is used to find matches. If no ID field exists, the import fails.</p> <p>Example:</p> <pre>modify=ID, MapName, Address, Latitude, Longitude</pre>
<i>Match</i>	<p>Comma-separated list of field names. Use this parameter to specify which of the columns you want to use to determine whether to modify device values.</p> <p>If no Match parameter is included, the ID field is used to find matches.</p> <p>If no ID field is included in the file, the import fails.</p> <p>Example:</p> <pre>match=MapName, Address</pre>

<i>Insert</i>	<p>Comma-separated list of field names. Use this parameter to specify the fields you want to set when creating the device.</p> <p>You must include a combination of at least two fields whose Access attribute is "CREATE" (MapPath, Address, DNSName, IMProbe, MapID). To see the valid combinations, see Device Attributes (Pg. 649). When no valid MapPath is included, one is created for you, named "Untitled 1".</p> <p>Once the device is created using one or more of these fields, Intermapper attempts to set the values of the remaining fields specified in the Insert parameter to the values in the corresponding columns.</p> <p><i>Insert</i> fields are evaluated from left to right. If, for example, you specify an Address, DNSName, and IMProbe in that order, the Address is set, and the DNSName is resolved to it, and remaining fields are set from the IMProbe parameter.</p> <p>Examples:</p> <pre>Insert=MapPath,Address,Name,Latitude,Longitude</pre> <p>(The example above creates devices in the specified maps with the specified addresses, names, latitude, and longitude.)</p>
<i>Delete</i>	<p>Comma-separated list of field names. Use this parameter to specify which of the columns you want to use to determine whether a device should be deleted.</p> <p>Example:</p> <pre>delete=MapName,Probe</pre> <p>(The example above would delete all devices in the specified maps that use the specified probes)</p>

<i>Group</i>	<p>Comma-separated list of field names.</p> <p>Behaves exactly like the Insert directive, except when it encounters a device to be inserted as a probe group. Devices immediately following the probe group with the same address (and not a probe group) are added to the group.</p> <p>When another probe group is encountered, the previous group is ended, and subsequent entries are added to the new group.</p> <p>Note: If the Intermapper server cannot resolve the DNS name, a probe group is added by IP address. This may prevent subsequent entries from being added to the probe group.</p> <p>Examples:</p> <pre>group=MapName,MapPath,Address,Name,Latitude,Longitude</pre>
--------------	---

Remaining Lines - Specifying the Data

The remaining lines of the file contain the data as specified in the **fields** definition described above. Each column is separated by a tab, and columns must appear in the order specified in the **fields** definition (for directive line imports) or must correspond to the field names specified in the first line of the file (spreadsheet-style imports).

Available values for the `table` directive are listed in [Data types \(Pg. 648\)](#), below.

Import File Example

Below is an example of an Import file. This file specifies itself as a tab-delimited file containing a list of devices. All devices are going into the map named "MapA", and each device definition contains Address, Probe, Latitude, and Longitude columns.

```
# format=tab table=devices
fields=MapName,Address,Probe,Latitude,Longitude
MapA 192.168.2.100 http 43.3 -72.0
MapA 192.168.2.101 http 43.9 -72.3
MapA 192.168.2.102 http 43.8 -72.8
MapA 192.168.2.103 http 43.0 -72.4
MapA 192.168.2.104 http 43.2 -72.3
MapA 192.168.2.105 http 43.6 -72.2
```

NOTE:

The example above creates the devices and assigns probes, but does not set the parameters for the probes. The most efficient way to do this is using the [IMProbe URL](#). It lets you specify the SNMP community string, the probe by file name, and any parameters needed.

Creating Probe Groups

Use the `group` directive to create a device and add probes to it as a group. The following example adds six devices, with the last one having a probe group. Groups are created in order - probes are added to the group until the IP address changes.

NOTE:

Like the example above, this one creates the devices and assigns probes, but does not set the parameters for the probes. The most efficient way to create and configure a probe group is to use the [IMProbe URL](#). It lets you specify the SNMP community string, the probe by file name, and any parameters needed.

```
# format=tab table=devices
fields=MapName,Address,Probe,Latitude,Longitude
group=MapName,Address,Probe,Latitude,Longitude
MapA 192.168.2.100 http 43.3 -72.0
MapA 192.168.2.101 http 43.9 -72.3
MapA 192.168.2.102 http 43.8 -72.8
MapA 192.168.2.103 http 43.0 -72.4
MapA 192.168.2.104 http 43.2 -72.3
MapA 192.168.2.105 group 43.6 -72.2
MapA 192.168.2.105 http 43.6 -72.2
MapA 192.168.2.105 snmp 43.6 -72.2
```

Automatic Placement of Devices

If your map contains no benchmarks (as described in [Using Geographic Coordinates](#)) latitude and longitude fields are ignored. You can place devices at specific locations using the `XCoordinate` and `YCoordinate` fields (described in the [Vertex Attributes \(Pg. 660\)](#)). X and Y coordinates are calculated from the upper left.

If the map contains benchmarks to specify geographic coordinates, Intermapper uses them to place devices at the proper location in the map.

NOTE:

In order for Intermapper to place devices accurately using geographic coordinates, two benchmarks must be specified before you import or update the devices. If you have imported the devices to the map before specifying the benchmarks, you can create an export file containing the MapPath, ID, Latitude and Longitude, then re-import the file after specifying your benchmarks. The devices are moved to the appropriate locations on the map.

How Intermapper Inserts Devices

Intermapper places new devices in horizontal rows across the top of the specified map. If either X/Y coordinates or geographic coordinates are specified for the device, Intermapper places it at the specified location on the map.

How Intermapper Handles Errors and Defaults

Intermapper strives to use sensible defaults. The import file needs only a server name, map path, and either an IP address or DNS Name for a new device. Intermapper uses its default settings for other values and parameters.

Note: If the Intermapper server cannot resolve the DNS name, the device is added by IP address.

The import process recovers sensibly from faulty, ill-formatted, or inconsistent input values. An invalid format for an IP address, for example, cannot succeed, and is reported as an error. Most other data is passed along so the device can be added to the map with appropriate defaults. The Intermapper Event Log file contains a line for each newly added device, along with indication of success or error.

If the attribute name in the header of the imported file is not recognized as a valid attribute, Intermapper displays an error message and ignores the contents of that column.

When the import is finished, a summary is written to the Event Log file.

NOTE:

- Every Intermapper server maintains a unique identifier (the "id") for each of its devices on each map. This makes it a convenient value for matching updated information to an existing device.
- Intermapper defines a new *IMProbe* URL that completely specifies all the parameters of an Intermapper Probe. This IMProbe: URL is defined in [The IMProbe URL \(Pg. 677\)](#).

Data Types

For each table for which data can be imported or exported, a data type is defined. For information on the different data types, and what information is readable, writable, or both, see the Attributes topic for each data type as linked below.

`table=[data type]`

- **devices** - imports data specific to devices. See the [Device Attributes \(Pg. 649\)](#) table.
- **vertices** - You can also control other aspects of a device in a map, such as the device's color, label, shape, or font. The `vertices` type imports data specific to the appearance of devices. See the [Vertex Attributes \(Pg. 660\)](#) table.
- **interfaces** - imports data specific to the switch and router interfaces. See the [Interface Attributes \(Pg. 662\)](#) table.
- **maps** - imports data specific to maps. See the [Map Attributes \(Pg. 667\)](#) table.
- **notifiers** - imports data to describe notifiers. See the [Notifier Attributes \(Pg. 669\)](#) table.
- **notifierrules** - imports data to describe how a notifier is applied. See the [Notifier Rules Attributes table. \(Pg. 670\)](#)
- **users** - imports user account information. See the [User Attributes \(Pg. 672\)](#) table.
- **retentionpolicies** - imports user account information. See the [Retention Policy Attributes \(Pg. 673\)](#) table

Device Attributes

Device attributes are supported as described in the table below. At minimum, **MapName** and **Address** are required. To create a device by importing, the following is required:

- One of **MapPath** or **MapID**
- One of **Address**, **DNSName**, or **NetBIOSName**

For any attribute that is not in the file, a default value is used. For example, if no probe is specified, the **Automatic** probe is used.

Use these attributes with the following table specification in line 1:

`table=device`

NOTE:

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.
- Fields with the Access attribute of "SENSITIVE" can only be imported by an administrator over a secure SSL connection.
- The columns are imported in the order specified. The last value specified takes precedence over previous values in the same line. Because of this, Fortra recommends that you use only one the following columns when importing: **Address, DNSName, IMProbe**. If more than one of these is specified, and there are conflicts, the last column's values are used.

Device Attributes

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map containing the device.
MapPath	Type: TEXT Access: READ-ONLY Attributes: CREATE Description: Full path of the map containing the device, including the name of the map.
Address +	Type: ADDRESS Access: READ-WRITE Attributes: CREATE Description: The IP or AppleTalk address of the device that is probed by Intermapper. The IP address is represented in dotted-decimal notation, e.g. 'a.b.c.d'. The AppleTalk address is represented in slash notation, e.g. 'a/b'.
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this device instance. The id will be unique across all maps on a single Intermapper server.

Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the device. The name is the first non-empty line in a device's label on a map.
Probe +	Type: TEXT Access: READ-WRITE Attributes: none Description: The human-readable name of the Intermapper probe.
Comment +	Type: TEXT Access: READ-WRITE Attributes: none Description: The comment associated with the device.
Community +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The SNMP community of the device.
DisplayIfUnNumbered +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is set to display unnumbered interfaces.
DNSName +	Type: TEXT Access: READ-WRITE Attributes: CREATE Description: The fully-qualified DNS name of the device.
IgnoreIfAppleTalk +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore AppleTalk interface information.

IgnoreIfDiscards +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore interface discards.
IgnoreIfErrors +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore interface errors.
IgnoreOutages +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to ignore outages.
AllowPeriodicReprobe +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the device's behaviour is to allow periodic reprobe.
IMProbe *+	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE,CREATE Description: A special URL representation describing the Intermapper probe and its parameters, e.g. improbe://address:port/...
Latitude +	Type: TEXT Access: READ-WRITE Attributes: none Description: The latitude of the device. The value will be a double within the range [-90..90] or empty string if the device does not have this attribute set.
Longitude +	Type: TEXT Access: READ-WRITE Attributes: none Description: The longitude of the device. The value will be a double within the range [-180..180] or empty string if the device does not have this attribute set.

LastTimeDown	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device last went down. Value is 0 if device has not gone down since we started monitoring it.
LastTimeSysUp	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device last came up (ie rebooted), based on the value of sysUpTime. The value is 0 if unknown.
LastTimeUp	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The time when the device status last transitioned from DOWN to UP. Value is 0 if this has not happened since we started monitoring.
MACAddress	Type: TEXT Access: READ-ONLY Attributes: none Description: The MAC address of the device. If the device has multiple interfaces, this field contains the MAC address associated with the main IP address of the device (the same address in the address field).
MapAs +	Type: TEXT Access: READ-WRITE Attributes: none Description: Value is one of { ROUTER , SWITCH , HUB, END SYSTEM }
MapId	Type: TEXT Access: READ-ONLY Attributes: CREATE Description: The unique Id of the map file containing the device.

MaxTries +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The maximum number of attempts to reach the device, typically indicates the maximum number of packets to send during each poll, for packet-based probes.
NetBIOSName +	Type: TEXT Access: READ-WRITE Attributes: CREATE Description: The NetBIOS/WINS name of the device.
PctLoss	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The percent loss (# packets lost/total # packets sent).
ShortTermPctLoss	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The short-term percent loss (# packets lost/# packets sent).
Availability	Type: DOUBLE Access: READ-ONLY Attributes: none Description: The percent availability (time up/time monitored).
PollInterval +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The poll interval of the device, in seconds. Value is 0 if non-polling.
Port +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The UDP or TCP port number. If the port number is not applicable, this value is always 0. (e.g. for ICMP)

Resolve +	Type: TEXT Access: READ-WRITE Attributes: none Description: Value is one of { name , addr , none }.
RoundTripTime	Type: INTEGER Access: READ-ONLY Attributes: none Description: The last round-trip time in milliseconds, if known.
SNMPv3AuthPassword +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The device's SNMPv3 authentication password.
SNMPv3AuthProtocol +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMPv3 authentication protocol (MD5, SHA, None).
SNMPv3PrivPassword +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The device's SNMPv3 privacy password.
SNMPv3PrivProtocol +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMPv3 privacy protocol (DES, None).
SNMPv3UserName +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMPv3 user name.
SNMPVersion +	Type: TEXT Access: READ-WRITE Attributes: none Description: The device's SNMP version (SNMPv1, SNMPv2c, or SNMPv3).

Status	Type: TEXT Access: READ-ONLY Attributes: none Description: The status of the device. The value is one of { 'UP', 'DOWN', 'UNKNOWN' }.
StatusLevel	Type: TEXT Access: READ-ONLY Attributes: none Description: The status level of the device. The value is one of { 'Unknown', 'OK', 'Warning, Acked', 'Warning', 'Alarm, Acked', 'Alarm', 'Critical', 'Critical, Acked', 'Down', 'Down, Acked' }.
StatusLevelReason	Type: TEXT Access: READ-ONLY Attributes: none Description: The reason the device has its status level.
SysDescr	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysDescr.
SysName	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysName.
SysContact	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysContact.
SysLocation	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysLocation.

SysObjectID	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The value of sysObjectID.
TimeOut +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The timeout of the device, in seconds. Value is 0 if not-applicable to the probe.
IMID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: Identifier of the device in the IMID format.
Type	Type: TEXT Access: READ-ONLY Attributes: none Description: One of { none, other, snmp, tcp, udp, icmp, cmd, bigbro, ntsvcs }. These values have been updated in 5.0 to match the values used by the database in the probekind field of the devices table.
ProbeXML	Type: TEXT Access: READ-ONLY Attributes: SENSITIVE Description: XML dataset DTD, type='probe'.
SNMPVersionInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: 1, 2, 3 - SNMP versions. 0 for non-SNMP.
SysServices	Type: INTEGER Access: READ-ONLY Attributes: none Description: 16-bits integer.

EntSerialNum	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalSerialNum of chassis).
EntMfgName	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalMfgName of chassis).
EntModelName	Type: TEXT Access: READ-ONLY Attributes: none Description: SnmpAdminString (entPhysicalModelName of chassis).
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Data retention policy for IM Database
CustomerNameReference	Type: TEXT Access: READ-ONLY Attributes: none Description: Customer-supplied device name reference, for linking to an external database.
EnterprisID	Type: TEXT Access: READ-ONLY Attributes: none Description: The value of sysEnterprisID.
DeviceKind	Type: TEXT Access: READ-ONLY Attributes: none Description: User-specified device type.
SysUpTime	Type: TEXT Access: READ-ONLY Attributes: none Description: System uptime.

LastModified	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: Timestamp of last modification to this device.
Parent	Type: TEXT Access: READ-ONLY Attributes: none Description: Device ID of the parent probe group; this device's id if this device is a probe group; 0 if the device is not part of a probe group.
Acknowledge +	Type: TEXT Access: READ-WRITE Attributes: none Description: The acknowledgement state of the device; one of { 'None', 'Basic', 'Maintenance' }. The AckMessage field must also be set to import this field. Indefinite maintenance will be set if AckExpiration is missing and state is set to 'Maintenance'.
AckMessage +	Type: TEXT Access: READ-WRITE Attributes: none Description: The message associated with the acknowledge state. If Acknowledge is not set and an AckMessage is supplied, Acknowledge will be set to 'Basic'.
AckExpiration +	Type: TEXT Access: READ-WRITE Attributes: none Description: The absolute time when the timed acknowledgement expires, if any. The AckMessage field must also be set to import this field. Acknowledge will be set to 'Maintenance' if not supplied.
AckTimer	Type: TEXT Access: READ-ONLY Attributes: none Description: The time in seconds remaining until the timed acknowledgement expires, if any.

VertexId	Type: TEXT Access: READ-ONLY Attributes: none Description: The Vertex Id of the vertex associated with the device. Matches the VertexId of the corresponding vertex in the vertices table.
Layer2	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if layer2 mapping is enabled for this device.

Vertex Attributes

Use the vertices data type to control the appearance of devices in your map, such as the device's color, label, shape, or font.

Use the following attributes with the following table specification in line 1:

```
table=vertices
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map file containing the vertex.
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this vertex instance. The id will be unique across all maps on a single Intermapper server.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the vertex. The name is the first non-empty line in a device or network's label on a map.

Color +	Type: TEXT Access: READ-WRITE Attributes: none Description: Color (valid names: white, black, red, orange, yellow, blue, green, brown)
FontName +	Type: TEXT Access: READ-WRITE Attributes: none Description: Font name, eg. Bodoni MT
FontSize +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Font size in points.
FontStyle +	Type: TEXT Access: READ-WRITE Attributes: none Description: Font style (bold, italic, plain)
Label	Type: TEXT Access: READ-ONLY Attributes: none Description: Vertex label.
LabelPosition +	Type: TEXT Access: READ-WRITE Attributes: none Description: Label position. Valid values are topleft, top, topright, left, center, right, bottomleft, bottom, bottomright
LabelTemplate +	Type: TEXT Access: READ-WRITE Attributes: none Description: Vertex label template.
LabelVisible +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the vertex label is visible (only used when the device is represented by an icon)

MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique Id of the map file containing the vertex.
Origin +	Type: TEXT Access: READ-WRITE Attributes: none Description: The origin determines whether the vertex coordinates are relative to the center or one of the sides of the vertex. Valid values: center, top, left, right, botom, topleft, topright, bottomright, bottomleft.
Shape +	Type: TEXT Access: READ-WRITE Attributes: none Description: Vertex shape (rect, oval, wire, cloud, text, or icon name).
VantagePoint +	Type: BOOLEAN Access: READ-WRITE Attributes: none Description: True if the vertex is a vantage point of the graph
XCoordinate +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Horizontal map coordinate, the positive direction is to the right.
YCoordinate +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Vertical map coordinate, the positive direction is to the bottom.
VertexId	Type: TEXT Access: READ-ONLY Attributes: none Description: The Vertex Id of the vertex. Corresponds to the device with a matching VertexID in the devices table.

Interface Attributes

The interfaces data type imports data specific to the switch and router interfaces.

Use these attributes with the following table specification in line 1:

```
table=interfaces
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.

Interface Attributes

Field Name	Description
MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: The name of the map to which the interface belongs.
InterfaceID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique persistent identifier for this interface instance.
DeviceID	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the adjacent device.
NetworkID	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the adjacent network.
Index	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface index (i.e. ifIndex) of the interface.

IntegerIndex	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface index (i.e. ifIndex) of the interface, as an integer.
Description	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface description (i.e. ifDescr).
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface name (i.e. ifName).
Alias	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface alias (i.e. ifAlias).
PhysAddress	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The interface's data-link layer address (i.e. ifPhysAddr). .
Type	Type: TEXT Access: READ-ONLY Attributes: none Description: The interface type as a human-readable string (i.e. ifType).
MTU	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface MTU (i.e. ifMTU).
Address	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The interface's first network-layer address.

SubnetMask	Type: ADDRESS Access: READ-ONLY Attributes: none Description: The subnet mask associated with "Address".
SubnetList	Type: TEXT Access: READ-ONLY Attributes: none Description: A comma-separated list of addresses/masks on this interface.
SubnetPrefixList	Type: TEXT Access: READ-ONLY Attributes: none Description: A comma-separated list of addresses/prefixes on this interface.
Speed	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface's speed in bits per second. (Derived from preferred speed and reported speed.)
PreferredSpeed +	Type: INTEGER Access: READ-WRITE Attributes: none Description: The preferred speed of the interface as set by the customer.
ReportedSpeed	Type: INTEGER Access: READ-ONLY Attributes: none Description: The speed of the interface as reported by the interface.
LastChange	Type: TIMESTAMP Access: READ-ONLY Attributes: none Description: The timestamp when the interface last changed status.

Status	Type: TEXT Access: READ-ONLY Attributes: none Description: The status of the interface (e.g. UP, DOWN, or ADMIN-DOWN).
Enabled +	Type: TEXT Access: READ-WRITE Attributes: none Description: Flag which indicates whether the interface is enabled or not.
MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: The unique persistent identifier for the map to which the interface belongs.
IMID	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: Identifier of the interface in the IMID format.
TypeInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: The interface type as a number.
RecvSpeed +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Unsigned 64-bit integer. 0 means baseband; speed in Speed.
StatusInt	Type: INTEGER Access: READ-ONLY Attributes: none Description: The status of the interface as integer. Values correspond to {UP, DOWN, ADMIN-DOWN, DOWN but locally acked}.

CustomerNameReference	Type: TEXT Access: READ-ONLY Attributes: none Description: Customer-supplied name, for referencing an external database.
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Database data retention policy.
Duplex	Type: TEXT Access: READ-ONLY Attributes: none Description: Interface Duplex status.
VLANs	Type: TEXT Access: READ-ONLY Attributes: none Description: Comma-separated list of this interface's VLANs.
NatVLAN +	Type: INTEGER Access: READ-WRITE Attributes: none Description: Native VLAN. Signed integer (0-4093). 0 means none.

Map Attributes

The maps directive contains data to describe maps. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=maps
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.

Field Name	Description
MapId	Type: TEXT Access: READ-ONLY Attributes: none Description: A unique, persistant identifier for this map instance.

MapName	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the map.
MapPath	Type: TEXT Access: READ-ONLY Attributes: none Description: Full path of the map, including the name of the map.
Status	Type: TEXT Access: READ-ONLY Attributes: none Description: Status of the map (e.g. down, critical, alarm, warning, okay).
DeviceCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in the map.
NetworkCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of networks in the map.
InterfaceCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of interfaces in the map.
DownCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices that are down.
CriticalCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in critical status.

AlarmCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in alarm status.
WarningCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of devices in warning status.
OkayCount	Type: INTEGER Access: READ-ONLY Attributes: none Description: Number of okay devices.
DataRetentionPolicy	Type: INTEGER Access: READ-ONLY Attributes: none Description: Database retention policy.
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the map in the IMID format.
Enabled	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if the map is currently running.
Layer2	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if the map is enabled for layer 2 polling.

Notifier Attributes

The notifiers data type contains data to describe notifiers. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=notifiers
```

Field Name	Description
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the notifier in the IMID format.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: Human readable, one-line name.
NotifierXML	Type: TEXT Access: READ-ONLY Attributes: none Description: XML dset DTD, type='notifier'.
enabled	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if the notifier is enabled.

Notifier Rules Attributes

The `notifierrules` data type contains data to describe how a notifier is applied. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=notifierrules
```

Field Name	Description
NotifierIMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the notifier in the IMID format.
EscalationIMID	Type: TEXT Access: READ-ONLY Attributes: none Description: Identifier of the escalation in the IMID format.

Down	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of DOWN events.
Up	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of UP events.
Critical	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of CRITICAL events.
Alarm	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of ALARM events.
Warning	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of WARNING events.
Okay	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of OKAY events.
Trap	Type: BOOLEAN Access: READ-ONLY Attributes: none Description: True if user is notified of TRAP events.
Delay	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification delay.

Repeat	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification repeat.
Count	Type: INTEGER Access: READ-ONLY Attributes: none Description: Notification count.

User Attributes

The users data type imports user account information.

Use these attributes with the following table specification in line 1:

```
table=users
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.

Field Name	Description
Id	Type: TEXT Access: READ-ONLY Attributes: INDEX Description: A unique, persistent identifier for this user.
Name *+	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE,CREATE Description: Login name of the user.
Password +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: If the user is to be validated locally, the user's password.
Guest +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: The user's autologin properties.

External +	Type: BOOLEAN Access: READ-WRITE Attributes: SENSITIVE Description: Indicates user is to be validated by an auth server.
Groups +	Type: TEXT Access: READ-WRITE Attributes: SENSITIVE Description: Comma-separated list of groups to which to add user. (Will not remove users from groups not in list.)

Retention Policy Attributes

The retentionpolicies data type contains data to describe retention policies. All fields are READ-ONLY.

Use these attributes with the following table specification in line 1:

```
table=retentionpolicies
```

- Fields marked with an asterisk (*) are required.
- Fields marked with an plus sign (+) can be updated during import.

Field Name	Description
IMID	Type: TEXT Access: READ-ONLY Attributes: none Description: IMID of the retention policy.
RetentionPolicyID	Type: INTEGER Access: READ-ONLY Attributes: none Description: Identifier of the retention policy.
Name	Type: TEXT Access: READ-ONLY Attributes: none Description: Name of the retention policy.

ServerStorageType	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long chart data is retained by the server; 0 = No data retained, -1 = data retained forever, -2 = data retained in memory only.
RawExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long raw chart data is retained by the database in days; -1 = forever.
FiveExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long five-minute sample data is retained by the database in days; -1 = forever.
HourlyExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long hourly sample chart data is retained by the database in days; -1 = forever.
DailyExpiration	Type: INTEGER Access: READ-ONLY Attributes: none Description: How long daily sample chart data is retained by the database in days; -1 = forever.

About D-Sets

When you export data, you can export a generic set of information about a probe or notifier. This information is in XML format, contained in an export field in the following export tables:

- **ProbeXML** - If this field is included in the export, a D-set is included for each selected device on the map.
- **NotifierXML** - If this field is included in the export, a D-set is included for each active notifier associated with the map.

ProbeXML D-Set

This D-set contains information about a specific probe. Depending upon the probe type, it can have more or fewer `<d>` clauses. For example,

```
<dset type='probe' hashcode='abcdef'>
  <d name='probe'>com.dartware.snmp</d>
  <d name='snmp_ver'>SNMPv3</d> // present only for snmp probes
  <d name='address'>192.168.1.23</d>
  <d name='username'>MyName</d> // present only for snmp_v3
  <d name='auth_protocol'>MD5</d> // present only for snmp_v3
  <d name='auth_passwd'>somePwd</d> // present only for snmp_v3
  <d name='priv_protocol'>DES</d> // present only for snmp_v3
  <d name='priv_passwd'>somePwd2</d> // present only for snmp_v3
  <d name='community'>public</d> // present only for snmp_v1
  and snmp_v2c probes
  <d name='port'>80</d>
  <d name='interval'>30</d>
  <d name='timeout'>3</d>
  <d name='tries'>3</d>
  <d type='param' name='Disk Usage Warning %'>75</d>
  <d type='param' name='Memory Usage Alarm %'>90</d>
  <d type='param' ... </d>
</dset>
```

NotifierXML D-Set

This D-set contains information about a specific notifier. Depending upon the notifier type, it may have more or fewer `<d>` clauses. For example,

```
<dset type='notifier'>
  <d name='method'>smtpmail</d>
  <d type='param' name='email_addr'>abc@dd.com</d>
  <d type='param' name='subject'>This is a subject</d>
  <d type='param' name='message'>This is a message.</d>
</dset>

<dset 'notifier'>
  <d name='method'>audible</d>
  <d type='param' name='down_sound'>name of the sound (as
string)</d>
  <d type='param' name='up_sound'></d>
  <d type='param' name='crit_sound'></d>
  <d type='param' name='alarm_sound'></d>
  <d type='param' name='warn_sound'></d>
  <d type='param' name='ok_sound'></d>
  <d type='param' name='trap_sound'></d>
```

```
<d type='param' name='down_vol'>3</d>
<d type='param' name='up_vol'>2</d>
<d type='param' name='crit_vol'>1</d>
<d type='param' name='alarm_vol'>1</d>
<d type='param' name='warn_vol'>1</d>
<d type='param' name='ok_vol'>1</d>
<d type='param' name='trap_vol'>5</d>
</dset>

<dset type='notifier'>
  <d name='method'>snmptrap</d>
  <d type='param' name='address'></d>
  <d type='param' name='community'></d>
</dset>

<dset type='notifier'>
  <d name='method'>snpppager</d>
  <d type='param' name='pager_id'></d>
  <d type='param' name='message'></d>
</dset>

<dset type='notifier'>
  <d name='method'>modempager</d>
  <d type='param' name='pager_id'></d>
  <d type='param' name='message'></d>
</dset>

<dset type='notifier'>
  <d name='method'>winpopup</d>
  <d type='param' name='popup_id'></d>
  <d type='param' name='message'></d>
</dset>

<dset type='notifier'>
  <d name='method'>cmdline</d>
  <d type='param' name='cmdline'></d>
  <d type='param' name='success'></d>
  <d type='param' name='message'></d>
</dset>

<dset type='notifier'>
  <d name='method'>syslog</d>
  <d type='param' name='address'></d>
  <d type='param' name='facility'></d>
  <d type='param' name='severity'></d>
  <d type='param' name='message'></d>
</dset>
```



```
<dset type='notifier'>
  <d name='method'>group</d>
  <d type='param' name='id_list'></d>
</dset>
```

The IMProbe URL Specification

Intermapper defines a URL format for specifying all the parameters for a probe in a single string. This makes it straightforward to import information about a probe into Intermapper from a text file.

When you export data from Intermapper, you can include the IMProbe field in the export file. The IMProbe field contains the IMProbe URL, which in turn contains all configuration information for a probe in URL-encoded format. You can use the IMProbe URL to change the parameters of probes editing the parameters of the URL, and then importing the URL into the map.

For example, you can change the username and password for all of your HTTP probes in all maps at once by doing the following:

1. Export the data, including the MapName, Address, and Id, and IMProbe fields for all maps.
2. Find and replace the username and password parameters in each URL.
3. Re-import the text file.

The following URL format specifies the information necessary to define a probe using the IMProbe scheme:

```
URL: 'improbe:///'[community'@']address[':'port] '/'probe
['?'parameters]
```

NOTE:

improbe:// is case-sensitive and must be lower-case.

The minimal information required for an IMProbe URL is the Address information, Probe type, and Authentication information.

- Address information
 - DNS name
 - IP address
 - Port number (optional)

- Probe type
 - Canonical probe name
 - Probe-specific parameters (optional)
- Authentication information
 - SNMP community name (optional)

The `probe` can be a canonical Intermapper probe name specified in full, ie. `com.dartware.radius`, `com.dartware.http.redirect`, or a unique probe suffix can be specified. For example, `radius`, `http.redirect`.

The `parameters` are the parameters for the probe, encoded as for a GET request. To make it simpler to create IMProbe URL's manually, the matching of parameter names is simplified. Before matching parameter names, the parameter names are converted to lower-case, and any spaces and underscores are removed. For a parameter named `Shared Secret`, this means that IMProbe parameters `shared%20secret`, `sharedsecret` and `shared_secret` will match and provide values.

If the `parameters` section contains a parameter name that is not defined for the probe, the parameter is ignored. If a probe parameter is left out of the IMProbe URL, it is set to its default value from the probe file.

Examples

Both of the IMProbe URLs below specify that the host `netopia.example.com` should be tested with the built-in Ping probe:

```
improbe://netopia.example.com/com.dartware.ping
improbe://netopia.example.com/ping
```

Both these URLs test a RADIUS server at `netopia.example.com`, with a shared secret of 'secret', a user name of 'im', and a password of 'pw'. The "Shared Secret" parameter can be written multiple ways:

```
improbe://netopia.example.com/com.dartware.radius?shared_
secret=secret&user_name=im&password=pw
```

```
improbe://netopia.example.com/radius?sharedsecret=secret&userna
me=im&password=pw
```

The URLs below specifies the SNMP probe, testing a device at `192.168.1.1`, using the community string of 'public'. The second URL a test against port 1611 instead of the default port 161 used in the first URL:

```
improbe://public@192.168.1.1/com.dartware.snmp  
improbe://public@192.168.1.1:1611/snmp
```

Encoding Special Characters

The IMProbe URL format uses the Common Internet Scheme Syntax as specified in section 3.1 of RFC 1738 (now deprecated) and in compliance with current RFC 3986. The following characters are illegal and must be encoded with %hh:

00-1F, 7F, 80-FF

The following characters are also considered unsafe and should be encoded with %hh:

< > " # %

The following characters are reserved for special purposes and should not appear unencoded except when used as delimiters in the URL:

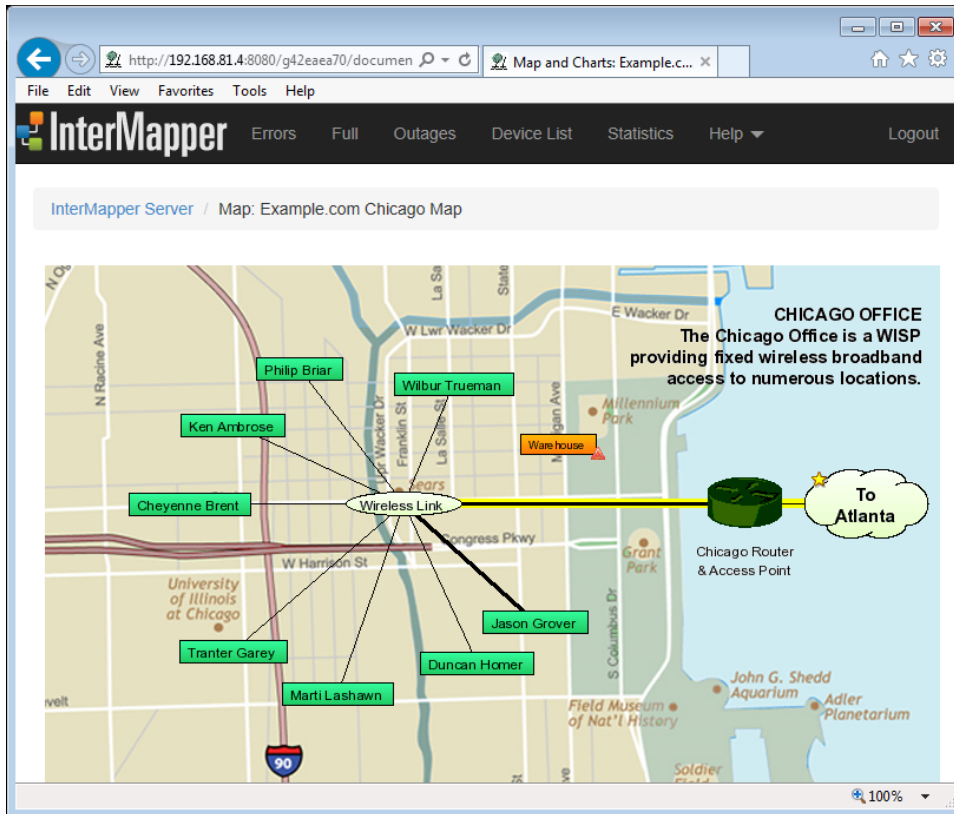
; / ? : @ = &

Using the Web Server

Each page that Intermapper serves contains the same controls at the top. The example below shows an Intermapper map as it appears in a web page.

NOTE:

To access the web server remotely, (that is, from a different machine connected to the network) you must configure the Intermapper firewall to permit the connection. You must also configure any other firewalls protecting the machine that is running Intermapper to allow traffic to the specified port. For more information, see [The Web Server](#) in the Server Settings section.



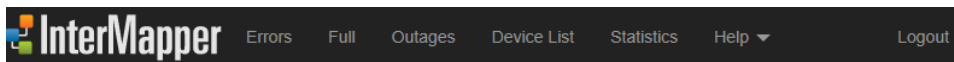
A typical InterMapper web page. the "Example.com" Chicago map.

The InterMapper web page typically has three parts:

- The header shows the map name or other title and a navigation bar for going to other pages. This is usually the same for every page.
- The content of the page varies, depending on which page is selected.
- The footer of the page shows the time the page was created.

Intermapper Web Page Navigation

Use the menu at the top of the InterMapper Web Page to access the available features of the web page. The example above shows a web page for a particular map. The image below shows the InterMapper Web Server menu, found at the top of each page.



Click any of the menu items at the top of the page to view the page. Here is a brief description of each page:

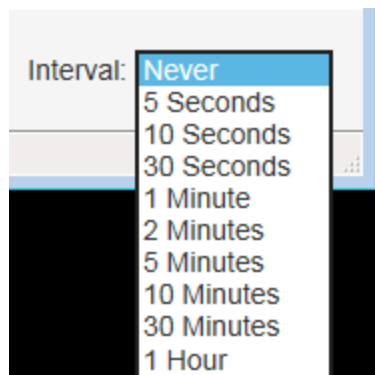
- **Home Page** - click the Intermapper logo to return to the Home page. View a list of open maps and the charts associated with those maps. Mouse over a map link to see a preview of a map. Click the link to view the map.
- **Error** - view a list of Intermapper errors.
- **Full** - view a list of devices and networks associated with all open maps.
- **Outages** - view a list of current outages (devices and networks that are currently down) and previous outages (devices and networks that failed in the past, but have returned to service).
- **Device List** - view a list of devices and networks associated with all open maps.
- **Statistics** - view information about the current version of Intermapper under which the Web Server is running.
- **Help (menu)** - select from a menu of options that allow you to get information about the Intermapper Web client and the current version of Intermapper. View and download files in the Intermapper Settings folder, view the User and Developer Guides, and connect to the Intermapper Telnet server.

Setting the Interval for Reloading the Web Page

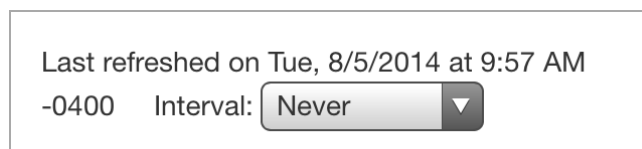
Intermapper pages can be set to refresh at a specified interval. This keeps the web page's information up-to-date.

To set the Reload interval:

- From the **Interval** menu, select one of the following reload intervals. The web browser refreshes the page at the specified interval.
 - Interval Menu on Computer



- Interval Menu on iPhone



Customizing Web Pages

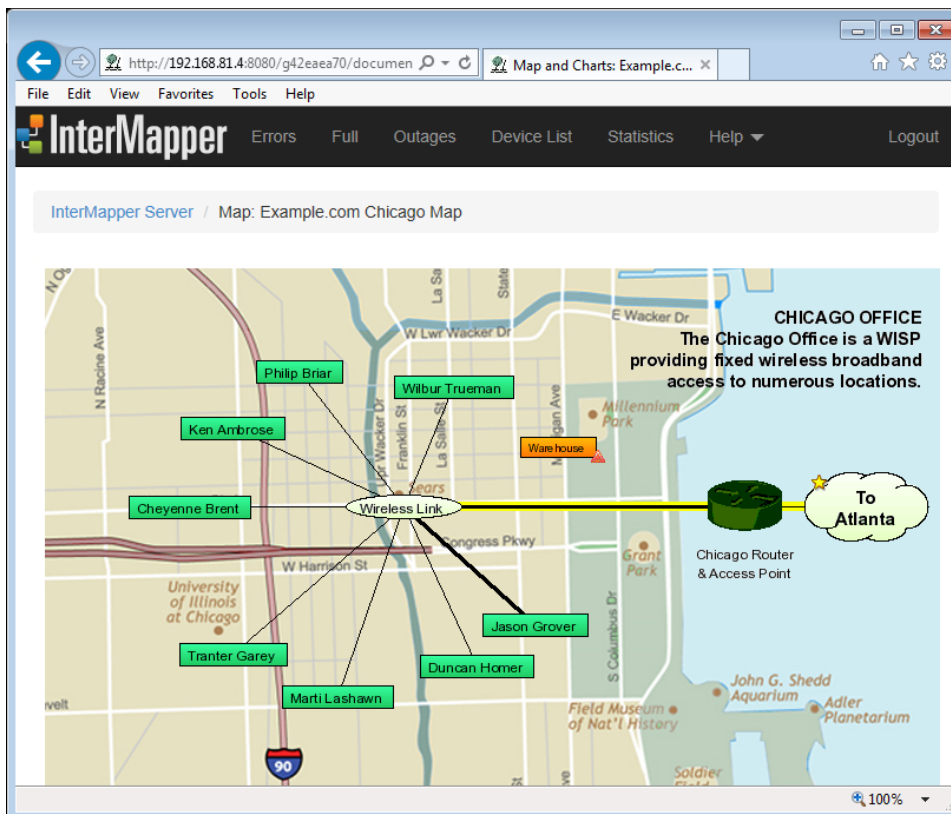
Intermapper's web page appearance is controlled by template files. For more information, see Customizing Web Pages in the [Developer Guide](#).

Using the Web Server

Each page that Intermapper serves contains the same controls at the top. The example below shows an Intermapper map as it appears in a web page.

NOTE:

To access the web server remotely, (that is, from a different machine connected to the network) you must configure the Intermapper firewall to permit the connection. You must also configure any other firewalls protecting the machine that is running Intermapper to allow traffic to the specified port. For more information, see [The Web Server](#) in the Server Settings section.



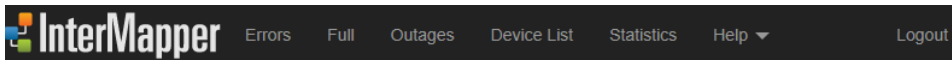
A typical Intermapper web page. the "Example.com" Chicago map.

The Intermapper web page typically has three parts:

- The header shows the map name or other title and a navigation bar for going to other pages. This is usually the same for every page.
- The content of the page varies, depending on which page is selected.
- The footer of the page shows the time the page was created.

Intermapper Web Page Navigation

Use the menu at the top of the Intermapper Web Page to access the available features of the web page. The example above shows a web page for a particular map. The image below shows the Intermapper Web Server menu, found at the top of each page.



Click any of the menu items at the top of the page to view the page. Here is a brief description of each page:

- **Home Page** - click the Intermapper logo to return to the Home page. View a list of open maps and the charts associated with those maps. Mouse over a map link to see a preview of a map. Click the link to view the map.
- **Error** - view a list of Intermapper errors.
- **Full** - view a list of devices and networks associated with all open maps.
- **Outages** - view a list of current outages (devices and networks that are currently down) and previous outages (devices and networks that failed in the past, but have returned to service).
- **Device List** - view a list of devices and networks associated with all open maps.
- **Statistics** - view information about the current version of Intermapper under which the Web Server is running.
- **Help (menu)** - select from a menu of options that allow you to get information about the Intermapper Web client and the current version of Intermapper. View and download files in the Intermapper Settings folder, view the User and Developer Guides, and connect to the Intermapper Telnet server.

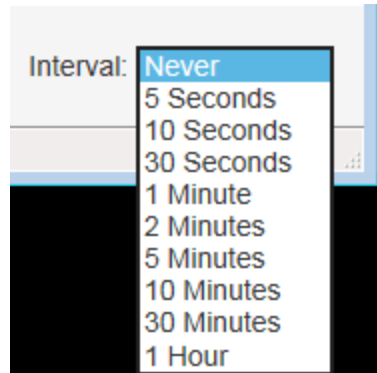
Setting the Interval for Reloading the Web Page

Intermapper pages can be set to refresh at a specified interval. This keeps the web page's information up-to-date.

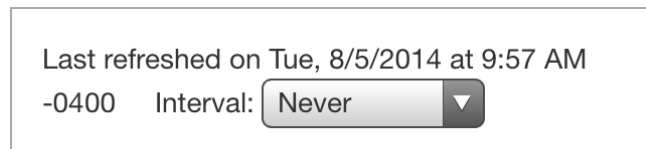
To set the Reload interval:

- From the **Interval** menu, select one of the following reload intervals. The web browser refreshes the page at the specified interval.

- Interval Menu on Computer



- Interval Menu on iPhone

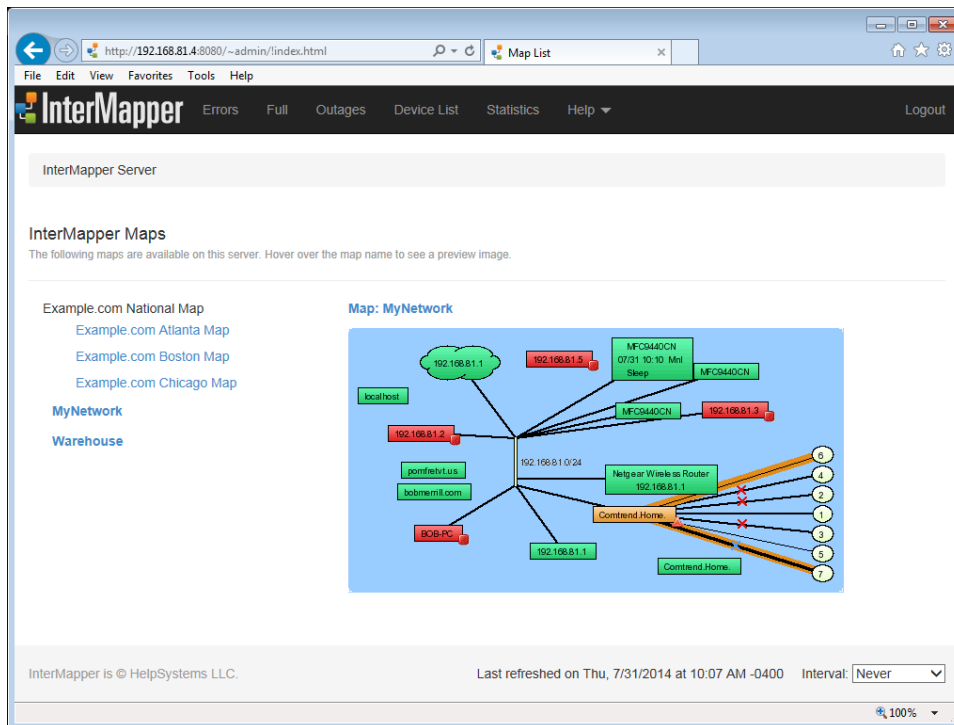


Customizing Web Pages

Intermapper's web page appearance is controlled by template files. For more information, see Customizing Web Pages in the [Developer Guide](#).

The Home Page

You can use the Home page to view a list of open maps and the charts associated with those maps.



The Intermapper Web Server Home page.

- Mouse over a map link to see a preview of a map.
- Click the link to view the map.

After you view a map:

- Click any link, device, or network on a map to view detailed information about that item.
- Click a chart link below the map if any charts have been created for this map. See [The Chart Web Page \(Pg. 692\)](#) for more information.
- View the map in Google Earth by clicking the link in Links to other pages.

NOTE:

A map on a web page is actually a snapshot image of the current state of the map at the time you request the page. The map image is static, so you need to refresh the page to see changes in the map state. You can use the **Interval** menu button to select the page's refresh interval.

Viewing Information for a Link, Device, or Network

Click any link, device, or network to view detailed information about that item. This is the same information that appears in a Status window. The following are the typical displays:

Device Status

Device Information

Name: router.company.net.
DNS Name:router.company.net.
Address: 192.168.1.1
Status: UP
Protocol:Ping/Echo
Up Time: n/a
Availability:100%(of 1 hour, 29 minutes, 12 seconds)
Packet Loss:0.0%(of 143 total attempts) [[Reset](#)]
Recent Loss:None
Last updated Jun 23, 12:16:42; interval: 30 seconds

Network Status

Network Information

Name: 192.168.1.0/24
IP Net:192.168.1.0/24 (255.255.255.0)
Sum In: 2 pkt/sec 548 byte/sec 0 error/min
Sum Out: 3 pkt/sec 316 byte/sec 0 error/min

Comment:

This is the network in the office.
It has an IP address of 192.168.1.0, and a subnet mask of 255.255.255.0.

Link Status

Interface Information (ifIndex = 1)

Device Name:router.company.net.
Description:EN1
Type: 10 MBit ethernetCsmacd (MTU=1500)
Status: UP for 4 days, 13 hours
Address: 192.168.1.1 (255.255.255.0)
MAC Address:00-00-C5-76-E2-EC

Interface Statistics

Utilization:0.01% (of 10 MBit bandwidth)
Percent Err:0.0% (59 pkts w/o error)
Transmit Statistics (0.01% utilization)
Pkt/Second:0 (5.88% multicast)
Byte/Second:73 (590 bps)

```

Err/Minute:0 (0 errors)
Disc/Minute:0 (0 discards)
Percent Err:0.0% (17 pkts w/o error)
Receive Statistics (0.01% utilization)
Pkt/Second:1 (59.5% multicast)
Byte/Second:93 (748 bps)
Err/Minute:0 (0 errors)
Disc/Minute:0 (0 discards)
Percent Err:0.0% (42 pkts w/o error)
Last updated Jun 23, 12:21:02; sample: 37.94 seconds.

```

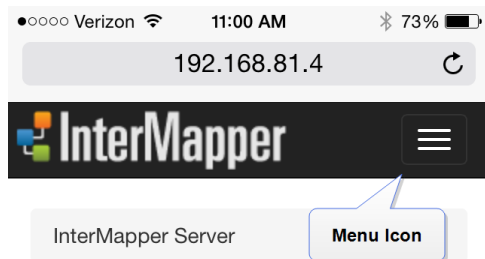
Map Status

When you click a Map Status item, the map associated with that device appears, rather than an information window.

Using Intermapper Web Server on Mobile Devices

The Intermapper Web Server supports viewing on mobile devices.

Tap the menu icon (shown at right) to view the web server menu.



InterMapper Maps

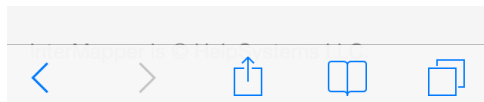
The following maps are available on this server. Hover over the map name to see a preview image.

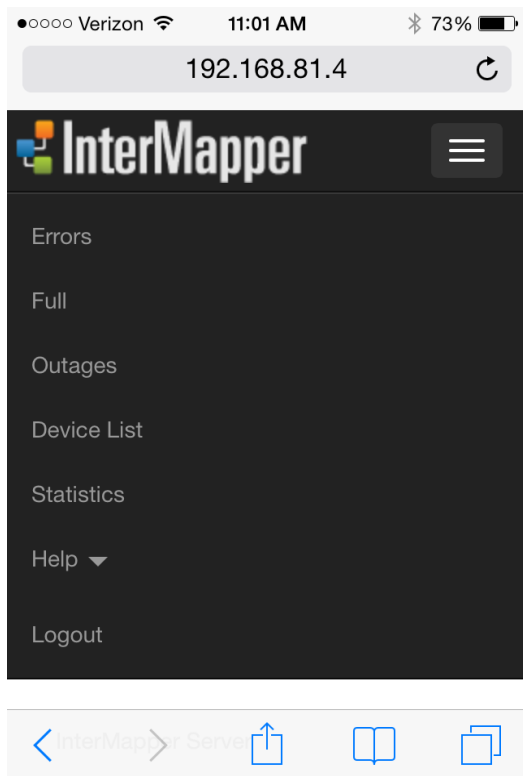
Example.com National Map

[Example.com Atlanta Map](#)

[Example.com Boston Map](#)

[Example.com Chicago Map](#)





Web Server menu on an iPhone

The Error and Full Pages

Use the **Error Page** to view devices, networks, and links that are down, or in alarm or warning states.

- If you are an InterMapper administrator, this page appears by default when you first connect your browser to the InterMapper web server.
- If you are not an administrator, the Error page is available only if you are a member of the FullWebAccess group.
- By default you are directed to the first map (alphabetically) in the map list to which you have access.

Use the Full Page to view all devices, networks, and links being monitored by InterMapper, not just those with problems.

Both the Error and Full web pages have the same format.

Click a link in the left column of either page to view detailed information about the link, device, or network.

The [Home Page \(Pg. 684\)](#) topic shows typical Device and Network Status.

The screenshot shows the Intermapper web interface at the URL `http://192.168.81.4:8080/~admin/error_screen.html`. The page title is "InterMapper Devices in Error". The breadcrumb trail is "InterMapper Server / Errors". The main heading is "Devices and Links with Errors". Below this, a summary line reads: "Jul 29 11:17:06 34 nodes, 1 down, 70 links, 1 down, 1075 pk/s, 120686 K by/s".

Device	Stat	SysUpTime (Down Since)	Avail	Loss	RTT	Probe	Address
Warehouse	ALRM		100.0	0.0	0	Map	127.0.0.1
192.168.11.222	DOWN	07/29 11:16 AM	99.3	3.2	0	Demo	192.168.11.222

Link	Prt	Stat	TPkt	TBytes	TErr	TDis	RPkt	RBytes	RErr	RDis	Util	Segment
Wired &	3	up	16	62277	1*	0	16	62277	1*	0	33.2%	to
John	1	up	18	0	1*	0	18	0	1*	0	0.0%	192.168.1.0/24
Susan	5	up	11	1602	1*	0	11	1602	1*	0	22.9%	192.168.1.0/24
Chicago Router	7	up	18	35342	2*	0	18	35342	2*	0	37.7%	To
Duncan Homer	1	up	31	0	6*	0	31	0	6*	0	0.0%	Wireless Link
Ken Ambrose	1	up	29	0	4*	0	29	0	4*	0	0.0%	Wireless Link
Philip Briar	1	up	14	0	2*	0	14	0	2*	0	0.0%	Wireless Link
Wilbur Trueman	1	up	19	0	2*	0	19	0	2*	0	0.0%	Wireless Link
Jason Grover	0	up	22	5596766	4*	0	22	5596766	4*	0	44.8%	Wireless Link
Jason Grover	0	up	22	5596766	4*	0	22	5596766	4*	0	44.8%	Wireless Link

The Intermapper Errors page

The screenshot shows the Intermapper web interface at the URL `http://192.168.81.4:8080/~admin/full_screen.html`. The page title is "InterMapper Full Device List". The breadcrumb trail is "InterMapper Server / Devices and Links". The main heading is "Full list of Devices and Links". Below this, a summary line reads: "Jul 29 11:17:52 34 nodes, 1 down, 70 links, 2 down, 1198 pk/s, 196169 K by/s".

Device	Stat	SysUpTime (Down Since)	Avail	Loss	RTT	Probe	Address
Wired &	UP		100.0	0.0	0	Demo	10.1.3.2
Fred	UP		100.0	0.0	0	Demo	192.168.5.172
Mary	UP		100.0	0.0	0	Demo	192.168.5.1
John	UP		100.0	0.0	0	Demo	192.168.5.171
Susan	UP		100.0	0.0	0	Demo	192.168.5.171
Chicago Router	UP		100.0	0.0	0	Demo	10.1.2.2
Duncan Homer	UP		100.0	0.0	0	Demo	192.168.4.174
Marti Lashawn	UP		100.0	0.0	0	Demo	192.168.4.177
Tranter Garey	UP		96.9	3.2	0	Demo	192.168.4.172
Cheyenne Brent	UP		93.9	3.3	0	Demo	192.168.4.175
Ken Ambrose	UP		100.0	0.0	0	Demo	192.168.4.173
Philip Briar	UP		100.0	0.0	0	Demo	192.168.4.178
Wilbur Trueman	UP		96.9	3.2	0	Demo	192.168.4.176
Jason Grover	UP		100.0	0.0	0	Demo	192.168.4.171
Warehouse	UP		100.0	0.0	0	Map	127.0.0.1
Router/	UP		100.0	0.0	0	Demo	192.168.1.2

The Intermapper Full page.

Viewing Summary Information

The top line shows a summary of items being monitored in all open maps.

- **date** and **time** the page was generated
- **number of nodes** being monitored
- **number of devices** currently shown as down
- **number of links** being monitored
- **number of links** currently shown as down
- **total packets per second** entering the network
- **total bytes per second** entering the network

Viewing Device Status

The first detailed section of the page shows *devices* that are down, or are in alarm or warning states. The Device section shows:

- **Device** - device name (click the link for more information)
- **Stat** - device status
- **SysUptime** - device uptime
- **Avail** - availability of the device
- **Loss** - packet loss
- **RTT** - round-trip time
- **Probe** - probe type
- **Address** - network address

Viewing Networks and Link Status

The second detailed section of the page shows *networks* and *links* that are down, or are in alarm or warning states. The Link section shows:

- **Link** - device name (click the link for more information)
- **Prt** - device port number
- **Stat** - device status
- **TPkt, TBytes, TErr, TDis** - transmit information (transmitted packets and bytes per second, transmit errors and discards per minute)
- **RPkt, RBytes, RErr, RDis** - receives information (received packets and bytes per second, received errors and discards per minute)

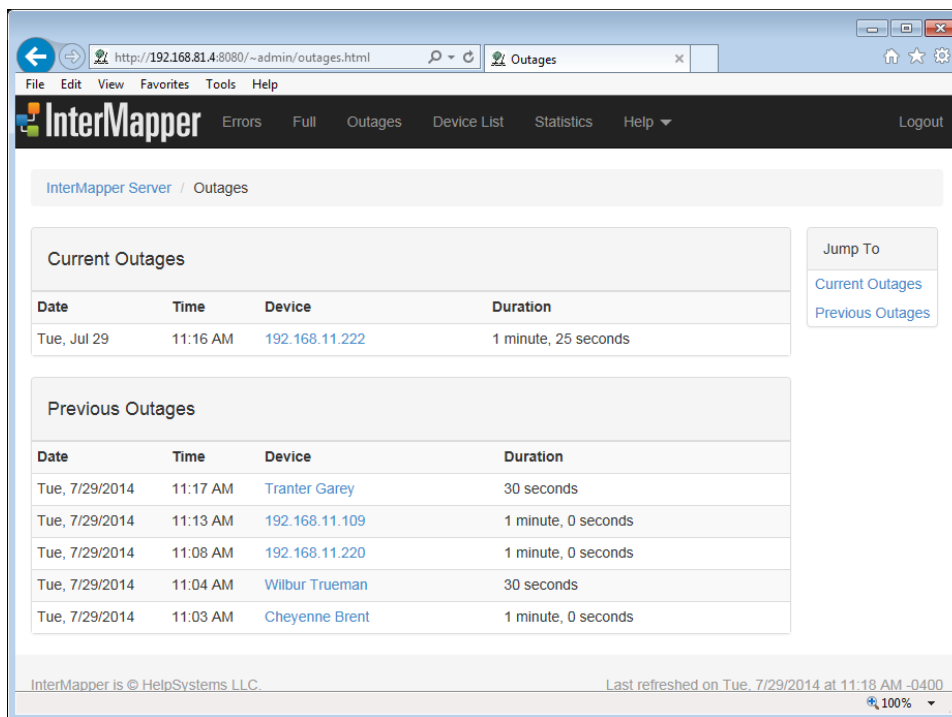
- **Util** - network utilization
- **Segment** - segment name (if any)

The Outages Web Page

Use the Outages web page to view a history of outages.

Click an active link on the Outages Web page to view detailed information as described in the [Map Web Page](#) topic.

The Outages web page lists up to 10 outages for each device.



The InterMapper Outages web page.

Device List Web Page

You can use the Device List web page to view a list of devices appearing in all open maps. The list shows each device's status, name, condition, and date and time of the last change in status.

Click a link to view detailed information about a device. The following example shows a typical Device List web page.

Status	Name	Condition	Date	Time	Probe	Port
Down	Susan	Down	07/29	11:20:15	Demo Probe	23
OK	Mary	OK	07/29	11:01:24	Demo Probe	23
OK	Router/	OK	07/29	11:01:24	Demo Probe	23
OK	Cheyenne Brent	OK	07/29	11:04:09	Demo Probe	23
OK	Chicago Router	OK	07/29	11:01:24	Demo Probe	23
OK	Duncan Homer	OK	07/29	11:01:24	Demo Probe	23
OK	Marti Lashawn	OK	07/29	11:01:24	Demo Probe	23
OK	Fred	OK	07/29	11:01:24	Demo Probe	23
OK	SMTP	OK	07/29	11:01:24	Demo Probe	23
OK	Ken Ambrose	OK	07/29	11:01:24	Demo Probe	23
OK	Philip Briar	OK	07/29	11:01:24	Demo Probe	23
OK	Wilbur Truman	OK	07/29	11:05:18	Demo Probe	23

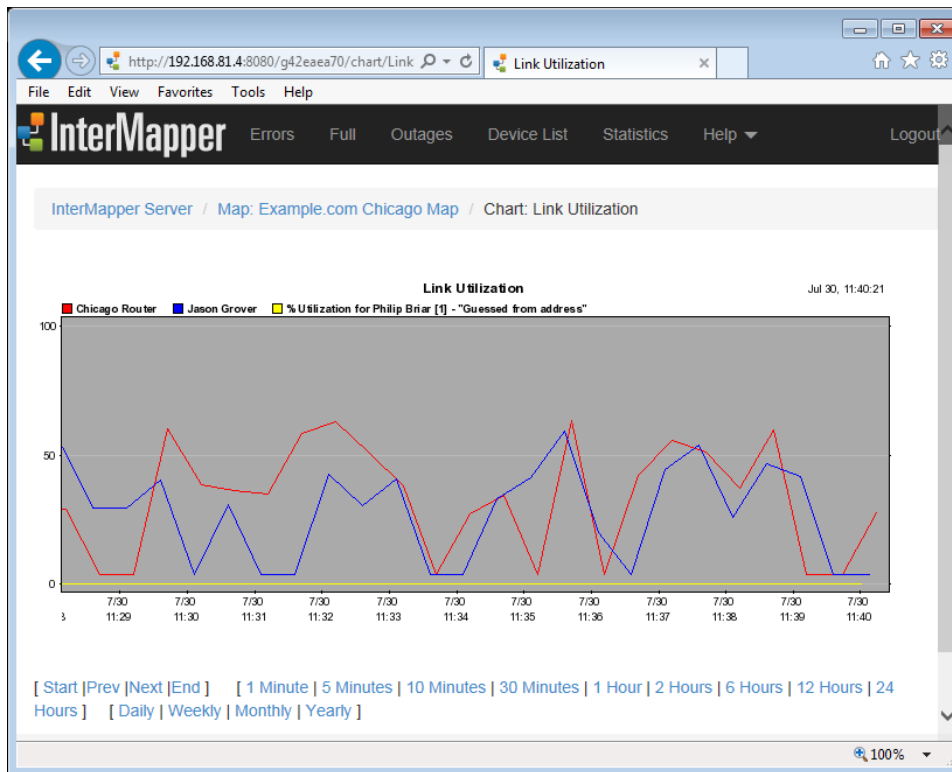
The Web Device list shows the status of all the devices Intermapper is monitoring, sorted by severity of their status.

Viewing a Chart

Use the Chart web page to view the selected chart.

When view a map's page, a list of the charts associated with the map is displayed. The list appears only if charts have been created.

- Click a chart name to view the chart.
- Click the **Start**, **Prev**, **Next**, or **End** links to show different parts of the history.
- Click the links below the chart to choose the period you want to view.



Telnet Server Command Reference

The Telnet Server uses a text-based command-line interface to provide information about devices and networks in maps that are open in InterMapper.

The following is a summary of the features and functions available from the Telnet Server, as shown through the server's help system. For each command listed below, click [details] to view the server help for that command:

```
Welcome to the InterMapper [version #] operations interface.
Enter 'help' for command list.
```

```
> help
=====
```

ERROR

```
- Shows a report of all devices and links that exceed some
  threshold. This
    report is updated every minute. For detailed information
  about the fields
    and columns of this report, type "help error". This is the
  default command
    when you connect. \[ details \] \(Pg. 696\) (Abbreviations: "E",
  "ERR")
```

FULL

- Shows a report of all devices and links being monitored. [\[details \]](#) **(Pg. 696)** (Abbreviations: "F")

NODE <name-prefix>

- Shows a report of the named device using the same format as the "ERROR" report. This report is updated every time Intermapper polls the device. [\[details \]](#) **(Pg. 696)** (Abbreviations: "N")

BUS <name-prefix>

- Shows a report of the named network or segment using the same format as the "ERROR" report. This report is updated every minute. [\[details \]](#) **(Pg. 696)** (Abbreviations: "B")

- DOWN-** Lists all devices that are down. The same functionality is also provided by the ERRORS command. [\[details \]](#) **(Pg. 697)**

- LDOWN-** Lists all interfaces (ie links) that are down. The same functionality is also provided by the ERRORS command. [\[details \]](#) **(Pg. 699)**

LOG []

- Displays the last entries from the event log window and continuously displays new log lines. [\[details \]](#) **(Pg. 700)**

KALI [<conn> ["compress" | "kill"]]

- Displays list of Kali connections and allows you to debug them. [\[details \]](#) **(Pg. 698)**

KALID

- Displays a list of the maps, log, lists, and other shared resources open by each Remote connection. [\[details \]](#) **(Pg. 699)**

HELP [<topic>]

- Without a parameter, the help command displays this help text. If you include the name of the command as the parameter, it displays detailed information about the format of the report generated by it. [\[details \]](#) **(Pg. 698)**

QUIT- End the telnet session and disconnect. [\[details \]](#) **(Pg. 700)**

RELOAD

- Closes all map files and reopens them. This command is only implemented in the server/daemon version of Intermapper. [\[details \]](#) **(Pg. 700)**

REMOTE <hostname> [<port>]

- Initiates a remote connection with a client at hostname, listening on <port>, rather than the usual procedure of a client initiating a connection with the server.

This is useful when the server is behind a firewall. Intermapper Support may

occasionally ask you to do this in order to let us take a look at your system

without requiring you to adjust your firewall. If the port is not specified, it is assumed to be 8181.

DETAILS < "net" | "graph" | "collaborator" | "smtp" | "probe" >

- Toggles detailed logging to the debug log for the indicated class of events. Intermapper Support may occasionally ask you to do this in order to provide us with more detailed information about what is happening when you run Intermapper.

SERVER <server> < "start" | "stop" | "status" > [<port>] ["secure"]

- Start, stop or change one of the three servers: Web, Telnet or Remote. [\[details \]](#) **(Pg. 700)**

TELNET

- Displays a list of current connections to the Telnet server. [\[details \]](#) **(Pg. 701)**

USERS [<UID>] - Displays a list of users with user IDs. Include the user ID to delete the user.

WEB

- Displays a list of current connections to the Web server. [\[details \]](#) **(Pg. 701)**

Command Details

> **help error**

The ERROR, FULL, NODE, and BUS commands emit a report with three parts:

- (1) a status line summarizing the condition of the entire network
- (2) a node report
- (3) a link report.

Example:

```
Jul 31 11:11:58    2 nodes,    1 down,    8 links,    0 down,    461
pk/s,    141 K by/s
```

Name	Stat	SysUpTime	Probe	Address
egg-1	DOWN	0+00:00:00	ICMP	127.110.13.210

Name	Prt	Stat	TPkt	TBytes	TErr	TDis	RPkt	RBytes	RErr
RDis		Util							
Segment									
egg-1	1	UP	46	13790	0	0	67	10152	12*
0	1% 127.0.13.0/24								
egg-1	2	UP	78	8330	0	0	586	144524	14*
0	12% 127.0.14.0/24								

(1) THE STATUS LINE

```
Jul 31 11:11:58    2 nodes,    1 down,    8 links,    0 down,    461
pk/s,    141 K by/s
```

In order, these fields are:

- the date and time of the report
- the total number of devices
- the number of devices which are down
- the total number of links
- the number of links which are down
- the sum of pkts per second transmitted on all links
- the sum of bytes per second transmitted on all links

(2) NODE REPORT

Name	Stat	SysUpTime	Probe	Address
------	------	-----------	-------	---------

The columns are:

- | | |
|-----------|--|
| Name | - the name of the device |
| Stat | - the status of the device (UP, DOWN, or ACK) |
| SysUpTime | - the number of days + hh:mm:ss that the device has been running |
| Probe | - the type of probe used to check the device |

Address - the address of the device (where the probes are sent)

(3) LINK REPORT

```
Name          Prt Stat TPkt TBytes TErr TDis  RPkt RBytes RErr
RDis  Util
Segment
```

The columns are:

Name - the name of the device
 Prt - the interface number
 Stat - the status of the interface (UP, DOWN, or ACK)
 TPkt - the number of pkts per second transmitted on this interface
 TBytes - the number of bytes per second transmitted on this interface
 TErr - the number of packets per minute lost due to errors
 TDis - the number of packets per minute dropped due to resource limitations
 RPkt - the number of pkts per second received on this interface
 RBytes - the number of bytes per second received on this interface
 RErr - the number of packets per minute received with an error
 RDis - the number of packets per minute dropped due to resource limitations
 Util - the percentage utilization of the interface
 Segment - the name of the network or segment attached to this interface

The * following a value indicates that the value is above the threshold. This is useful because it tells you why the link is being displayed as part of the error report.

> **help down**

The DOWN command lists all devices which currently have the 'DOWN' or 'DOWN-ACK' status.

Each line of the DOWN list has the format:

```
mm/dd hh:mm:ss  DOWN      <Device-Name>
```

For devices which are acknowledged down, the following format is

used:

mm/dd hh:mm:ss DOWN-ACK <Device-Name>

> **help**

HELP [<topic>]

- Without a parameter, the help command displays this help text. If you include the name of the command as the parameter, it displays detailed information about the format of the report generated by it.

> **help kali**

KALI [["compress" | "kill"]]

Displays a list of current Intermapper Remote Access connections and allows you to monitor them.

When you enter "KALI" without any arguments, the response is a list of the current Intermapper Remote Access connections in the form:

ID	USER	REMOTE ADDRESS	IN	OUT	
LOGIN@					
366a58	<listener>	<server-port 8181>	0	0	-
485d58	Guest	198.115.166.18:58619	20339	177408	Oct 02, 15:51:12
2d18b8	<listener>	<server-port 8181>	0	0	-

The second and third columns identify the user and their source IP address. The two users marked "<listener>" are the server's two pending listening connections for port 8181.

The first column of output is the identifier for the connection. To monitor an existing connection, type "KALI <conn>" where <conn> is a connection ID.

To monitor the next new connection to the server, use "next" for the connection ID; i.e. type "KALI NEXT".

Monitoring a remote connection turns off compression for the data stream; this makes it easier to see the actual traffic. To leave compression enabled when while monitoring, include the "compress" option; i.e. type

"KALI <conn>

COMPRESS".

To forcibly disconnect an existing connection, type "KALI <conn> KILL".

This command will terminate the remote connection and release its resources on the server.

> **help kalid**

Displays a list of the maps, log, lists, and other shared resources open by each Remote connection.

Here is some sample output:

```
+ CKaliOpenMapList [2d6008] user='Guest' [ADMIN]
  - [485d58] Guest@198.115.166.18:58619
+ CKaliOpenLogList [351cd8] addr='198.115.166.18' user='Guest'
  [ADMIN]
  - [485d58] Guest@198.115.166.18:58619
+ CKaliOpenSoundSetList [351d68]
  - [485d58] Guest@198.115.166.18:58619
```

This indicates that the remote connection [485d58] is responsible for an "open map list", an "open log list", and an "open sound list". Essentially, this means that client will be notified of any changes to those lists. If this user had opened a map, you would see them registered for that "open map"; i.e. they would be notified of any changes.

Multiple connections may be registered for the same resource, the output above only shows the server state with one connection.

> **help ldown**

The LDOWN command lists all interfaces which currently have the 'DOWN'

status. The LDOWN report does not include interfaces which are hidden

and therefore not being polled.

Each line has the following format:

```
mm/dd hh:mm:ss DOWN <Device-Name>:<ifIndex>:<ifDescr>
```

<ifIndex> is the index of the interface in the interface table, and <ifDescr> is a description of the interface.

> help log

Displays the last <num-lines> entries from the event log window and

continuously displays new log lines.

The format of the LOG output is exactly the same as the format of the

"Event Log" window of the Intermapper program.

> help quit

QUIT

- End the telnet session and disconnect.

> help reload

RELOAD

Closes all map files and reopens them. This command is only implemented in the server/daemon version of Intermapper.

This command is for experimental purposes. You should avoid using it; it may go away in future versions.

> help server

SERVER <server> < "start" | "stop" | "status" > [<port>] ["secure"]

Start, stop or change one of the three servers: Web, Telnet or Remote.

To start a server on the same or different port number (with SSL/TLS disabled), type:

```
server <server> start <port>
```

To start the server with SSL/TLS enabled, type:

```
server <server> start <port> secure
```

In both cases, <server> must be one of "web", "telnet" or "remote".

To stop a server, type:

```
server <server> stop
```


Note: You cannot stop the Telnet server using the SERVER command. However, you can restart the telnet server on a different port number. When you do this, your own telnet connection will be disconnected immediately.

To receive a quick status report on all three servers, type "server status". This command combines the output of the "web", "telnet" and "kali" commands.

> help telnet

TELNET

Displays a list of current connections to the Telnet server.

```
ID USER REMOTE ADDRESS IN OUT LOGIN@
404c28 <listener> <server-port 23> 0 0 -
3f63a8 Guest 192.168.1.21:49176 0 0 -
2d60e8 <listener> <server-port 23> 0 0 -
```

This command is similar in output to the KALI command. It lists the source and login ID of any existing telnet connections. However, unlike the KALI command, you cannot monitor or terminate telnet connections using the TELNET command; you can only receive a status report.

Note: The IN, OUT, and LOGIN@ stats are not implemented for the TELNET command.

> help web

WEB

Displays a list of current connections to the Web server. The web server normally does not allow HTTP connections to linger, so the list of current connections should never grow very large.

```
ID USER REMOTE ADDRESS IN OUT LOGIN@
38af68 <listener> <server-port 80> 0 0 -
35f518 <listener> <server-port 80> 0 0 -
```

```
478478 <listener> <server-port 80> 0 0 -
39f308 <listener> <server-port 80> 0 0 -
473e98 <listener> <server-port 80> 0 0 -
481bb8 <listener> <server-port 80> 0 0 -
```

This command is similar in output to the KALI command. It lists the source and login ID of any existing web connections. Since the web server has to deal with the possibility of many simultaneous hits, the number of reserve pending listeners is larger than for the other server.

Unlike the KALI command, you cannot monitor or terminate web connections using the WEB command; you can only receive a status report.

Note: The IN, OUT, and LOGIN@ stats are not implemented for the WEB command.

Configuring Intermapper Server Using a Command Line

A number of command line options are available for use with Intermapper.

Usage:

```
Intermapperd [OPTIONS] (macOS/Linux)
Intermapper.exe [OPTIONS] (Microsoft Windows)
```

*For macOS and Linux, you might need to use the full path to the executable (/usr/local/bin/Intermapperd) in order for some options to work correctly.

Argument	Description
-h -? --help	Display this help text and exit.
-v --version	Print the version number.
-f <file>	Use the specified configuration file.

-A <user-addr>	Add the specified 'user[:pass]@address' to the access list. Extended options: -u --user <name> Run as this user. (Overrides 'User' directive) --group <name> Run as this group. (Overrides 'Group' directive)
-u --user <name>	Run as this user. (Overrides 'User' directive)
--group <name>	Run as this group. (Overrides 'Group' directive)
--settings <path>	Specify path to 'Intermapper Settings' directory. (Overrides 'SettingsFolder' directive)
--fonts <path>	Specify path to 'Font' directory. (Overrides 'FontFolder' directive)
--listen <address>	Listen only on the interface with the specified IPv4 address. Disable IPv6.
--port <port>	Listen for remote connections on the specified TCP port.
--no-daemonize	Do not fork and disassociate from the controlling terminal.
--no-ipv6	Disable IPv6 support.
--no-ssl	Disable SSL for remote connections.
--test-only	Run tests and exit.
-d --debug	Enable debug mode; don't disassociate from controlling terminal.
--printconfig	Print the daemon's configuration.
--getenv <var>	Get the value of <var> in the InterMappe renvironment.
--setenv <var>=<val>	Set the value of <var> to <val> in the Intermapper environment.
--wrap <filename>	Wrap the probe bundle defined by the bundle header at <filename>.
--output <filename>	Put output of wrap operation in file at <filename>.
--suppress-avail	Suppress the 'availability' statistic in device status windows.
--verify- permissions	Check the permissions of all files in the 'Intermapper Settings' directory.
--check-upgrade <date>	Check the release manufacture <date> against the maintenance contract date.

<code>--detail <log></code>	Turn on detailed logging for the type indicated by <log>.
<code>--ciphers <all default list></code>	Show supported SSL ciphers.
<code>--chart-purge <days></code>	Purge chart data to maximum <days> history. NOTE: If you have a large amount of chart data, using this option to purge chart data may take a significant amount of time. If you start Intermapper with this option, monitoring may be affected adversely until the purge is completed.

Configuring Intermapper Server Using a Command Line

A number of command line options are available for use with Intermapper.

Usage:

```
Intermapperd [OPTIONS] (macOS/Linux)
Intermapper.exe [OPTIONS] (Microsoft Windows)
```

*For macOS and Linux, you might need to use the full path to the executable (/usr/local/bin/Intermapperd) in order for some options to work correctly.

Argument	Description
<code>-h -? --help</code>	Display this help text and exit.
<code>-v --version</code>	Print the version number.
<code>-f <file></code>	Use the specified configuration file.
<code>-A <user-addr></code>	Add the specified 'user[:pass]@address' to the access list. Extended options: <code>-u --user <name></code> Run as this user. (Overrides 'User' directive) <code>--group <name></code> Run as this group. (Overrides 'Group' directive)
<code>-u --user <name></code>	Run as this user. (Overrides 'User' directive)
<code>--group <name></code>	Run as this group. (Overrides 'Group' directive)

<code>--settings <path></code>	Specify path to 'Intermapper Settings' directory. (Overrides 'SettingsFolder' directive)
<code>--fonts <path></code>	Specify path to 'Font' directory. (Overrides 'FontFolder' directive)
<code>--listen <address></code>	Listen only on the interface with the specified IPv4 address. Disable IPv6.
<code>--port <port></code>	Listen for remote connections on the specified TCP port.
<code>--no-daemonize</code>	Do not fork and disassociate from the controlling terminal.
<code>--no-ipv6</code>	Disable IPv6 support.
<code>--no-ssl</code>	Disable SSL for remote connections.
<code>--test-only</code>	Run tests and exit.
<code>-d --debug</code>	Enable debug mode; don't disassociate from controlling terminal.
<code>--printconfig</code>	Print the daemon's configuration.
<code>--getenv <var></code>	Get the value of <var> in the InterMappe renvironment.
<code>--setenv <var>=<val></code>	Set the value of <var> to <val> in the Intermapper environment.
<code>--wrap <filename></code>	Wrap the probe bundle defined by the bundle header at <filename>.
<code>--output <filename></code>	Put output of wrap operation in file at <filename>.
<code>--suppress-avail</code>	Suppress the 'availability' statistic in device status windows.
<code>--verify-permissions</code>	Check the permissions of all files in the 'Intermapper Settings' directory.
<code>--check-upgrade <date></code>	Check the release manufacture <date> against the maintenance contract date.
<code>--detail <log></code>	Turn on detailed logging for the type indicated by <log>.
<code>--ciphers <all default list></code>	Show supported SSL ciphers.
<code>--chart-purge <days></code>	Purge chart data to maximum <days> history. <div> NOTE: If you have a large amount of chart data, using this option to purge chart data may take a significant amount of time. If you start Intermapper with this option, monitoring may be affected adversely until the purge is completed. </div>

Command-Line Options for Intermapper Clients

Two client applications are available for Intermapper:

- **Intermapper client** runs on the same machine as Intermapper Server, so it has a limited set of command-line arguments.
- **Intermapper Remote Access client** runs on any machine, and connects to multiple Intermapper servers, so it has a larger set of options.

Usage:

```
java -jar [jar file] [Options]
```

- For Intermapper client, the jar file name is `Intermapper.jar`.
- For Intermapper Remote Access, the jar file name is `Intermapper_RemoteAccess.jar`.
- Depending on your installation, you may need to change your working directory, supply the full path to the jar file, or both. See *Microsoft Windows Users* on page 707, below.

You can call Intermapper Remote Access from a command line, and control a significant number of functions. This can be useful for automating the updating of maps, or for various testing purposes.

NOTE: The examples below assume the Intermapper server is running on the host you are connecting to.

Intermapper clients support the following command-line arguments:

NOTE:

- **IMRA:** applies to Intermapper Remote Access client only
- **Both:** applies to both Intermapper and Intermapper Remote Access clients

Argument	Client	Description
-host --host <HOST>	IMRA	connect to the specified HOST
-port --port <PORT>	Both	connect to the specified PORT on HOST (defaults to 8181)

-map --map <MAP_NAME>	Both	load the specified map(s) from HOST. For multiple maps, use one "--map" option per map
-import --import <FILE_NAME>	Both	import the specified file (use - for stdin)
-importmap --importmap <FILE_NAME>	Both	import the specified map.
-export --export <EXPORT-SPEC>		export the specified data to stdout. Note: Data for all maps is exported.
-exportmap --exportmap <MAP_ID>	Both	export the specified map Note: The easiest way to get the map ID is to look in the Maps folder in the Intermapper Settings folder. Each map name has a prefix that begins with "g". The text between the "g" and the hyphen ("-") is the Map ID.
-f --file <FILE_NAME>	Both	open the specified shortcut file
-d --debug <DEBUG_CONFIG_FILE>	Both	use the specified configuration file to configure debugging output
-D<name>=<value>	Both	set a system property
-user --user <USER>	IMRA	log in as USER
-pass --pass <PASSWORD>	IMRA	log in as USER with PASSWORD
-ignore-cert-check	IMRA	accept all server SSL certificates without prompting
-agree-to-license	Both	accept the End User License Agreement
-version --version	Both	print product version
-env --env	Both	print out system properties
-test --test [TIMEOUT]	Both	test the connection - automatically quit after TIMEOUT seconds
-h -? --help	Both	print this help message

Microsoft Windows Users

The syntax for Microsoft Windows users is essentially the same as the Linux examples below, except that the command line may require that the working directory must be set to the Intermapper installation folder, or Java jar file must include the full Windows path.

The following example sets the working directory to the Intermapper server installation folder, invokes java with the .jar file, and opens the MyNetwork1 and MyNetwork2 maps.

```
cd "C:\Program Files\Intermapper"java\bin\java.exe -jar "Intermapper.jar" --map
MyNetwork1 --map MyNetwork2
```

Import Command Examples

To import to a specified server, IM Remote is invoked as follows:

```
java -jar <jar-file> --host <Intermapper-server> [--user <username> --pass <password>]
--import <import-file>
```

The example below reads imported data from newdata.tab.

```
java -jar Intermapper_Remote Access.jar --host big.dartware.com --user admin --pass
adminpw --import newdata.tab
```

The example below reads imported data from *stdin*.

```
java -jar Intermapper_Remote Access.jar --host big.dartware.com --user admin --pass
adminpw --import -
```

The stdin form of the --import option allows users to create self-contained executable files that import stuff:

```
#!/usr/bin/java
-jar Intermapper_Remote Access.jar --host big.helpsystems.com --import -#import blah
blah
```



```
blah blah blah
blah blah blah
blah
```

One use for this would be to automate testing of Intermapper Server.

Export Command Examples

To export from a specified server, IM Remote is invoked as follows:

```
java -jar <jar-file> --host <Intermapper-server> [--user <username> --pass <password>]
\
  --export "format=<output-type> table=<table-name> fields=<field-list>
```

The example below writes exported data to *stdout*.

```
java -jar Intermapper_Remote Access.jar --host big.dartware.com --user admin --pass
adminpw --export "format=tab table=devices fields=*
```

Invoking Intermapper Clone

CloneIM (or CloneIM.sh for Microsoft Windows systems) is a script that synchronizes a local Intermapper installation with (or mirrors a file system directory from) a remote Intermapper server. It creates successive requests to the remote server's embedded web server by either HTTP or HTTPS using a curl command. It is supported on macOS, Linux, and Microsoft Windows systems that have Cygwin.

If your Microsoft Windows installation of Intermapper does not include Cygwin, you can use the VBScript implementation CloneIM.vbs. In the default invocation, CloneIM copies all accessible resources from the following categories from the Intermapper server on the specified host to the corresponding locations in the local Intermapper server installation: icons, sounds, mibs, probes, tools, webpages, fonts, extensions, maps, and translations. Alternatively, the -D (or /d for Microsoft Windows systems) option allows you to specify an alternate location in the local file system to which the resources are copied instead. You can limit the categories of resources transferred by specifying one or more categories as positional parameters. Note that downloading of chart data is not supported. The Preferences database is always downloaded.

Linux, macOS, and Cygwin on Microsoft Windows

For Linux and macOS systems, the script is called CloneIM. This script is used to synchronize local and remote Intermapper servers using the following command:

CloneIM options categories

For example,

```
CloneIM [-[bs]] [-S] [-q] [-C] [-v] [-h] [-r remote-host] \  
        [-P protocol] [-t port] [-u user [-p password]] \  
        [-D target-dir] [-L log-file] \  
        \
```

For Cygwin on Microsoft Windows systems, the script is called CloneIM.sh. This script is used to synchronize local and remote Intermapper servers using the following command:

sh CloneIM.sh options categories

For example,

```
sh CloneIM.sh [-[bs]] [-S] [-q] [-C] [-v] [-h] [-r remote-host] \  
\  
        [-P protocol] [-t port] [-u user [-p password]] \  
        [-D target-dir] [-L log-file] \  
        \
```

Options

Argument	Description
-b	bounces the local Intermapper server across synchronization (if appropriate)
-s	the synonym for -b

Argument	Description
-S	<p>Runs in secure mode. Normally, ClonelM uses the HTTP protocol to connect to the remote server. If the -P (protocol) option is used to specify HTTPS but the -S option is not used, ClonelM connects to the server using HTTPS and the port specified by the -t option (or it defaults to port 443), it does not check the client SSL certificate.</p> <p>If -S is specified, ClonelM uses the HTTPS protocol and the specified port (or it defaults to port 443) and checks the client SSL certificate. On each platform where you are using the shell script implementation of ClonelM, make sure that the SSL certificate for the target Intermapper server is accessible to your local implementation of the curl command. On Cygwin, the relevant implementation of curl can be Microsoft Windows or the Cygwin, depending on your Cygwin installation.</p> <p>You can verify that you have the correct certificate using a browser (such as Mozilla Firefox or Chrome) hosted by your intended host for ClonelM to access the URL (<code>https://Intermapper server IP:port/~files</code>). If you can access the URL through your browser without adding a security exception, and your browser and curl are referencing the same certificate storage, you can use ClonelM with the -S option.</p> <p>SSL certificates are sometimes bound to a domain, server name, or hostname. They are installed on a server to tie an organization's identity to its location. For this reason, they are only granted for a Fully Qualified Domain Name (FQDN). This means that you might need to specify the target Intermapper server hostname as an FQDN when supplying it as the argument for the -r option when using the -S option.</p>
-q	operates quietly
-C	assumes compatibility
-v	prints the version number
-h	prints the Help message
-P	specifies the protocol (<code>http</code> by default or <code>https</code> which is implied by -S)
-r	specifies the remote host with which to synchronize
-t	specifies the remote Intermapper server's web service listener port (defaulted from protocol)
-u	specifies the user that invokes the web service. The default is <code>admin</code> .

Argument	Description
-p	specifies the user's password for the destination Intermapper server. The default is <code>password</code> .
-L	specifies the log file to which to append execution details. Use <code>-</code> for none.
-D	specifies the local destination directory. The default is the local Intermapper installation.

Categories

- icons
- sounds
- mibs
- probes
- tools
- webpages
- fonts
- extensions
- maps
- translations

Files

Linux Systems

```
/var/local/InterMapper_Settings/Scripts/CloneIM
```

macOS Systems

```
/Library/Application Support/InterMapper_  
Settings/Scripts/CloneIM
```

Microsoft Windows

For Microsoft Windows systems, the script is called `CloneIM.vbs`. This script is used to synchronize local and remote Intermapper servers using the following command:

```
cscript CloneIM.vbs options categories
```

Options

NOTE:

For the following options, you can alternatively use the words listed after the single-letter options. For example, for `/r`, you can also use `/host`, or `/remote-host`.

Argument	Description
<code>/r</code> <i>host,remote-host</i>	Specifies the Intermapper server host from which to make the download requests. Because the default remote host name is <code>intermapper1</code> , this option is typically mandatory. Unless the <code>/d</code> option is supplied, this is an error that specifies the local host as the argument to this option.
<code>/p protocol</code>	Specifies the protocol used for making resource requests to the remote server. <i>protocol</i> must be <code>http</code> or <code>https</code> . The default is <code>http</code> .
<code>/t port</code>	Specifies the port number used for resource requests to the remote server. The default is <code>80</code> for <code>http</code> and <code>443</code> for <code>https</code> .
<code>/s</code>	<p>Runs the <code>curl</code> command in secure mode. Normally, <code>CloneIM.vbs</code> uses the HTTP protocol to connect to the remote server. If <code>/p</code> (protocol) is specified with <code>/p:https</code> but <code>-s</code> is not used, <code>CloneIM.vbs</code> uses <code>https:443</code> to connect to the remote server and ignores checking the client SSL certificate.</p> <p>If <code>/s</code> is used, <code>CloneIM.vbs</code> uses <code>https:port</code> to connect to the remote server and checks the client SSL certificate.</p> <p>On Microsoft Windows, you should import the SSL certificate that the Intermapper server is using to a local browser, such as Mozilla Firefox or Chrome. If you can verify that <code>https://IM Server IP/port/~files</code> (the port is usually <code>443</code>) works on your browser without SSL certificate error (where it does not use an exception), then you should be able to use <code>CloneIM.vbs</code> with the <code>/s</code> option.</p> <p>SSL certificates are sometimes bound together to a domain and server name or hostname. They are installed on a server to associate an organization's identity to its location. For this reason, they are only granted to a Fully Qualified Domain Name (FQDN) because the server address specified with the <code>/r</code> option might need to be the FQDN of the server.</p>

Argument	Description
<i>/u user</i>	Specifies the Intermapper user account that is making the requests to the remote server. The account must be an Intermapper administrator within the remote Intermapper server. In the ClonelM script, as distributed, the default user account is <code>admin</code> .
<i>/pw password</i>	Specifies the password for the Intermapper user account that is making the requests to the remote server. You cannot specify a password without specifying a user. In the ClonelM script, as distributed, the default is <code>password</code> .
<i>/d target-dir</i>	By default, ClonelM.vbs downloads the requested resources into the Intermapper Settings directory of the local Intermapper installation. You can use this option to specify an alternative directory as the root directory of a sub-tree of the file system into which the resources are downloaded. The directory is created if it does not already exist. Otherwise, if ClonelM is ran with the root privilege, the directory must be empty to avoid errors.
<i>/b</i>	If ClonelM.vbs is required to overwrite the installation directory of the local Intermapper installation, it checks if the local Intermapper server is running. By default, it terminates with an error message if the local server is active. By supplying this option, you can request that it attempts to deactivate the local Intermapper server before the first download request and attempt to reactivate it before a successful termination (after completing the last download request).
<i>/L log</i>	ClonelM normally writes time-stamped records to a log file. By default, the log file is ClonelM.log in the current directory. This option allows the specification of an alternative log file. You can suppress logging using the <code>/L:-</code> or <code>/L-</code> options.
<i>/q</i>	Operates the command quietly. By default, ClonelM.vbs displays a message verifying each download request. This option suppresses these messages.
<i>/v</i>	Instructs ClonelM.vbs to display a message including the Intermapper version number.
<i>/h</i>	Instructs ClonelM.vbs to display a help message and then terminate.

Categories

- icons
- sounds
- mibs
- probes

- tools
- webpages
- fonts
- extensions
- maps
- translations

File

C:/ProgramData/InterMapper/InterMapper
Settings/Scripts/CloneIM.vbs

NOTE:

The CloneIM.vbs script can only be run by the intermapper and administrator users because the text might contain a hard-coded default password. If you want to enforce a policy prohibiting this, you can relax the execution permission criteria. Contact Fortra before attempting such configuration. When CloneIM.vbs is invoked to copy maps from the remote server, it retrieves only enabled maps. Disabled maps in the remote Intermapper installation are ignored. CloneIM.vbs always connects to the Intermapper Server in IPv4 mode. If you use CloneIM.vbs to synchronize Intermapper installations at differing major or minor versions, the version skew is detected and reported. The synchronization attempt is abandoned unless you specify the /d option. If your destination directory is not the local Intermapper installation, execution proceeds, otherwise an interactive execution prompts for confirmation from the standard input.

Using Intermapper With Splunk

Intermapper works with Splunk by sending syslog entries in a specific format when an Intermapper device changes state. An add-on application in Splunk allows you to analyze and view various events through an Intermapper-specific dashboard.

Use the information below to connect Intermapper to Splunk.

System Requirements

To use Splunk with Intermapper, you need the following:

- A local or remote installation of Splunk Enterprise.
- The Intermapper web server must be running.
- The Splunk machine must have access to the Intermapper server.
- A syslog notifier that sends information to Splunk must be attached to all devices you want to track with Splunk.

Installation Overview

In order to use Splunk and Intermapper together, you need to do the following:

1. Prepare Intermapper. This includes enabling the Web server, adding a syslog notifier for Splunk, and setting the syslog message for compatibility with Splunk.
2. Set up Intermapper to send syslog notifications to Splunk.
3. Install the Intermapper App for Splunk.

Preparing Intermapper for Use with Splunk

Before you can use Splunk with Intermapper, you have to set up Intermapper to allow Splunk to access it. The steps are as follows:

Step 1: Enabling the Web Server

Before you can use Splunk, you need to enable the Intermapper web server.

To enable the web server:

1. From the Edit menu, choose **Server Settings**. The Server Settings window appears.
2. In the left pane of the Server Settings window, click **Web Server**. The Web Server configuration panel appears.
3. In the Web Server configuration panel, click **Start**.

NOTE: You can run the web server on a different port, but will need to enter that port in the Splunk application when you set it up.

4. Add an access control list entry to allow web server access by the Splunk host machine. Access is based on IP address.

5. Add one or more access control list entries to allow web server access by any users of the Splunk application. Access is based on IP address or address range.

Step 2: Adding a Splunk User

You need to add a user account to Intermapper that Splunk can use to log in to the Intermapper server.

To add a user:

1. In the left pane of the Server Settings window, click **Users**. The Users panel appears.
2. Click the **+** button and choose **Add User**. The User Information dialog appears.
3. In the **Name** box, enter a user name for the Splunk Server.
4. In the **Automatic Login** text box, enter the IP address of the Splunk server.
5. Click **OK**. The Splunk Server user appears in the user list.
6. Drag the Splunk Server user to the Administrators group. The Splunk Server user requires elevated privileges to export details about Intermapper maps.

Step 3: Add a syslog notifier for Splunk

Splunk acts as a syslog server. You need to create a syslog notifier that Intermapper can use to send syslog entries to Splunk.

To create a syslog notifier:

1. From the Server Settings window, click **Notifier List**. The list of existing notifiers appears.
2. Click the **+** button. The Configure Notifier window appears.
3. Give the notifier a name, such as SplunkLog.
4. From the Notifier Type dropdown menu, choose **Syslog**.
5. Enter the Splunk server's IP address in the **Send syslog message to** box.
6. Click Edit Message, then edit the syslog message as follows:

```
timestamp="<Timestamp>" map_name="<Document Name>" notification_
level="<Event>" device_host="<Device Name>" device_ip="<Device
Address>" probe_type="<Probe Type>" probe_message="<Device
Condition>" device_imid="<Device-IMID>"
```

NOTE: The message above must be on one line.

This format allows Splunk to extract syslog data and make it available in Splunk.

Step 4: Attaching the Notifier to All Devices

Once you have created the Splunk notifier, you need to attach it to all devices in Intermapper.

To attach a notifier to all devices:

1. From Intermapper's Window menu, choose **Device List**. The Device List window appears, showing a list of devices.
2. Click **Notifier View** near the left end of the window's toolbar. A set of checkboxes appears for each device.
3. From the dropdown menu just to the right of the View selection buttons, choose the Splunk syslog notifier you just created.
4. For each state you want to record in Splunk, hold **Alt** and click a check box in the column for that state. All check boxes are selected.
5. Recommended settings for Delay, Repeat time, and Count:

Delay = none

Repeat time = 5 minutes

Count = infinite

Hold **Alt**, click the dropdown menu for each column, then release the **Alt** key and choose the value from the dropdown menu. It is set for each device in the list.

NOTE:

- Set your Splunk notifier to be attached to new devices by default from the Default Notifiers panel of the Map Settings window.
- To send data to Splunk for only a single map, you can view devices in the map's Notifier View and attach only the devices in that map to the Splunk notifier.

Step 5: Sending Layer 2 Information

To send Layer 2 information to Splunk you must do the following:

- Set up Intermapper to collect Layer 2 information. See the Intermapper User Guide for more information.
- Add a device to any Intermapper map, and apply the Splunk > Layer 2 Output probe to it. Otherwise, use the information below to locate and upload the probe.

NOTE: *One and only one* device using this probe should exist on an Intermapper server. Running multiple instances of this probe uses Intermapper server resources unnecessarily, with no benefit to the Intermapper App for Splunk.

The probe is located in the Splunk install directory (%SPUNK_HOME%) at:

```
%SPLUNK_HOME%\etc\apps\Intermapper\default
```

Probe file name: `com.dartware.layer2`

The probe sends switch port data in CSV format to Splunk; the data is then interpreted and indexed in Splunk.

Step 6: Getting Notifications Into Splunk

Assuming a clear network route between Intermapper and Splunk, and that you are running Splunk as `root`, indexing of syslog data by Splunk begins nearly immediately.

To verify that Splunk is receiving Intermapper data:

- Do a search in Splunk on `sourcetype=Intermapper`.

Step 7: Installing the Intermapper App for Splunk

The Intermapper App for Splunk automatically configures Splunk to receive and interpret syslog data from Intermapper.

In order for Splunk to present collected data in an Intermapper-specific way, you need to install the Intermapper App for Splunk.

To install the Intermapper App for Splunk:

1. From Splunk's **Apps** menu (in the Web interface), choose **Find More Apps**. The Browse More Apps page appears.
2. Enter "Intermapper" in the search box, and click the Search button or press **Enter**. The Intermapper App for Splunk appears.
3. Click the **Read More** link. The description page for the Intermapper App for Splunk appears.
4. Click **Download**, log into your Splunk account, and save the file in a location accessible to your browser.

5. From the Web interface or your Splunk installation, select **Manage Apps** from the Apps menu. The Apps Manager page appears, showing all currently installed Splunk Apps.
6. Click **Install App from File**. The Upload an App page appears.
7. From the **File** area, click **Browse**, and navigate to the App file you downloaded.
8. If you have installed a previous version, click to select **Upgrade App**.
9. Click **Upload**. The app is installed. You will be asked to restart your Splunk server.
10. Click **OK** to restart your Splunk server.
11. From the Apps menu, choose **Intermapper**. A configuration notice appears.
12. Follow the links to the Configuration page.
13. Enter the IP address and port of the Intermapper web server in the format of [address]:[port] and the name of a default map, and click **Save**.
14. After a few moments, the Intermapper page appears with the default map.

Intermapper FAQs

How can I stop the Intermapper server from polling for a while?

The easiest way to stop Intermapper's polling for a while is to disable all the maps.

1. Open **Server Settings**.
2. Click the **Enabled Maps** tab.
3. Clear all maps. They are no longer polled or tested.

Alternatively, you can disable maps individually from the Map List by right-clicking on a map in the list and selecting the 'Disable' command.

How can I stop the Intermapper server? How can I restart it?

On macOS, Intermapper installs a Menu Bar Application that gives a summary of Intermapper's status, and allows you to start and stop the Intermapper daemon.

On Microsoft Windows, Intermapper installs an icon in System Tray (lower right corner) that does much the same thing.

On all Linux installations, Intermapper services should be controlled using the systemd command line interface command of systemctl. For more information, see the "Managing Intermapper Services for Linux Systems" section in the *Intermapper Developer Guide*.

We recommend you read the Readme file on the [Downloads page](#) for information specific to your version.

How can I move Intermapper from one server to another?

The recommended way to move Intermapper to another server is to follow these steps:

1. Install Intermapper on the new server, and stop the Intermapper service/daemon when installation is complete.

2. Stop the Intermapper service/daemon on the old server and copy your Intermapper Settings folder to the new platform, replacing the one created when you installed Intermapper on the new server.
3. On the new server, start the Intermapper service/daemon.

The default location for the Intermapper Settings folder depends upon the platform where installed:

- Windows: C:\Program Files\Intermapper\InterMapper Settings
- macOS: /Library/Application Support/InterMapper Settings
- Linux: \$HOME/Intermapper_Settings/, where \$HOME is the home directory for the specified user Intermapper is running under.

Note: If you are migrating from Mac OS X PowerPC to Mac Intel, Microsoft Windows or any other Intel-based system, please contact support@Intermapper.com prior to installing on the new platform. Additional steps are necessary in order to preserve the historical chart data when migrating between these platforms.

How can I uninstall the Intermapper server?

Each version of Intermapper comes with its own uninstaller. Find the original distribution file (or retrieve the current version from <http://www.Intermapper.com/files>) and use its uninstall feature.

Why do I have trouble with Telnet using my Windows terminal program?

Q: When I use HyperTerminal to telnet into Intermapper's server, I don't see character echoes. Why not?

A: Two commonly-available Windows telnet clients, HyperTerminal and the command-line telnet client, do not work correctly with Intermapper in their default configuration. Neither of them do local echoing by default, and both refuse to turn it on when asked to do so by the Intermapper server.

Therefore, neither of these clients work out-of-the-box with Intermapper, so you need to turn on local echoing yourself.

Enabling Local Echoing in HyperTerminal

With your Intermapper session loaded, choose File > Properties. Click the Settings tab. Click the ASCII Setup... button. Check the box labelled "Echo typed characters locally". When connecting to earlier versions of Intermapper, you should also check the box labelled "Send line ends with line feeds". Later versions of Intermapper do not require this (although it won't hurt.) Click Ok to close the ASCII Setup dialog, then click Ok to put away the Properties dialog. Remember to save your session to make the new settings permanent.

Enabling On Local Echoing with Built-in Telnet Client

Start your telnet session with Intermapper. Press Ctrl+] to enable the client to process setup commands. Type "SET LOCAL_ECHO" and press Enter to turn on local echoing. Press Enter again to return to your session. I'm not aware of any way to save this setting for future sessions, so you'll need to do this each time.

Putty

A free Windows telnet client we have had good luck with is Putty. Putty is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Putty requires no configuration to work correctly with Intermapper. You may find this nicer to use than either of the built-in options that come with Windows.

On an Xserve, can I use the serial port for paging?

You can use the built-in serial port to drive an external modem that can in turn send page notifications. To do this, you must disable the getty process that's usually listening on that port.

On the Xserve, open this file:

```
/System/Library/StartupItems/SerialTerminalSupport
```

At about line 72 is:

```
ENABLE_SERIAL_TERMINAL=$TRUE
```

Change this to:

```
ENABLE_SERIAL_TERMINAL=$FALSE
```

Re-init the system, and there should be no getty and Intermapper will get to the modem just fine. (Thanks to Charlie Winchcombe for this tip.)

How can I know that the embedded Java is secure?

The Intermapper rich client UI applications (IM-Console and IMRA) are each implemented using Java desktop facilities. For all platform combinations except for IMRA on Linux, the relevant Intermapper product bundles a Java runtime to support the application. Fortra recognizes that, although the Java platform is intensively and expertly maintained, it presents a large attack surface to a potential attacker and is therefore reasonable that security-sensitive sites seek reassurance as to the implications for their Intermapper deployments of the discovery and disclosure of security defects in the Java platform.

It is Fortra's policy in maintaining Intermapper to ensure that the bundled Java runtime is updated to a version incorporating the latest security fixes. If you cannot wait for the next Intermapper release, you can remove execute permissions from the bundled JRE and run an Intermapper application with an alternative external JDK or JRE.

Read the following to take such a proactive approach to the security of your installations:

Microsoft Windows and Linux Systems

To invoke Intermapper on Microsoft Windows using a version of JDK other than the one included with Intermapper, invoke the `InterMapper.jar` file from the installation directory (by default `C:\Program Files\InterMapper`) specifying the desired Java virtual machine at the Microsoft Windows command line. For example,

```
C:\> "C:\Program Files\AdoptOpenJDK\jdk-11.0.5.10-hotspot\bin\java"  
-jar "C:\Program Files\InterMapper\InterMapper.jar"
```

Similarly, on Linux, run the following command:

```
$ /opt/java/bin/java -jar  
/usr/local/share/intermapper/intermapper.jar
```

macOS

To use an alternative version of Java on macOS systems, replace `app.runtime=$APPDIR/PlugIns/Java.runtime` (located in the `/Library/Applications/InterMapper.app/Contents/Java/InterMapper.cfg` file) with the path name of the directory where your externally-sourced JRE file resides (this should be a sub-directory of `/Library/Java/JavaVirtualMachines`).

NOTE:

Make sure you install a .pkg file that installs a JRE rather than a JDK.

Intermapper FAQs

How can I stop the Intermapper server from polling for a while?

The easiest way to stop Intermapper's polling for a while is to disable all the maps.

1. Open **Server Settings**.
2. Click the **Enabled Maps** tab.
3. Clear all maps. They are no longer polled or tested.

Alternatively, you can disable maps individually from the Map List by right-clicking on a map in the list and selecting the 'Disable' command.

How can I stop the Intermapper server? How can I restart it?

On macOS, Intermapper installs a Menu Bar Application that gives a summary of Intermapper's status, and allows you to start and stop the Intermapper daemon.

On Microsoft Windows, Intermapper installs an icon in System Tray (lower right corner) that does much the same thing.

On all Linux installations, Intermapper services should be controlled using the systemd command line interface command of systemctl. For more information, see the "Managing Intermapper Services for Linux Systems" section in the *Intermapper Developer Guide*.

We recommend you read the Readme file on the [Downloads page](#) for information specific to your version.

How can I move Intermapper from one server to another?

The recommended way to move Intermapper to another server is to follow these steps:

1. Install Intermapper on the new server, and stop the Intermapper service/daemon when installation is complete.

2. Stop the Intermapper service/daemon on the old server and copy your Intermapper Settings folder to the new platform, replacing the one created when you installed Intermapper on the new server.
3. On the new server, start the Intermapper service/daemon.

The default location for the Intermapper Settings folder depends upon the platform where installed:

- Windows: C:\Program Files\Intermapper\InterMapper Settings
- macOS: /Library/Application Support/InterMapper Settings
- Linux: \$HOME/Intermapper_Settings/, where \$HOME is the home directory for the specified user Intermapper is running under.

Note: If you are migrating from Mac OS X PowerPC to Mac Intel, Microsoft Windows or any other Intel-based system, please contact support@Intermapper.com prior to installing on the new platform. Additional steps are necessary in order to preserve the historical chart data when migrating between these platforms.

How can I uninstall the Intermapper server?

Each version of Intermapper comes with its own uninstaller. Find the original distribution file (or retrieve the current version from <http://www.Intermapper.com/files>) and use its uninstall feature.

Why do I have trouble with Telnet using my Windows terminal program?

Q: When I use HyperTerminal to telnet into Intermapper's server, I don't see character echoes. Why not?

A: Two commonly-available Windows telnet clients, HyperTerminal and the command-line telnet client, do not work correctly with Intermapper in their default configuration. Neither of them do local echoing by default, and both refuse to turn it on when asked to do so by the Intermapper server.

Therefore, neither of these clients work out-of-the-box with Intermapper, so you need to turn on local echoing yourself.

Enabling Local Echoing in HyperTerminal

With your Intermapper session loaded, choose File > Properties. Click the Settings tab. Click the ASCII Setup... button. Check the box labelled "Echo typed characters locally". When connecting to earlier versions of Intermapper, you should also check the box labelled "Send line ends with line feeds". Later versions of Intermapper do not require this (although it won't hurt.) Click Ok to close the ASCII Setup dialog, then click Ok to put away the Properties dialog. Remember to save your session to make the new settings permanent.

Enabling On Local Echoing with Built-in Telnet Client

Start your telnet session with Intermapper. Press Ctrl+] to enable the client to process setup commands. Type "SET LOCAL_ECHO" and press Enter to turn on local echoing. Press Enter again to return to your session. I'm not aware of any way to save this setting for future sessions, so you'll need to do this each time.

Putty

A free Windows telnet client we have had good luck with is Putty. Putty is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Putty requires no configuration to work correctly with Intermapper. You may find this nicer to use than either of the built-in options that come with Windows.

On an Xserve, can I use the serial port for paging?

You can use the built-in serial port to drive an external modem that can in turn send page notifications. To do this, you must disable the getty process that's usually listening on that port.

On the Xserve, open this file:

```
/System/Library/StartupItems/SerialTerminalSupport
```

At about line 72 is:

```
ENABLE_SERIAL_TERMINAL=$TRUE
```

Change this to:

```
ENABLE_SERIAL_TERMINAL=$FALSE
```

Re-init the system, and there should be no getty and Intermapper will get to the modem just fine. (Thanks to Charlie Winchcombe for this tip.)

How can I know that the embedded Java is secure?

The Intermapper rich client UI applications (IM-Console and IMRA) are each implemented using Java desktop facilities. For all platform combinations except for IMRA on Linux, the relevant Intermapper product bundles a Java runtime to support the application. Fortra recognizes that, although the Java platform is intensively and expertly maintained, it presents a large attack surface to a potential attacker and is therefore reasonable that security-sensitive sites seek reassurance as to the implications for their Intermapper deployments of the discovery and disclosure of security defects in the Java platform.

It is Fortra's policy in maintaining Intermapper to ensure that the bundled Java runtime is updated to a version incorporating the latest security fixes. If you cannot wait for the next Intermapper release, you can remove execute permissions from the bundled JRE and run an Intermapper application with an alternative external JDK or JRE.

Read the following to take such a proactive approach to the security of your installations:

Microsoft Windows and Linux Systems

To invoke Intermapper on Microsoft Windows using a version of JDK other than the one included with Intermapper, invoke the `InterMapper.jar` file from the installation directory (by default `C:\Program Files\InterMapper`) specifying the desired Java virtual machine at the Microsoft Windows command line. For example,

```
C:\> "C:\Program Files\AdoptOpenJDK\jdk-11.0.5.10-hotspot\bin\java"
-jar "C:\Program Files\InterMapper\InterMapper.jar"
```

Similarly, on Linux, run the following command:

```
$ /opt/java/bin/java -jar
/usr/local/share/intermapper/intermapper.jar
```

macOS

To use an alternative version of Java on macOS systems, replace `app.runtime=$APPDIR/PlugIns/Java.runtime` (located in the `/Library/Applications/InterMapper.app/Contents/Java/InterMapper.cfg` file) with the path name of the directory where your externally-sourced JRE file resides (this should be a sub-directory of `/Library/Java/JavaVirtualMachines`).

NOTE:

Make sure you install a .pkg file that installs a JRE rather than a JDK.

Intermapper Flows FAQs

When the Intermapper Flows server is restarting and reloading the sessions, the Flows Window displays the number of records loaded so far vs. the total number of sessions. Sometimes the first number is larger than the second. What's going on?

The NetSAW server estimates the number of flows it will load into its cache, based on the flowrate that's learned from the actual records in the DB. Since this estimate is never perfect, you'll sometimes notice that the actual number of records exceeds the estimated records. Other times it'll fall short and finish early.

Is there any additional information available for troubleshooting or debugging a problem with Intermapper Flows?

Intermapper can provide some debug information via the Telnet server. To do this, turn on the Telnet server in the Intermapper Settings. Then telnet to the Intermapper server and use the "flows" command to list the exporters that Intermapper knows about. Use the "ext" command to check that Intermapper has its own connection to the IMFlows server.

You can copy/paste the output of these two commands into a bug report (Help -> Report a Bug...).

In the directory in which Intermapper Flows is installed, (see the Readme file in the installation package for a file location) there is a log file named "ns2flows.log". The server logs significant information in this file. If you feel the file is getting too large, you can delete it safely.

Does Intermapper Flows work on LAN links? On WAN Links?

Yes, Intermapper Flows will work on any link where there's an "exporter" (the router/switch) to keep track of the traffic statistics. Many kinds of Cisco equipment can export flow records that summarizes the data flowing through that device.

How much bandwidth will NetFlow consume? How frequent is the traffic flow?

A quick answer is "not much". According to Cisco reference documents, NetFlow consumes 5 to 10 percent of your network bandwidth, depending on your configuration. In Help/Systems' experience, it is often much less. The switch/router summarizes the flow information, and typically will send an update about the flows it has seen every 60 or 120 seconds (this is configurable).

It is easy to set up your Cisco gear to send flow records, so you can see the effect on the traffic. You can find a brief document that describes the commands at:

http://dartware.com/support/tech_notes/imflows/netflowconfig.html

Does IM Flow act as collector at each location so that the central server can pull the data from each collector and correlate the same?

No. In our first release, all the flow records must be sent to one Intermapper Flows machine (the "collector"). You can have multiple exporters sending flow records to the single collector, though.

About IP Addresses

Note: Intermapper now supports 128-bit IPv6 addresses. Most of the information in this topic is still relevant and accurate. In addition, you can enter an IPv6 address anywhere in Intermapper that you can enter a 32-bit IPv4 address.

What is an IP address? How do I get one?

An IP address ("Internet Protocol address") is a number that represents a single unique computer on the Internet. IP addresses are similar to telephone numbers, in that each computer (or telephone) must have its own unique IP address (telephone number.) Like telephones, there's a directory system - called the Domain Name System, or "DNS" - that can convert a name such as "www.apple.com" into a corresponding numeric IP address.

32-bit IPv4 Addresses are written as a sequence of four numbers separated by ".", like this: 208.123.246.35. Each of the four numbers in the IP address can take the value between 0 and 255.

Intermapper now supports 128-bit IPv6 addresses.

Every computer on the Internet must have a unique IP address. ISPs purchase large blocks of consecutive IP addresses, and then allocate smaller ranges of these addresses to their customers. Thus, a particular company might be assigned all the 254 IP addresses in the range 208.123.246.1 to 208.123.246.254. (The addresses ".0" and ".255" are not usually assigned.) Companies then assign the IP address to individual computers within the organization.

How do computers send data through the Internet?

Computers send information through the Internet by dividing the data to send into small chunks ("packets") and transmitting them to the other device. All this happens without your doing anything - the web browser, e-mail program, etc. all take care of these low level details.

When your computer wants to send to another computer, it creates the packet, then places the other computer's address in the *destination address* of the packet, places its own address in the *source address* of the packet, and then sends the packet off, either directly to the destination computer, or to a nearby router that takes responsibility for routing the packet.

There's an analogy with the post office here. Packets are like envelopes, with destination addresses and return addresses. Routers are like post offices: they check the destination address and have the responsibility for delivering the packet to the final destination computer or to another router that's closer to the destination.

What is a subnet? Why do I care?

A *subnet* is a range of IP addresses. The special attribute of a subnet is that all the computers within the subnet (a "sub-network") can talk directly to each other, and don't need a router to communicate.

As mentioned above, your computer delivers a packet directly to the destination computer or sends it to the router for ultimate delivery.

But how does your computer know whether the packet's destination is within its subnet? The answer is that your computer uses the subnet mask to determine the members of the subnet.

The chart below associates the number of IP addresses in a subnet to the subnet mask. For example, the subnet mask "255.255.255.0" represents 254 consecutive IP addresses. If your computer's IP and the destination computer's IP addresses are in the same subnet address range, then they can send packets directly to each other. If they're not in the same range, then they must send their data through a router for delivery.

What does the "/24" mean? How does that relate to my subnet mask?

Intermapper uses a shorthand notation to represent an IP subnet's information. The number in the "/xx" shorthand stands for the number of bits (technically, bits set to one) in the subnet mask. The convention is always to start at the left end of the 32-bit (IPv4) subnet mask. The table below shows the correspondence between the "/xx" notation and the actual numeric representation.

	Subnet Mask	# of Addresses			Subnet Mask	# of Addresses
/1	128.0.0.0	2.1 billion	/17		255.255.128.0	32,766

/2	192.0.0.0	1 billion	/18	255.255.192.0	16,382
/3	224.0.0.0	536 million	/19	255.255.224.0	8,190
/4	240.0.0.0	268 million	/20	255.255.240.0	4,094
/5	248.0.0.0	134 million	/21	255.255.248.0	2,046
/6	252.0.0.0	67 million	/22	255.255.252.0	1,022
/7	254.0.0.0	34 million	/23	255.255.254.0	510
/8	255.0.0.0	17 million (Class A)	/24	255.255.255.0	254 (Class C)
/9	255.128.0.0	8.4 million	/25	255.255.255.128	126
/10	255.192.0.0	4.2 million	/26	255.255.255.192	62
/11	255.224.0.0	2.1 million	/27	255.255.255.224	30
/12	255.240.0.0	1 million	/28	255.255.255.240	14
/13	255.248.0.0	524 thousand	/29	255.255.255.248	6
/14	255.252.0.0	262 thousand	/30	255.255.255.252	2
/15	255.254.0.0	131 thousand	/31	255.255.255.254	RFC 3021
/16	255.255.0.0	65,534 (Class B)	/32	255.255.255.255	Loopback address

What is a "private IP address range"?

The Internet Assigned Numbers Authority (IANA) has reserved several blocks of IP addresses that an organization may assign for its own private internet. These blocks are defined in RFC 1918 (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>).

From the RFC:

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

We will refer to the first block as "24-bit block", the second as "20-bit block", and to the third as "16-bit" block. Note that (in pre-CIDR notation) the first block is nothing but a single class A network number, while the second block is a set of

16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.

Quick Intro to IPv6 Address Formatting

This table gives the major forms of IPv6 addresses. The most important/common are **Localhost** (::1), **Global Unicast** (usually starting with "200x"), and **Link-Local Unicast** (starting with "FE80").

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA (*)	1111 110	FC00::/7
Global Unicast (**)	001	2000::/3
IPv4-Mapped	00...0:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (***)	1111 1110 11	FECO::/10
IPv4-compatible (***)	00...0 (96 bits)	::IPv4/128

* Unique Local Address (ULA) is an IPv6 unicast address that is generated to be unique in a local context. It is highly likely to be unique globally.

** Global Unicast address are all currently being assigned with a 2000::/3 prefix. Other three-bit prefixes are reserved for future use.

*** Site-Local Unicast and IPv4-compatible prefixes are deprecated. Use ULA and IPv4-mapped addresses, respectively.

About DNS

What resolver does Intermapper OSX use for its DNS?

Intermapper uses two different DNS resolvers. When you add a device using the **Add Device...** command, Intermapper uses the system's resolver, configured in the OSX Network settings panel. When you use the "DNS Check" feature, Intermapper does its own DNS

operations, via UDP packets, to the domain name servers listed in the DNS Monitor Preferences panel. Intermapper's built-in domain name resolver assumes that the domain name is fully-qualified. The interval for verifying the domain name is determined by the TTL in each DNS response (with the minimum interval specified in the DNS Monitor preferences panel).

When you discover devices, Intermapper initially looks up the FQDN name from the IP address (address --> name), then it settles down to monitoring the domain name (name --> address). Intermapper's built-in DNS resolver doesn't handle partially-qualified or invalid domain names; they fail to resolve.

Intermapper sometimes won't show a device's DNS name...

From the Edit menu, you can choose the Set Info submenu, then choose **Set Address...** to change the DNS option for each affected device from **Resolve name to address** to **Resolve address to name**. With this setting Intermapper always resolves the address to a name, and you don't see errors with names that aren't fully-qualified domain names.

What is a FQDN?

This is an acronym for a "Fully-Qualified Domain Name." Within an organization, it's convenient to refer to a computer by the first part of its name, knowing that "everyone" will know that the remainder is the same as the other computers in the organization. Thus, you may speak of "sneezy" and "dopey", knowing that they're really two computers at "seven-dwarves.org".

To identify a computer uniquely, you need the FQDN, such as "sneezy.seven-dwarves.org." Most user software can add a "search domain" to a partially-qualified domain name, adding the missing part of the FQDN. Some DNS servers require the FQDN to work properly with Intermapper. It's always best to enter the full domain name.

Tip: Even though you enter a FQDN when specifying a computer, you can use the *Short, Smart Name* when [constructing a label for a device \(Pg. 387\)](#).

Tip: Technically, a FQDN requires a "." at the end. Just as the search domain is tacked onto the end of a partial domain name, most user software adds the trailing "."

SNMP Information

What is SNMP?

SNMP stands for the Simple Network Management Protocol. At its heart, SNMP is a set of rules that allows a computer to get statistics from another computer across the Internet.

Computers keep track of various statistics that measure what they're doing. For example, routers can keep track of the number of bytes, packets, and errors that were transmitted and received on each interface (port). Web servers might keep a tally of the number of hits they have received. Other kinds of equipment have configuration information that's available through SNMP.

Management Information Base (MIB)

Each of these pieces of information (packet statistics, page hits, configuration) is kept in a database described by a *Management Information Base* (a *MIB* in SNMP parlance.) There are a many different MIBs, describing many different aspects of a computer's operation.

MIB Variables and OIDs (Object Identifiers)

The various values that can be retrieved from a MIB are called *MIB variables*. These variables are defined in the MIB for a device. Each MIB variable is named by an *Object Identifier* (OID), which usually has a name in the form of numbers separated by periods ("."), like this:

1.3.6.1.xxxx.x.x.x.x...

For example, the MIB-II (pronounced, "MIB two") has a variable that indicates the number of interfaces (ports) in a router. It's called the "ifNumber", and its OID is 1.3.6.1.2.1.2.1.0

Intermapper can query a device for the MIB variables and display the results. When a device receives a SNMP Get-Request for this ifNumber OID, it responds with the count of interfaces.

Note: The trailing ".0" in the example above is technically part of the OID. Although you will often see OIDs written without it, Intermapper requires that it be present wherever you enter an OID.

Enterprise Numbers and OIDs

You may notice that most OIDs start with 1.3.1.6.1.x. If the 6th number is 4, the OID is generated by a private enterprise. The 7th number is the Enterprise number, assigned to the organization by the IANA as defined here:

<http://www.iana.org/assignments/enterprise-numbers>

The remaining numbers are generated by and under the control of the registered enterprise.

What is the 'Read-only Community String'?

The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. Most network vendors ship their equipment with a default password of "public". (This is the so-called "default public community string".) Many network administrators will change the community string to keep intruders from getting information about the network setup. This is a good idea. Even if it's only read-access, SNMP can divulge a lot of information about the network that could be used to compromise it.

If there's a "read-only community string", you might expect that there is a "Write community string". You'd be correct. There is also a SNMP Set-Request, which is a command to set certain SNMP MIB variables (e.g., certain OIDs) to a specified value. These writes are protected by the write community string (which should *never* be set to 'public!'). Many SNMP-speaking devices also have IP address filters that ignore requests (read and write) unless the source address is on an access list.

There's also a SNMP Trap, which is an unsolicited message from a device to an SNMP console (for example, Intermapper) that the device is in an interesting state. Traps might indicate power-up or link-up/down conditions temperatures exceeding certain thresholds, high traffic, etc. Traps provide an immediate notification for an event that might otherwise be discovered only during occasional polling.

Why can't I get SNMP information from a device?

Intermapper requires that SNMP be available and configured to display traffic information. The most common cause of not being able to see traffic is that you haven't entered the SNMP Read-only community string. (This is like a password that controls whether another computer can retrieve SNMP information.)

In order of simplest to most complex, here is a list of reasons that Intermapper might not get SNMP information from a device:

- **Wrong DNS name/IP address** - (not likely, but we have to mention it)
- **No connectivity** - Can you ping the device from Intermapper?
- **No SNMP agent on the device** - Many devices or computers have optional SNMP capabilities that must be installed separately.
- **Is the SNMP agent disabled?** - Many devices allow you to disable the SNMP capability totally, or from certain ports.
- **If the SNMP agent is based on net-snmp or UCD-snmp package** - be sure that the configuration file specifically lists Intermapper's IP address/subnet as an allowed client

- **In a custom probe, have you specified the OID properly?** - (See the [OID Format FAQ \(Pg. 734\)](#) for details.)
- **Wrong Community string** - (have you tried 'public' ?)
- **Access lists: does the equipment only allow SNMP access from certain addresses?**
- **Firewalls: does a firewall block the SNMP port between your macOS and the equipment?**
- **Bugs in the SNMP agent on the equipment** - Intermapper uses SNMP Get-Next-Requests in several places. We've seen certain equipment that fails when queried this way.

If you're sure that you've checked all these things and you still can't get SNMP information, please get back to us at support@Intermapper.com. We may have some tricks up our sleeves. (Or we may wind up learning something!)

How can Intermapper query a particular MIB variable?

There are two kinds of MIB variables: scalar values and table entries.

- **Scalars** have a single value, such as the interface number shown above. For example, the `ifNumber` MIB variable of a router is a single number that represents the total number of its interfaces (ports).
- **Table values**, on the other hand, provide the same pieces of information for different items, such as the traffic for each of a router's ports, or information about each of the TCP connections in a device.

Intermapper can read and display both scalar variables and table variables in its custom SNMP probes.

Scalar values must have a ".0" suffix in their OIDs. For example, the OID for `ifNumber` in MIB-II is often written as "1.3.6.1.2.1.2.1". In custom probe files, it should be represented as "1.3.6.1.2.1.2.1.0". (This ".0" is technically part of the OID - it's convenient not to write it, though.)

Table variables are generally suffixed with the index of the row. (This isn't always true: see the note below). For example, the Cisco Environment Monitoring MIB defines two variables for the input air temperature and input voltage as the first rows in each of these tables:

```
ciscoEnvMonTemperatureStatusValue 1.3.6.1.4.1.9.9.13.1.3.1.3
ciscoEnvMonVoltageStatusValue 1.3.6.1.4.1.9.9.13.1.2.1.3
```

If you add a suffix ".1" to each of these, you'll get the value of the first row; add ".2" to as a suffix, you'll get the second row, etc.

Do all tables have an index?

As noted above, some tables don't have a separate index column. These rows are named (their OIDs are specified by) data in the row. For example, the OID for `tcpConnState` row, the status of a particular TCP connection is "1.3.6.1.2.1.6.13.1.1". Its index is the source and destination IP address and port (all four values) which are appended to the `tcpConnState` OID. Thus, the full OID for the state of a TCP connection from 9.8.7.6 port 543 to 123.45.67.89 port 8765 would be:

```
1.3.6.1.2.1.6.13.1.1.9.8.7.6.543.123.45.67.89.8765
```

Where can I read more information about SNMP?

A periodic newsletter, *The Simple Times*, is online at:

<http://www.simple-times.org/>

A great site pointing to various snmp products:

<http://www.simpleweb.org/>

How do I interpret an unknown enterprise number?

Q: My error log file shows the following lines:

```
14/02 15:13:07 TRAP CITRIX1:: coldStart14/02 15:13:07 TRAP
CITRIX1:: linkUp, ifIndex = 114/02 15:13:07 TRAP CITRIX1::
linkUp, ifIndex = 1677721914/02 15:14:07 TRAP CITRIX1::
1.3.6.1.4.1.3845.3.1.1 (8) { <no variables> }
```

Can you tell me what that SNMP ID is? (1.3.6.1.4.1.3845.3.1.1 (8))

A: The "1.3.6.1.4.1..." prefix of the OID indicates that the trap is from a private enterprise MIB. You can find out what enterprise by downloading the Enterprise Numbers RFC from:

<http://www.iana.org/assignments/enterprise-numbers>

Reading through the file indicates this:

```
3845 Citrix Systems Keith Turnbull
      keitht@citrix.com
```

You should contact the Citrix company (or read their MIB) to find out the exact interpretation of the trap's OID.

Is there a way to scan a network for all SNMP devices?

Intermapper will do a very good job of finding SNMP-speaking devices if you know the devices' SNMP Read-only Community string. Detailed instructions for scanning a subnet are available from the network scanning page. Be sure to set the default SNMP Read-only Community String as shown in the [SNMP Preferences. \(Pg. 228\)](#)

Intermapper may not be able to find a device for [any of these reasons. \(Pg. 734\)](#)

About WINS Names

Microsoft's Windows Internet Naming Service (WINS) is a name resolution service that resolves computer names to Internet Protocol (IP) address. Using WINS, the computer name can be resolved to a specific IP address.

Intermapper uses WINS names as follows:

- Intermapper (all platforms) queries devices for a NetBIOS (WINS) name. This name is used as the device's smart name if the DNS name is unknown or contains the word "DHCP".
- When adding a device that is in the same LAN as Intermapper server, you can use the device's NetBIOS/WINS name. To cause a name to be treated as a WINS name, place "\\\" in front of the name when adding a device. The name is not looked up in the DNS.

Note: Intermapper does not use the WINS server - it only resolves local device names.

Cross-Platform Questions

How can I move from Traditional to the service/daemon version on Windows/Linux?

The recommended way to upgrade to Intermapper on another platform is to follow these steps:

1. Set up Intermapper on the other platform, configuring the preferences anew as well as your notification settings.
2. Copy your map files to the "InterMapper Settings/Maps (Disabled)" folder on the new platform. (If you wish, you can also use Intermapper RemoteAccess to "import" them onto the new server.)
3. On the new platform, open the Server Settings window and "enable" the maps that you want to run.
4. Go through your maps and re-attach notifications to devices; these connections were lost in the transfer.

It is also possible to copy your Intermapper Settings folder and maps directly from one platform to another. This will preserve the attached notifiers for devices in your maps, but the procedure is slightly more complicated:

If you are running Intermapper "traditional" on a pre-macOS system (for example, macOS 9.2 or earlier), you need to convert your preferences file ("InterMapper Prefs"). The easiest way to do this is to run Intermapper on macOS -- start up the program and quit it -- Intermapper fixes the file so it is cross-platform.

If you have any icon files in your "Custom Icons" folder, you need to convert these to "data-fork" based resource files. You can use the [Custom Icon Conversion Script \(Pg. 740\)](#) on a macOS system to convert the file format. If that is not convenient, send an email to support@Intermapper.com.

You must double-check your modem pager settings on the new platform; the location of the modem device stored in the preferences file will be completely different.

All of the other files should transfer without any problems.

How can I use custom icons from my macOS Classic installation?

There is a droplet that converts resource-based icons (used by the Classic/macOS 8-9 versions) to a "data-fork" version that works on macOS. You can retrieve the droplet from: http://www.Intermapper.com/binaries/Convert_Custom_Icon_File.sit

Drag your icon files onto this droplet program, and they will be converted to a form usable by the macOS version of Intermapper. Drag the resulting files to the */Library/Application Support/InterMapper Settings/Custom Icons* folder.

How can I stop the Intermapper server from polling for a while?

The easiest way to stop Intermapper's polling for a while is to disable all the maps. To do this:

1. Open the **Server Settings** window
2. Click the **Enabled Maps** tab.
3. Clear all of the maps. They are longer be polled or tested.

How can I stop the Intermapper server? How can I restart it?

The Intermapper server is controlled separately from the Intermapper console and the Intermapper remote (IMRA) client. This process depends on the platform.

On Microsoft Windows and macOS systems, use the Intermapper Control Center (IMCC) desktop UI client to start or stop the Intermapper server.

To start and stop the Intermapper server from the command line on macOS systems, run the following commands:

```
sudo /usr/local/share/intermapper/Start.sh
sudo /usr/local/share/intermapper/Stop.sh
```

On Linux systems, as the super user (root) run the following commands using the systemctl command line interface that is provided by the systemd Linux service manager:

```
sudo systemctl start intermapperd.service
sudo systemctl stop intermapperd.service
```

For more information, see the "Intermapper Service Management for Linux" section in the *Intermapper Developer Guide*.

How can I uninstall the Intermapper server?

Each server-based version of Intermapper comes with its own uninstaller. Find the original distribution file (or retrieve the current version) and use its uninstall feature.

Troubleshooting Intermapper

How do I change the community string?

You can open the **Show Info** window on a device as described in the [Monitor menu \(Pg. 365\)](#) reference topic.

To set the community string:

1. Select the devices for which you want to change the community string.
2. From the Monitor menu, choose **Set Community**. The Set Community window appears.
3. Enter a Community string and click **OK**.

Use this procedure to set the Read-Only community string for one or more devices at once.

How do I monitor a fixed IP address?

In the **Add Device...** dialog, enter an IP address in dotted-decimal notation .

IP addresses discovered using the IP discovery feature are fixed by default.

I still can't make my router talk...

If you still can't make the router work with Intermapper, try the following:

- From the Help Menu's Diagnostics submenu choose **Server Log**, or from the Window menu's Logs submenu, choose **Debug**. Look for any messages related to that device.
- Let us know. Send E-Mail to support@Intermapper.com with information about the type of device and the trouble you're having.

My switches are always orange and showing lots of errors (or discards). Why?

We frequently hear of devices that appear to have high levels of discards and/or errors. They are usually orange on the map, and the status window shows a message like this:

```
Reason: Discards = 738: [1] sc0
```

The most likely reason that Intermapper shows a high rate of discards from a device is that the device is actually reporting these errors. It's common that when Intermapper reports errors (from its SNMP queries), the manufacturers' own monitoring tools will report zero errors. (It's also normal that the affected devices are operating normally, without problems, in this state.)

Experiments and Workarounds:

1. Use the vendor's own network monitoring tool (by telnetting in, using a web browser, etc.) to see if errors are being reported through the native management interface. It's possible that there actually is a problem.
2. This may be a bug in the SNMP implementation of the device. You can check with your vendor to see if there's a firmware upgrade that addresses the problem.
3. To test Intermapper's accuracy, use another SNMP console to check out the particular MIB variables for the device. Intermapper monitors the `ifInDiscards` and `ifInErrors` MIB variables (and the corresponding `ifOutxxxx` variables) listed on the [Network and Server Probes \(Pg. 599\)](#) page to compute its error & discard figures.

You can monitor these same variables with your SNMP Console to see if the same errors are reported there.

4. Run a ping test through the device that's reporting the errors.
 - If packets are actually being discarded, you'll see a higher than normal packet rate of dropped packets.
 - If packets aren't being dropped, it's another clue that the values reported by SNMP are incorrect.
5. As a workaround, if you've satisfied yourself that the error reports are bogus, you can instruct Intermapper to ignore the discards and/or errors. To do this, Get Info on the affected device and check the "Ignore Interface Errors" or "Ignore Interface Discards" box as desired.

What does it mean when Intermapper says a "subnet mask is discontinuous"?

In usual network configurations, a device's subnet mask contains one bits in the left side of the number, and zero bits on the right. Intermapper can then use the convention that a subnet mask is described as the number of bits in the subnet mask, and uses the notation of "/24" to indicate a subnet mask of 24 one-bits, or "255.255.255.0". For more details, see the [IP Addressing FAQ. \(Pg. 731\)](#)

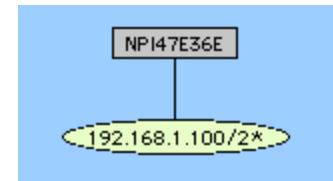
A subnet mask that has zero bits interspersed with the one bits in the left half of the value is often a configuration error. Intermapper points this out when you click and hold on a link: the status window resembles the figure at the right.



Normally, the address line contains the IP address and the subnet mask. This example shows a device whose IP address and subnet mask are set to the same value. This error is shown in the status window.

Why do network labels sometimes have a "/2*"?

This is another indication that there's a problem with the subnet mask. The figure at the right shows the network oval with a discontinuous subnet mask. The /2* indicates that the subnet mask has zero bits in the left half; clicking on the link will give a status window similar to the one above.



This example comes from an HP printer that has a bug in its SNMP implementation. The subnet mask of the printer is actually configured properly, and the printer is working. However, the SNMP software in the printer is reporting the incorrect value (it's reporting the IP address) for the subnet mask. Help/Systems has reported this to HP.

There are two separate network ovals on my map where I only expect one...

Examine the network's Status window to determine whether the subnet masks are the same in both ovals. If the subnet masks are different, one of the devices connected to the oval with the "wrong" subnet mask probably has a misconfigured subnet mask. (Look for the device that is being polled with SNMP.)

Note: For devices polled with ICMP echoes, Intermapper tries to guess whether it should draw a link to the network that contains the IP address. If both network ovals look equally good, it may draw a link to the "wrong" one, or alternate between them.

Some network ovals have more than one IP network number...

It's possible for a router or host to have two or more configured IP addresses for a particular interface. This form of secondary IP addressing can be common if your addressing is in transition. Rather than bringing everything to a halt to change IP addresses, a network administrator will support two IP subnets on the same logical wire. All the devices in the subnet can then have their IP addresses changed at their leisure, rather than forcing everyone to change them all at once. When all the addresses have changed, the administrator usually gets rid of the old network number.

It's also possible that Intermapper is only reporting what it knows, and the information it is using is incomplete. This may be true of multi-point network technologies (like frame-relay clouds). If you find a situation where Intermapper is reporting multiple networks on a logical network and you know it's wrong, please send us email (support@Intermapper.com) so we can figure out a way to make Intermapper's depictions more accurate.

We would also like to hear about a network with multiple IP network numbers where Intermapper does not show them correctly.

Does Intermapper support unnumbered IP links?

Yes.

To display unnumbered links:

1. From the Monitor menu, choose **Set Behavior...** The Set Behavior window appears.
2. Select the **Display unnumbered interfaces** check box.
3. Click **OK**. Unnumbered interfaces are now shown.

For more information, see the [Set Behavior \(Pg. 370\)](#) window reference section of the Monitor Menu reference topic.

What does it mean when a Status Window shows "[ifIndex not in ifTable]" ?

It is a normal situation for VLANs. Intermapper first traverses the ipAddrTable which maps IP addresses to ifIndex entries. If the ipAddrTable looks like:

```
ifIndex 1 --> 192.168.1.1/24
ifIndex 2 --> 192.168.2.1/24
ifIndex 3 --> 192.168.3.1/24
```

And the ifTable looks like:

```
ifIndex 1 --> Ethernet 10/100
ifIndex 3 --> Ethernet 10/100
```

Then the interface description for ifIndex 2 will be listed as "[[Not in ifTable]]".

How can I find out how many devices I'm monitoring with Intermapper. Do I have to count all the boxes on each map?

The Server Information pane of the Server Settings window shows the number of devices you are monitoring.

I discovered a multi-protocol router (TCP/IP & AppleTalk) using TCP/IP, but I could not go back and change the protocol to RTMP?

This problem is related to having only one "target" address for each device, even though Intermapper knows the addresses of the other ports. When a device is discovered using TCP/IP, it gets added with a target address in IP. You can't switch to use RTMP because that's an AppleTalk-only protocol.

Troubleshooting Intermapper Remote Access

Where do I find debugging information for Intermapper Remote Access

Linux Systems (including macOS)

Sending a SIGQUIT message to Intermapper Remote Access initiates a full thread dump. If you launch Intermapper Remote Access using the command line (for example, `java -jar <Intermapper RemoteAccess>`), `Ctrl-\` to stdin also works.

To send a SIGQUIT message, type the following in a terminal window (pid is the process id for Intermapper Remote Access):

```
kill -QUIT pid
```

The thread dump will be sent to stderr. On macOS, this is always the Console, unless you are running from the Terminal.

Microsoft Windows Systems

If you have launched Intermapper Remote Access from the command line (for example, `java -jar <Intermapper RemoteAccess>`) press `Ctrl-Break` in the command prompt to force the stack trace.

The stack trace always goes to stderr.

On Microsoft Windows, this is the equivalent of `/dev/null`, unless you are running from a command prompt or redirected stdout/stderr to a file using the Debug Window's Redirect System Output menu item.

Troubleshooting Intermapper DataCenter

I get an error message: "This Intermapper Server already appears to be associated with the Intermapper Database. Existing UUID is associated with a different URL"

Because multiple Intermapper installations can report to a single Intermapper Database, when Intermapper registers with Intermapper Database, it supplies a UUID to uniquely identify it. The Intermapper Database makes note of the URL and other characteristics of the server and associates them with the UUID. If Intermapper Database receives the same UUID from a different URL, it generates the error above. This may happen, for instance, if you copy your server settings from one copy of Intermapper to another, or move Intermapper to a new host or IP address. Your choices are to:

- **Cancel** - Stop the registration of the server
- **Force** - Force the UUID to be associated with the new URL.
- **Regenerate** - Have Intermapper generate a new UUID.

If you are certain that the installation of Intermapper which has generated this error is the same installation that was associated with the UUID previously, or if you know it should replace it, you can choose "Force".

If this is a different installation of Intermapper, choose "Regenerate".

Note: *It is important to pay attention to this error; map ids, device ids, etc., are only unique within a given server; if you associate a completely different installation of Intermapper with an existing UUID, the information about maps, etc. on the old server will be replaced or updated by information from the new server. When that occurs, datapoints from completely different datasets may be associated as if they were from one dataset.*

Index

1

16-bit 732

2

20-bit 732

24-bit 732

24 Hour Time 198, 244

3

32-bit subnet 731

6

64-bit 229

A

About DNS 733

About InterMapper 402

About IP Addresses 730

About Packet-Based Probes 589

About SNMP Versions 228, 590

About WINS Names 739

Access 154, 194, 214, 251-253, 259,
261, 267, 272, 277, 279, 633, 645,
650

Chart dropdown menu 194

Controlling 252, 279

InterMapper RemoteAccess 214

Remote Server 253

set 251

tcp 216

Telnet 252, 271, 276

Telnet Server 260

Web Server 258

Access Control 251

Access Control Examples 277

Access Control Process 252

ACK 175, 179, 212, 696

Acknowledgements 175, 365, 400

Acknowledge-message 212

Acknowledge Message Window 364

Acknowledgements window 365,
401

Acknowledging 175, 179

Device Problems 175

remove 178

Use 363

Action 39

Action dropdown menu 37

Active Hours 119

Add All 626

- Add Benchmark Coordinates window 635
- Add Device 46, 49-50, 733, 742
- Add Devices window 49
- Add Network 103
- Add Subnet 52
- Adding 8, 49, 52, 54, 62, 70, 84, 102, 108, 124, 130, 137, 193, 227, 231, 253, 258, 260, 277, 282, 622, 626, 634
 - Background Image 70
 - Background Images To Your Map 84
 - dataset 193
 - Devices Manually 49
 - firewall 277
 - Networks 52
 - submap 55
 - Unmanaged Hubs 102
- Adding Datasets 193
 - Charts 192
- Addr 696
- ADDRESS 63
- Address Change 214
- Address Ranges 251
 - Entering 251
- Addresses 47, 54, 106, 122, 253, 259, 261, 632, 635, 645, 649, 677, 693, 730, 733
 - InterMapper 54
 - Remote Server firewall 254
 - SNMP-speaking 44
 - syslog 106
 - Telnet Server firewall 261
 - Web Server firewall 259
- Admin 708
- ADMIN 699
- Administrator 253, 271, 276, 279, 593
 - Administrator's username 594
 - Administrators Group 253
- Adminpw 708
- Advance Data Importing 634
- AES 231
- AIF 121
- Aiff 623
- Alarm 29, 71, 108, 112, 121, 141, 154, 156, 179, 410
 - OK 108
 - Warning 106
- Alert 120
- Align 385

- ALLOW 250, 252, 277
 - automatic-login 278
 - matches 251
- Alpha-numeric Pager 125, 130, 132
 - Configure Notifier window 132
- Alrm 212
- Alt-click 76
- Alt/Option-click 98
- Analogue Modem 124
- Anti-aliasing 38
- ants 22, 40, 157
- Apache Mod-SSL httpd.conf file 283
- App 61
- Appearance 69, 84
- AppleTalk
 - AppleTalk-only 746
 - AppleTalk Name Binding Protocol 390
 - AppleTalk subnets 391
- Apply 632, 643
 - Vertex 633
- AppName 213
- ARGS 63
- Arrange Commands 94
- Arrange submenu 97
- Arranging 79
 - Arranging Your Maps 98
- ASN.1 141, 151
- AT Subnet List 391
- ATE0V1 131
- ATM 602
 - ATM AAL5 603
- Attach 106, 112
 - Attach Notifier dialog 107
 - Attach To 104
 - Notifier 106, 112
- Attribute 731
- AU 121
- Auth 252, 267, 272, 672-673
- Authentication 677
- Authentication Server 267, 272
- AuthLevel 219
- Auto 31, 155
 - Auto-adjust 197, 244
- Auto-Discover 41, 43, 378
 - stop 44

Auto-discovery 44, 347, 349, 378

 initiate 347, 349, 378

Autodiscovered 99

Autodiscovery 42, 45, 230, 382

 Autodiscovery window 378

 During 46

Automatic-login 269, 274, 278

 Allow 277

 called 278

automatic-login user 278

Automatic Device Discovery dialog 43

Automatic Device Discovery
 window 45

Automatic Login 252, 269, 274, 277

 matches 252, 269, 274

Automatic Placement 647

Axes Tab 243

B

Back-up 237

 Back-up SMTP 237

Background 68, 84

 Background Image 70

 Background Images To Your
 Map 84

Backup Map window 67, 352

Backup Name 67

Backups 67, 621

Baseband 221, 602

Basic Acknowledge 178

Basic, Timed 176

BBDISPLAY 599

BEGIN IMPORTS 151

Behaviour 734

Benchmarks 635

 Setting 635

Big Brother Probes 598

Big Brother State 599

Big.dartware.com 708

Bits 126

Block 176, 730

 Check 176

 IP 730

 select 176

Both 636

Bottom 392

 Bottom Left 392

 Bottom Right 392

- Bound 197
- Bps 220, 686
- Brightness/Contrast 85
- BroadcastPkts MIB 602
- Browse 284, 594
- Built-in Shapes 386
 - Built-in Shapes icon 385
- Built In 39, 67
- Built On 226
- Bus 94, 98, 385, 694
- By/s 696
- Byte/Second 602, 686
- Bytes Per Second 68
- Bytes/second 602
- C**
- Can't obtain/lock QPixmap 212
- Capacity/bandwidth 602
- Census 638
- Certificate 283
- Certificate Authority 284
 - Certificate Signing Requests 250, 283
- CFileName 216
- Changes 86, 154, 365, 677, 733
- DNS 733
- Edit 363
- Labels 86
- Map Zoom 155
- Poll Interval 154
- username 677
- Characteristics 76
- Chart 692
 - Chart Data 622
 - Chart Defaults 243
 - Chart Log Files 201
 - Chart Menus 194-195
 - Chart Options 195, 246
 - Chart Options window 195
 - Chart Title 195
 - Chart window 195
 - Charts popup 192
 - Charts submenu 192, 194
- Chart Defaults 243
- Chart dropdown menu 194
- Chart dropdown menu icon 194
- Chart Menu 194

- Charts 191-192
 - Adding Datasets 193
 - Creating 191
 - Deleting 194
 - Editing 193
- Cisco 603
 - Cisco's Icon Library 80
 - Cisco Environment Monitoring MIB 734
 - CiscoEnvMonTemperatureStatusValue
 - ciscoEnvMonVoltageStatusValue 734
- Citrix 738
- CKaliOpenLogList 699
- CKaliOpenMapList 699
- CKaliOpenSoundSetList 699
- Class 47, 157
- Classic/macOS 8-9 739
- Client 403
 - Client Log 222
 - Client Log window 223, 405
 - Client window 223
- Cmd 136
 - Cmd-A 97
 - Cmd-L 104
 - Cmd/Ctrl-L 86
 - CmdName 219
- Cmd-line 706
- Color-selection window 246
- Color Picker 238
 - Color Picker window 69
- Colors 68, 200, 245, 385
 - Colors Tab 200, 245
- Com.dartware.http.redirect 678
- Com.dartware.radius 678
- Comma-delimited 353
- Comma-separated list 236, 644
 - Domain Name Server 236
 - WINS 235
- Command 135, 137, 347-348, 355, 359, 363, 378, 397, 402, 693
- Command-line 409
 - Command-line Notifiers 135
 - Command-Line Probes 592
- Command + Option 222
- Command Details 696
- Command key 350

- Command Line 63, 135, 137
 - Command Line Interface 643
 - Command Line Program 137
 - Configuring 136
- Command Line Interface 706
- Comment 363
- Common Internet Scheme Syntax 679
- Common Name 286
- Community
 - Community String Types 229
- Compress 219, 694
 - JPEG 219
 - PNG 219
- Compute
 - byte/second 602
- Configd 604
- Configuration 117
- Configure Notifier 117
 - Configure Notifier window 109, 117, 122, 125, 132, 135, 283
 - Configure Notifier Window Reference 118
- Configure Notifier window 109, 283
- Configuring 117, 120, 122, 124, 132, 136, 139, 250, 259
 - Command Line 135
 - e-mail 122
 - E-Mail Notifier 122
 - Firewall 250
 - firewalls 259
 - Notifier 117
 - Page Notifier 132
 - Pager Notifier 124
 - Sound Notifier 120
 - Syslog Notifier 139
- Confirm Password 594
- Connecting 99, 250, 260
 - Devices 99
 - InterMapper 251
 - Web Server 258
- Connecting Devices 99
 - Switch Ports 99
- Context Menus 406
- Contrasty 85
- Control 252, 279, 407
 - Access 252, 279
 - Map Access 279

- User Access 280
- Control key 350
- Copy 221, 282, 285, 350, 403
 - CSR 284
 - InterMapper 37, 213
 - InterMapper RemoteAccess 402
 - mapname 221
 - Retaining 621
- Count 113
- CPU 40
- CR's 289
 - LF's 289
- CR-LF 289
- CRAM-MD5 237
- Create 41, 43, 54, 83, 191, 213, 268, 273, 277, 284, 349, 403, 632, 645
 - An Import File 632
 - Certificate Signing Request 284
 - Charts 191
 - CSR 284
 - Custom Icon Files 83
 - Guest 277
 - New Map 41
 - New User 267, 272
 - Reverse Connection 403
 - Sub-maps 54
- Create Log File window 202
- Critical 71, 114, 121
- Cross-platform Questions 739
- CSR 250, 284
 - copy 285
 - create 284
 - CSR file 287
 - generate 285
 - send 284
- CSV 42, 629
- Ctrl-click 628, 635
- Current Wireless Probes 279
- Currently-defined 124
 - set 124
- Custom Icons 80, 82, 622
 - Custom Icon Files 83
 - Setting 80
- Custom Probe 159, 216
- Customize 62, 159, 679, 682
 - Status Window 159

Cycle 94, 98, 385

 Cycle Command 97

 illustrated 385

 result of 94

D

D<name 707

Daemon 9

 start 740

Dartware

 DARTWARE-MIB DEFINITIONS 154

 Dartware MIB 141, 151

 Dartware OBJECT IDENTIFIER 151

Data 42, 196, 243

 Importing 42

 Use 195, 243

Data File 350

Data From Maps 626

 Exporting 626

Data Into Maps 631

 Importing 631

Data Retention 364

Data Tab 198, 244

Dataset 193

 add 193

Date & Time 35

Days/weeks 233

Dbug 215

DDis 603

Debug 204, 223, 398, 404

 InterMapper 402

Debug file 231

Debug Log file 404

DEBUG_CONFIG_FILE 707

Debugging 223

Default 38, 51, 409, 648

 Default Appearance 80

 Default button 61

 Default Device 239

 Setting 240

 Default Device Thresholds 185

 Setting 181

 Default Map Colors 238

 edit 238

 Default Network 240

- Default Notifiers 73, 110
 - Default Notifiers dialog 107
 - Default Notifiers window 111
 - Defining 110
- Default Thresholds 181
 - Setting 181
- Default Traffic Thresholds
 - Setting 181
- Labels 387
- Default Notifiers window 111
- Defaults 706
 - 8181 706
- Define SNMPv1 Traps 154
- Defining 110
 - Default Notifiers 110
- Delay 113
- Delayed Notifiers 114
- Delete 9, 105, 200, 228
 - interface/oval 99, 105
- Delete Chart 195
- Delete Data window 200
- Deleting
 - Charts 194
- Demo 8, 22, 409
 - Demo Map file 22
 - open 22
 - find 409
 - Try out 22
- DENY 251-252, 278
 - matches 251-252
- Dependencies 178
- DErrs 603
- DES 229
- Describing 61
 - Launcher 62
- DESCRIPTION 154
- Detail 105
 - Hiding 105
- Detailed Logs 403
- DETAILS 695
- Determine 215
 - DNS 214
 - IP 213
- Developer Guide 142, 159, 405, 411, 592, 631, 682, 684
- Developing 409
 - Nagios 409

Device 55, 70, 79, 99, 175, 212, 239,
385, 633, 635, 643, 688

Automatic Placement 647

Connecting 99

Default Appearance 80

Importing 635

Unacknowledging 178

Device-Name 697

Device Address 123

Device Attributes 633, 649

Device Condition 123

Device Defaults 239

Device Descriptions 81

Importing 81

Device Kind 364

Device List 398, 681, 683, 691

Manipulating 35

Use 398, 691

Device List Columns 34

Device List Web Page 691

Device List window 398

Open 397

Device Name 123, 686

Device Notifiers window 112

Device Problems 175

Acknowledging 175

Device States 121

Device Status 83, 686

Coloring According 83

Device Status window 159, 374, 599

Device Threshold window 377

Device Thresholds window 181

Device Variables 390

Device. Add Device 378

Device/link 238

Device?Intermapper 734

Devicename 217

Devices - Adding Manually 49

Devices/probe 631

DHCP 739

DHCP-Discover 604

DHCP-Inform 604

DHCP Message Type 604

DHCP/Bootp 604

Diagnostics menu 223-224

Dialup 130

- Directive 633, 643
 - Directive Line 633
 - Directive Line Technique
 - Importing 633
 - Directive Parameter 643
- Directive Line 643
- Disable 264, 736
 - SNMP 734
- Disc/Minute 687
- Disconnected 217
- Discontiguous subnet 741
- Discovery Options 46
- Discovery Status bar 43
- Display 102, 745
 - interconnections 102
 - Select 742
- Distribute Command 385
- Dividers, Sub-Dividers 197, 244
- DNS 42, 44, 50, 86, 140, 154, 214, 233, 235, 286, 374, 382, 390, 400, 589, 594, 637, 677, 730, 733, 739
 - change 734
 - determine 215
 - DNS-Related Messages 214
 - DNS Check 733
 - DNS Monitor Preferences 236, 733
 - Setting 235
 - DNS Monitor prefs 733
 - DNS Name 390, 648, 686
 - DNS x.x.x.x 215
 - DNS z.z.z.z 214
 - DNS/WINS Settings 235
 - Use 235
 - DNSName 634, 645, 650
 - enter 49, 363
 - monitoring 733
 - processing 215
 - see 594
 - specify 235
 - DNUcast 603
 - DocName 213
 - Document Name 123
 - Domain Name
 - Domain Name Server 236
 - Comma-separated list 236
 - Domain Name Service 235

Domain Name System 730
 called 730
Double-click Actions 65, 362
Down 71, 106, 112, 131, 141, 154, 179,
 212, 222, 364, 410, 589, 694
 generate 71
 set 363
DOWN-ACK 697
DOWN list 697
Down Thresholds 71
Downloading 738
 Enterprise Numbers RFC 734
Drag 98, 251
 firewall 250
Dropdown menu 27, 61, 375
Dt 216
DUcast 603
Duplicate 109, 283

E

E-mail 6, 22, 106, 112, 117, 122, 217,
 223, 236, 730
 Configuring 122
 enter 122, 236
 outgoing 237
 send 106, 112, 122, 236
 specify 106
 Use 122
E-mail Notification Message 122
E-Mail Notifier 122
 Configuring 122
E-Mail Preferences 236
 Setting 237
Echo 378
Edit 24, 49, 62, 86, 108, 123, 154, 160-
 161, 185, 192, 231, 238, 240, 250,
 267, 272, 282, 360, 363
 change 365
 Charts 192
 Default Map Colors 238
 Device 385
 Helper Applications 61
 Label 387
 Labels 86
 Notifier List 282
 Text 123
 User Information 268, 270, 273, 275
Edit Chart 195
Edit Default Notifiers 111

- Edit Device Label dialog 86
- Edit Device Label window 86
- Edit E-mail Message window
 - shows 122
- Edit Label 241
- Edit List 125, 130
- Edit Map 76, 360
- Edit menu 22, 68, 79, 84, 86, 97, 111, 118, 130, 185, 225, 228, 231, 240, 243, 254, 259, 261, 282, 285, 347-348, 355, 734
 - From 734
 - Use 347-348
- Edit Message 119, 125, 132, 137, 139
- Edit Network Label dialog 86
- Edit Network Label window 86
- Edit Notifiers 74, 112
- Edit window 63
- Editing Helper Apps 62
- Editing Your Map 76
- Electronic 122
- Email 107
- EmailAddr 219
- Enabled Maps 264, 350, 741
- Enabling 346
 - Remote 345
- Encoding 679
 - Special Characters 679
- Encrypted 284
- End 154, 695
 - 32-bit subnet 731
- EndTagStr 216
- telnet 693
- Enhancing 80
 - Your Map's Appearance 80
- Enter 39, 49, 52, 56, 66, 71, 103, 122, 132, 175, 196, 235-236, 244, 251, 254, 259, 261, 268, 273, 278, 352, 363, 380, 385, 404, 591, 734, 742
- Address Ranges 251
- DNS 50, 374
- e-mail 122, 236
- Host 237
- ID 132
- IP 132, 268, 273, 278, 378, 402
- IP subnet 52
- list 235
- Map Name 56
- Multiple Licenses 9, 227

Name 350

OID 735

SNMP Community 380

SNMP Read-only 591, 736

subnet 103

TCP 254, 259, 261

URL 39, 66, 260

User 237

User Name 56

WINS Scope 236

Enter dialup 126

Enterprise 6306 151

Enterprise Numbers RFC 734

 downloading 738

Env 707

ERR 214

Err/Minute 687

Error 181, 214, 688, 693

 Setting 181

Error Page 688

Error/min 686

ERRORS 694

Errors-per-minute 181

Errors-To 237

ErrorThe ERROR 693

ESCAPED_MESSAGE 136

Ethernet 80, 96, 396, 602

 represent 96

Ethernet 10/100 745

Event 123, 231

Event Log 211, 694

Event Log file 175, 212, 233, 648

Event Log Messages 212

Event Log window 211, 213

 open 211

EventLog file 179

EventMesg 218

Example Notification 137

Excel 632

Exe 135

Execute 356, 595

 NT Services 592

 Undo 355

Exit/Quit 351

Expand

 frontmost window 397

- Preference 243
- Server Settings 264, 282
- Expand/contract
 - frontmost window 397
- Experiments 742
- Export 707
- EXPORT-SPEC 707
- Export Map 349
- Export submenu 628
- Exporting 195, 264, 354, 626, 643
 - Data From Maps 626
 - Schema 643
- Exterior - Click 195

F

- FDDI 80
- Field Export Order 626
- Fields 628
- File Format 234
- File Menu 31, 41, 43, 67, 347-349
- File Save dialog 627
- FILE_NAME 707
- Filter 382, 404
- Find Next 356

- Find window 356
- Finding 407, 409, 739, 741
 - Demo 409
 - Legacy 409
 - Menu Item Shortcuts 407
 - SNMP-speaking 736
- Firewall 249-250, 252, 277, 403, 737
 - Add 277
 - Configuring 250
 - drag 251
 - move 251
- Firewall's list 250, 252, 255, 260-261
 - IP 250, 253, 260-261
- Firewall Definition dialog 278
- Firewalls 230, 252, 255, 259, 737
 - configuring 259
 - InterMapper's 252
- FoldersInterMapper saves its files 618
- Font, Size 397
- Format 81, 94, 385
- Format menu 76, 80, 86, 98, 104, 348-349, 385
- Format/Options 643

- FQDN
 - enter 734
 - require 734
- Frontmost window 397
- FTP 66, 160
- FULL 688, 694
- Full Pages 688
 - Use 688
- FullDuplex 221
- FullLogAccess 253, 271, 276, 278
- Fullname 212
- FullTelnetAccess 253, 271, 276
- FullTelnetAccess Group 253
- FullWebAccess 253, 271, 276-277
- FullWebAccess Group 253
- Fully-qualified 236, 733
- Fully-Qualified Domain Name 734
- FullyQualifiedDomainName.csr 285
- Function 10
 - MacOS 9
- G**
- General Messages 213
- General Rules 407
- Generate 71, 285
 - 1,024-bit 285
 - CSR 284
 - Down 71
 - Warning 71
- Geocoding 638
- Geographic Coordinates 81, 634
 - Setting 80
- Geographic Information Systems 638
- Get 678
- Get-Next-Requests 737
- Get Info 385, 743
- GIF 80, 83, 86, 635
- GraphicConverter 85
- Graphics 38
- Graphing 603
 - Percent Err 603
- Grayscale 82
- Grep bootpc 604
- Group 123, 266, 272
- Group Information dialog 266, 272
- Group notifiers together so 123

Guest 277

 create 277

H

Handle 61

 URL 61

HCOctets 602

Help 223-224, 693

Help Menu 348-349, 401

 Use 347-348, 401

Helper App 39, 65

Helper Applications 61

 Editing 62

 Removing 63

Helper Applications Customize
 window 62

 Use 61

 view 62

Helper Applications submenu 62

Helper apps 364

Helper Apps submenu 62

Helper Apps window 63

HelpNo 693

Hide 159

 Status window 159

Hide Charts 194

Hide Selection

 Use 105

Hiding 99, 105

 Detail 105

 Inactive Ports 99

Hiding Charts 192

Highlight 200

Highlight popup

 Use 243

Horizontal Dividers 197

Host 9, 237, 592

 Enter 236

 InterMapper 592

 InterMapper Server 9

HOST 706

HTML 629

I

IANA 732

ICMP 42, 744

ICMP Echo 380

ICMP Ping 383

Icon Sets 82

Icon Size 83

Icon window 81, 386

Icons 386

Icons on Maps 81

Id 125, 132, 215, 643, 677, 693

ID,MapName,Address,Latitude,Longitude 644

Id,name,address 643

Id/phone 131

IfAdminStatus 168-169, 600-601

IfAlias 167, 601

IfAlias The ifAlias 167

IfConnectorPresent 601

IfCurrStats.inDiscards 603

IfCurrStats.inErrors 603

IfCurrStats.inNUcastPkts 603

IfCurrStats.inUcastPkts 603

IfDescr 220, 601, 699

IfHCInOctets 601

IfHCOctets 602

IfHighSpeed 601

IfInBroadcastPkts 602

IfIndex 100, 168-169, 220, 686, 699, 738, 745

IfInDiscards 600-601, 603, 743

IfInErrors 600-601, 603

IfInErrors MIB 741

IfInMulticastPkts 602

IfInNUcastPkts 600, 602

IfInOctets 221, 600, 602

IfInUcastPkts 600-602

IfLastChange 601

IfMTU 601

IfName 601

IfNumber MIB 734

IfNumber OID 735

IfOperStatus 168-169, 600-601

IfOutBroadcastPkts 602

IfOutDiscards 600-601, 603

IfOutErrors 600-601, 603

IfOutMulticastPkts 602

IfOutNUcastPkts 600, 602

IfOutOctets 221, 600, 602

IfOutUcastPkts 600-602

IfOutxxxx 743

IfPhysAddress 601

IfPrevStats.inDiscards 603

- IfPrevStats.inErrors 603
- IfPrevStats.inNUcastPkts 603
- IfPrevStats.inUcastPkts 603
- IfPromiscuousMode 601
- IfSpeed 168, 221, 601-602
- IfType 601
- Ignore Interface Discards 603, 741
- Ignore Interface Errors 743
- IgnoreInterface Errors 603
- IM 349, 677
- IM-Remote.jar 708
- Im&password 678
- Image 635
- Import 42, 264, 349, 386, 631-632, 635, 677, 707
 - Data 42
 - Data Into Maps 631
 - Device Descriptions 81
 - Devices 635
 - SNMP MIB file 350
 - URL 677
- Import button 81
- Import file 643
- Import File Example 646
- Import Sound 120
- Import submenu 353
- IMProbe 645, 677
 - include 677
- IMProbe URL 648, 677
 - contains 677
 - use 677
- IMProbe URL Specification 677
- Inactive Hours 119
- Inactive Ports 99
 - Hiding 99
- Includes 8, 41, 61, 227, 677
 - IMProbe 677
 - MapName 677
 - SNMP 42
 - URL 61
- Indefinite Acknowledgements 176
- Info - View 349
- Info window 39, 161, 363, 599
 - Use 161
- Information 82, 688
 - Viewing 685, 690
- Information window 364

- Init 131
- InOctetPrev 220
- Insert 643
- Insert menu 49, 52-53, 56, 80, 103, 347, 349, 378
- InstantSSL 287
- Interconnections 25, 44, 98, 102, 395
 - display 102
 - see 98, 386
- Interface 603
- Interface Attributes 662
- Interface Information 686
- Interface Statistics 686
- Interface/oval 99, 105
 - delete 105
- Interfaces window 167, 179, 363
 - Opens 363
 - view 167
- Intermapper's Remote Server 253, 746
- Intermapper Control Center 9, 37
- Intermapper Control Center
 - application 10
- Intermapper Control Center icon 12
- Intermapper daemon 9
 - stop 9
- Intermapper Errors 689
- Intermapper Event Log file 648
- Intermapper Files 618
- Intermapper Handles Errors 648
- Intermapper Help 402
- Intermapper icon 115
- Intermapper Inserts Devices 648
- Intermapper Labels 43
- Intermapper Logs 231, 622
- Intermapper Map 353
- Intermapper menu 39
- Intermapper OBJECT IDENTIFIER 151
- Intermapper on Mac OS 740
- Intermapper Outages 691
- Intermapper Preferences 225
- Intermapper Prefs 740
- Intermapper Prefs file 622
- Intermapper Probe 648
- Intermapper Remote 283, 706

- Intermapper RemoteAccess 31, 121, 212, 214, 234, 250, 252-253, 345, 356, 362, 402, 627, 632, 698, 746
 - access 214
 - copy 403
 - stopping 214
 - Troubleshooting 746
- Intermapper RemoteAccess application 253
- Intermapper RemoteAccess Help 402
- Intermapper Server 6, 9, 31, 226, 249, 709
 - hosting 9
 - running 249
 - testing 706
- Intermapper Server Preferences Overview 228
- Intermapper Server Status window 10
- Intermapper Servers window 632
- Intermapper service/daemon 739
- Intermapper Settings 82, 137, 212, 234, 287, 619, 621-622, 740
 - create 213
 - Tools subdirectory 135
- InterMapper Settings
 - state 621
- Intermapper Settings Folder 622
- Intermapper Settings/Intermapper Logs 211
- Intermapper Settings/Maps 67, 266, 740
- Intermapper Settings/Sounds 121
- Intermapper Status 599
- Intermapper Telnet 250, 679, 682
- Intermapper Telnet-based Interface 6
- Intermapper Tray window 12
- Intermapper User List 623
- Intermapper User Preferences 37
- Intermapper Version 226
- Intermapper Web Page 680, 682
- Intermapper Web Page Navigation 680, 683
- Intermapper Web Server 260
- Intermapper Web Server menu 680, 683
- Intermapperauthd 619
- IntermapperCondition 142, 154
- Intermapperd 619
- IntermapperDeviceName 142, 154
- IntermapperMessage 142, 154
- IntermapperTimestamp 142, 154

- IntermapperTrap 154
- Internet 106, 133, 735
- Internet Assigned Numbers Authority 732
- Internet Protocol 730, 739
- Interval 681, 683
 - Setting 681, 683
- Invalid Probe Human Name 216
- Invalid Probe ID 216
- Invalid Probe Name 216
- IP 41, 44, 50, 52-53, 86, 102, 132, 140, 157, 160, 175, 213, 233, 235, 250, 252-253, 260-261, 268, 273, 278, 284, 346, 363, 378, 385, 402, 594, 598, 631, 635, 643, 677, 686, 699, 730, 734-735, 739
 - assign 730
 - blocks 730
 - contains 743
 - corresponding 235
 - determine 215
 - Enter 132, 268, 273, 278, 380, 404
 - firewall's list 250, 255, 260-261
 - ICMP Echo 380
 - reporting 742
 - scan 53
 - set 599
 - Set 363
 - switching 631
 - use 592
- IP Address 278, 390, 730
- IP Net 686
- IP subnet 52, 382, 731
- IP Subnet List 391
- IP subnets 391, 744
- IpAddrTable 745
- ISPs 730
- Item
 - Alt/Option-click 98
- ItsMailServer 218
- ItsUserName 218
- J**
- Java Version 402
- Joint Photographic Experts Group 83
- JPEG 80, 83, 219, 635
- JPG 86
- JSON 629
- K**
- Kali 214, 694

- KALI NEXT 698
- Kali Starting KALI 214
- Kali Stopping KALI 214
- KalidDisplays 693
- Keyboard Shortcuts 406
- KeySpan Twin Serial 128
- KILL 694
- Klaxon 121
- L**
- Label 43, 81, 86, 102, 196, 385, 387
 - Changing 86
 - Editing 86
 - Select 86
- Label Font 241
- Label Position 385
- Label Position submenu 385
- Label Size 241
- Label Variables 389
- LAN 739
- Last Down 123
- Latitude 635, 644
- Launcher 62
- Launching Intermapper 8
- LDAP 410
- LDOWN 694
- LF's 289
- CR's 289
- Library/Application Support/InterMapper Settings/Custom Icons 739
- License List 226
- Line 633, 637, 693
 - Directive 633
 - DOWN list 697
- Line Style 243
- Linear 197
- LineStr 216
- Link 52, 102, 378, 688, 690
- Link-up/down 736
- LINK REPORT 696
- Link Status 686
- Link Status Window 160
- LinkUp 738
- Linux 61, 224, 407, 619-621
- Listen 231
 - SNMP 228
 - SNMP Traps 230

- Lists 359, 694
 - kalidDisplays 693
 - Local Security Policy 594
 - Localhost 253
 - Locality 286
 - LocalSystem 594
 - Locations 618
 - LOG 694
 - Log Entries 233
 - Redirecting 233
 - Log File 127, 131, 195, 201, 204, 231
 - Paging 125, 130
 - Log File Name 202, 233
 - Log File Parameters 232
 - Setting 231
 - Log File Preferences 201
 - Log File Sources 234
 - Log In 351
 - Log Messages 212
 - Log On 593
 - Log Out 351
 - Log Windows 204
 - Logarithmic 197
 - Login 269, 274, 277
 - Logins 355
 - Logon 594
 - Logs 211, 231, 347-349, 398
 - Preferences 231
 - viewing 347, 349
 - Logs submenu 205, 211, 222, 231
 - Long-term Packet Loss 174
 - Longitude 364, 635, 644
 - Loopback 732
 - Lost Packets 410
 - Lower-left 388
 - Lower Bounds 197, 244
- M**
- Mac 161, 737
 - MAC Address 686
 - Mac OS 121, 604
 - Mac OSX 128
 - Macintosh 407, 592
 - macOS 619-621
 - MacOS 9, 61, 235
 - function 10
 - InterMapper 235

- Mailto MyProbe 219
- Main Logger 107
 - Syslog 106
- Management Information Base 735
- Managing 270, 275
 - Users 266, 272
- Manual Entry 42
- Manually-connected 53
 - remove 53
- Map 23, 37, 41, 52, 79, 102, 154-155, 181, 264, 277, 279, 349, 621, 626, 635, 643, 684
 - Switches 102
 - Understanding 155
- Map's Colors 69, 239
 - Setting 68
- Map's Default Device Thresholds 71
 - Setting 68
- Map's Default Notifiers 73
 - Specifying 73
- Map's Default Traffic Thresholds 72
 - Setting 68
- Map Access 253, 279
 - Controlling 279
- Map Access Panel 279
- Map Access Permission Levels 281
- Map Area 30
- Map Attributes 667
- Map Background 80
 - Setting 80
- Map Benchmark 379
- Map Data 632
- Map Edit 360, 366
- Map Editable 154
 - Making 154
- Map Editor 155, 347, 349, 378
- Map Files 265, 623
- Map Legend 29
- Map List 398, 681, 683
- Map List window 31, 54, 226, 240, 349, 356, 360, 398
 - Open 397
- Map Name 35, 56, 281
- Map Settings 68, 111, 185, 228, 356
- Map Settings Window 68, 111, 157, 185, 356
- Map Status 55, 687
 - Probe Type 55

- Map Status item 687
- Map Status Probe 55
- Map View button 44
- Map Web Page 684
- Map window 23, 44, 154, 355, 359, 363, 378
- Map Zoom 31, 155
- MAP_NAME 707
- MapName 221, 633, 637, 644, 677
- MapName,Address 644
- MapName,Address,Name,Latitude,Longitude 645
- MapName,Probe 645
- Maps
 - Deleted 623
 - Disabled 623
 - Enabled 623
- Maps, Free 634
- Matches 251-252, 269, 274, 592, 644
 - Allow 250
 - Automatic Login 252, 269, 274
 - DENY 251-252
 - username 593
- Mbps 161
- MD5 230
- Menu Bar 24
- Menu Bar Application 9
- Menu Command 385
- Menu Item Shortcuts 407
 - Finding 407
- Menu Reference Overview 347-348
- MESSAGE 136
- Message Editor window 123
 - Use 122
- Message Format 212
- MIB 142, 157, 350
 - SNMP-enabled 157
 - use 349
- MIB-II 168, 735
- MIB-II 32 602
- MIB file 350
- Microsoft's Windows Internet Naming Service 739
- Misc 224
- Miscellaneous Probes 411
- Misconfigured subnet 744
- Missing HTTP Version 220
- Modem Compatibility 128

Modem Page Settings dialog 128

Modem Pager Settings window 130

Monitor 23, 62, 154, 159, 360, 592, 733

- DNS 733
- Network 154
- NT Services 592

Monitor menu 50, 108, 112, 115, 161, 167, 175, 187, 347, 349, 362, 599, 741

Move 115, 251

- firewall 250
- Vantage Point 114

Msec 160

Msg 217

MTU 686

Multicast 686

MulticastPkts 602

Multiple Licenses 9, 227

MultiTech MT5634ZBA-USB 128

MyProbe 216

N

Nagios 409

- developing 409

Nagios Plugins 411

Nagios Template 592

Name 117, 126, 130, 132, 167, 212, 268, 273, 350, 739

- Enter 352
- Internet Protocol 739
- SNPP Server 132

Name, IP Address 637

Name,MapName,Address 634

NBP 42

NBP Name 390

Net-snmp 736

NET USE 594

NetBIOS 739

NetBIOS/WINS 739

Netmask

- InterMapper 226

Netopia.example.com 678

Network 52-53, 79, 86, 154, 239, 599, 688

- Adding 52
- Monitoring 154
- Open 604
- Scanning 53
- Troubleshooting 599

- Network-specific 596
- Network Defaults 239
- Network Defaults Preferences 239
- Network Filter Dialog 45
- Network Info Window 166
- Network Monitor 598
- Network Monitoring 6
- Network Preferences 239
- Network Scanning window 45, 53, 378
- Network Status 686
- Network Status Window 160
- Network Techs 107
- Network Variables 391
- Network. Add Network 378
- New 43
- New Group 267, 272
- New Map 41, 349
 - Creating 41
- New Map Constructor window 41, 43
- New Service 130
- New User 267, 272
 - Creating 268, 273
- Newdata.tab 708
- Newline 140
- NNTP 410
- NODE 694
- NODE REPORT 696
- Non-localhost 253
- Non-Polling Probe 411
- Notification 140
- Notification Escalation 114
- Notification Messages 217
- Notification Using 130
 - Numeric Pager 130
- Notification_dt Valid 137
- Notifier 106, 112, 117, 359
 - attach 106, 112
 - Configuring 117
 - Parts 107
 - Removing 118
- Notifier List 74, 107-108, 112, 118, 130, 282
 - edit 282
 - open 108
 - Use 108, 282
 - view 108

Notifier List window 108, 118

 use 108

Notifier Name 107

Notifier Parameters 107

Notifier Schedule 107, 125, 132, 139

Notifier Settings window 112-113

Notifier Type 106, 117, 122, 125, 132,
 135

Notifier Type dropdown menu 123,
 130

Notifiers window 108, 113, 363

 open 108, 363

Notifiers/Alerts 106

 Overview 106

NT 592

NT Services 249, 592, 739

 choose 593

 execute 595

 Monitoring 592

 open 593

NT Services item 594

NT Services Probe 592

Ntfy 217

NUcastPkts 601

Num-lines 700

Numeric Pager 130

 Notification Using 130

O

OBJECT IDENTIFIER 154, 735

OCTET STRING 141

Octets 601

Offscreen 219

OID 231, 600, 735

 ifNumber 735

 specified 736

 tcpConnState 738

OK 44, 51-52, 54-55, 67, 69, 81, 108-
 109, 114, 121, 125, 132, 139, 141,
 154, 200, 202, 239, 270, 275, 278,
 284, 352, 375, 380, 386, 410, 593,
 742

 Alarm 108

OKAY 411

Old Maps 221

Older Formats 621

Only SNMP 187

Open Recent 350

Open Status Window 159

Open URL 39

OpenSSL 287

Organizational Unit 286

OS 213, 226, 739

OSX 65, 128

OSX Network 733

Other Thresholds 71

Other Tips 98

 Arranging Your Maps 98

Outage Alarms on Interfaces 179

Outages 222, 691

Outages file 231

Outages Log 222

Outages Log window 222

Outages Web Page 691

Outages window 222

Outgoing 123, 237

 E-mail 236

 SMTP 122

OutOctetNow 220

OutOctetPrev 220

Output 628

Oval 385

P

Packet-based Test Procedure 589

Packet Loss 160, 174, 686

 reset 160

Page Notifier 132

 Configuring 132

Page Setup 351

Page Setup dialog 351

Page Using SNPP 132

Pager ID 127, 132

Pager Notifier 124

 Configuring 124

Pager Settings window 124

Paging 125, 130

 Log File 127, 131

Paging Services 125, 130

 shows 125

Paging Services list 130

Paging Settings window 126

Paging Subscribers 125, 130

 shows 125

Paging<date>.txt 128, 131

Partially-qualified 734

Password 56, 237, 249, 268, 273, 277, 355, 593

PASSWORD 707

PATH 63

Pem 288

Pending.csr 287

 Certificate Signing Request 284

Percent 602

Percent Err 603, 686

 graphing 603

PERCENT ERROR 603

Ping 61, 678

Ping/Echo 160, 410, 686

Ping/UDP-based 187

Pk/s 696

Pkt/Second 686

Pkts 601, 696

 number 696

 sum 693

PLAIN 237

Platform-dependent 62

Platform-specific 62

Plugins 411

PNG 80, 83, 219, 628, 635

 compress 219

 Save 349

PNG file 83

Poll Interval 31, 154

 Changing 154

Popup 604

PORT 56, 63, 237, 706

 Specify 56

Port Number 390

PORT on HOST 706

Port/interface 23, 167

Portable Network Graphics 83

Portnumber 214

Porttype 214

Position 241

Possible Arrangement Approaches 80

Pound/hash 643

Powers 197

PPP 604

Pre-CIDR 732

Pre-Mac OS 739

Preferences 37, 228, 231, 238-239, 243, 356

- Logging 232
- Setting 231
- Use 37, 228

Preferences window 37, 238, 356

Prefix 196

Primary SMTP 237

Print 349

Print Sharing 596

Print Single Page 351

Privacy 229

Private Address Space 732

Private Key 285

Probe 350

Probe Configuration window 591

Probe File Error Messages 215

Probe Picker window 409

Probe Reference Overview 409

Probe timeout 410

Probe Type 35, 49, 55, 123, 390, 599

- Map Status 55

Probename 221

Probes 409, 591, 632, 637, 645, 677, 696

- running 696

Processing 215

- DNS 214
- SNMP 216

Program Files 618

Prompts 252, 592

Properties 594

Proprietary 409

Protocol-specific 411

Province 286

Prt 690, 696

Purple Oval 155

Pw 678

Pw improbe 677

Q

Quick Reference 76

QUIT 695

QuitNo 693

Quitting 213, 222, 347-348

- appName 213
- InterMapper 347-348

R

- RADIUS 410, 678
- RBytes 690, 696
- RDis 690, 696
- Read 31
- READ-ONLY 229, 742
 - set 742
- Read-Only Access 281
- Read-only Community String 736
- READ-WRITE 229, 633
- Read-Write Access 281
- Read/write 253
- Receive Statistics 687
- Received Discards/Minute 603
 - see 599
- Recent Loss 686
- Recently-opened 350
 - Choose 350
- Redirect 233
 - Log Entries 233
- Reference 633
- Register button 8, 227
- Registering 8, 227
- Relaunch 219
- Reload 386, 681, 683, 685
- Reload button 81
- Remote 214, 252, 277, 279, 345, 698, 746
 - enabling 346
- REMOTE 695
- Remote Server 253, 277
 - access 253
 - stop 254
- Remote Server firewall 254
- Remove 53, 62, 108, 115, 118, 178, 198, 202, 232, 264, 267, 272, 283, 381, 636
 - acknowledgement 175
 - Helper Application 61
 - manually-connected 53
 - Notifier 117
 - Users 266, 272
 - Vantage Point 114
- Remove button 266, 272
- Remove Vantage Point 116
- Removing Group Members 270, 275
- Removing Links 52
- Rename 350

- Repeat 113
 - Replacing 677
 - username 677
 - Reply 215
 - ReplyCode 219
 - Report 742
 - Reprobe 363
 - Reprobe/Reprobe Selection 362
 - Request 252
 - username/password 252
 - RErr 690, 696
 - Reset 160
 - Packet Loss 160
 - Resolve
 - address 733
 - Update Address 374
 - Update Name 374
 - Responsibilities 27
 - Restore 67, 350
 - Restore Map window 352
 - Retaining 621
 - Copies 621
 - Reverse Connection 403
 - ReversePath 219
 - Revert 67
 - choosing 67
 - RFC 732
 - RFC 1738 679
 - RFC 1918 732
 - River/water 638
 - Round-Trip Time 181
 - RPC 596
 - RPkt 690, 696
 - Running 8, 226-227, 249, 253, 592, 604, 696
 - InterMapper 226, 249, 253, 592
 - InterMapper Server 249
 - Probe 696
 - Windows NT 592
 - Running Time 226
- S**
- SASL 355
 - Save 67, 199, 285, 349, 627
 - PNG 628
 - Your Map 67
 - Save File dialog 285
 - Save Name 355

- Sbin/ping on Unix 61
- Scale 196
- Scan Network 382
- Scanning 53, 739
 - IP 53
 - Network 53
 - subnet 736
- Schedule window 141
- Scheduled Hours 117
- Schema 643
 - exporting 643
- SCM 593
- Screenshot 402
 - Send 348-349, 402
- Search Domain 236
- Secret&user_name 678
- Secret&username 678
- Segment 691
- Select 68, 81, 86, 99, 176, 230, 355, 385, 591, 742
 - Block 176
 - Display 745
 - Icon window 81, 386
 - Label 86
 - SNMPv1 591
 - SNMPv3 591
 - Use 68
- Select Adjacent 357
- Select All 97, 356
- Select Map Status 54
- Select Other 77
- Select Other submenu 99
- Select Probe Window 49-50
- Select submenu 355
- Send 106, 112, 122, 132, 139, 236, 255, 259, 284, 398, 402
 - Back 398
 - CSR 284
 - e-mail 106, 112, 122, 217, 236
 - mailto MyProbe 219
 - Page Using SNPP 132
 - Screenshot 402
 - SNMP 106
 - syslog 139
 - Use 398
- Send E-Mail 742
- Send Log File Entries 234
- Send syslog 140

- SENSITIVE 650
- Server 139, 403, 619
- Server "MyProbe 219
- Server Command 403
- Server Configuration 118, 234, 249, 254, 258, 260, 285
- Server Configuration Overview 249
- Server Information 226, 745
- Server Information Overview 226
- Server Messages 216
- Server Name 226
- Server Preferences 202, 243, 249
- Server Probes 599
- Server Probes - Proprietary 135, 137, 159, 212, 283, 409, 634, 677
- Server Running Time 226
- Server Settings 112, 118, 130, 224, 231, 240, 243, 254, 258, 260, 264, 282, 285, 356, 591, 740
 - Open 740
 - Use 357
- Server Settings dialog 595
- Server Settings list 594
- Server Settings window 8, 68, 107, 109, 118, 130, 202, 204, 224, 226-228, 231, 238-239, 243, 250, 254, 258, 260, 264, 267, 272, 277, 279, 282, 285, 350, 356, 623, 740, 745
 - Disable 350
 - open 740
 - Use 224, 357
- Server Settings Window Overview 224
- Server Settings>SNMP 230
- Service 124
- Service Control Manager 249, 593
 - opens 593
- Set 68, 80-81, 114, 120, 124, 181, 195, 228, 231, 235, 237, 240, 249, 251, 363, 599, 635, 681, 683, 731, 733, 742
 - Access 251
 - Benchmarks 635
 - Chart Title 195
 - Custom Icons 80
 - Default Device 239
 - Default Device Thresholds 185
 - Default Thresholds 181
 - DNS Monitor Preferences 236
 - DOWN 364
 - E-mail Preferences 236
 - Error Thresholds 181

Geographic Coordinates 81

Interval 681, 683

IP 363, 598

Log File Parameters 232

Map's Colors 69

Map's Default Device Thresholds 71

Map's Default Traffic Thresholds 72

Map Background 80

Notifiers 123

Object's Icon 81

Preferences 231

Read-Only 742

Reload 681, 683

SNMP 364

SNMP Community 229

SNMP Preferences 228

Text 385

Thresholds 181

User 249

Vantage Point 114

WINS Preferences 236

Y-axis 197

Set Address 363, 734

Set Alignment dialog 393

Set Behavior 745

Set Behavior window 741

Set button 679, 682, 684

Set Comment 363

Set Community 231, 364, 742

Set Community window 741

Set DNS Monitor 236

Set Info submenu 50, 231, 734

Set Latitude/Longitude 362

Set Poll Interval 375

Set Probe 50, 231, 364

Set Probe Info submenu 410

Set Probe window 55

Set Thresholds 181, 376

Set Timeout 410

Set Timeout window 362

Set Vantage Point 115, 364

Settable 589

Settings/user/IMRemote 746

SHA 230

Shared Secret 678

Shared%20secret 678

- Shared_secret 678
- Sharedsecret 678
- Shift 224
- Shift-click 77, 381
- Short 734
- Short-term Packet Loss 174
- Short DNS Name 390
- Short, Smart Name 390
- Show Charts 194
- Show Client Log 405
- Show Date 198, 244
- Show Day 198, 244
 - Week 198, 244
- Show Info Window 161, 741
- Show InterMapper Control Center 12
- Show Legend 195
- Show Legend submenu 194
- Show Server Log 405
- Show Time 198, 243
- Show User 279
- Show/Hide Checkbox 168
- Show/Hide Toolbar 360
- Showing 49, 54, 117, 124, 132, 151, 355, 378, 603, 679, 682, 693
 - Chicago 54
 - Configure Notifier window 117, 125, 132
 - Dartware MIB 151
 - InterMapper 679, 682
 - InterMapper Web Server menu 680, 683
 - Paging Services 125
 - Paging Subscribers 125
- Signed Certificate 284
 - Uploading 287
- Silenced 217
- Silenced e-mail 217
- Silenced SNMP 218
- Simple Network Management Protocol 735
- Simple Network Paging Protocol 106
- Simple Networking 595
- SIZE 154
- Slideshow 398
- Smart Name 390, 734
- SMTP 122, 237, 410
 - outgoing 123

- specify 123
- SMTP Failure 218
- SNMP 42, 44, 106, 121, 140, 151, 157, 159, 216, 228, 364, 380, 400, 409, 589-590, 637, 678, 734
 - AirPort If 378
 - disable 736
 - If 44
 - including 42
 - listen 231
 - processing 215
 - sends 106
 - Set 363
 - specify 44, 591
 - Use 228, 409
- Snmp-device-display 216
- Snmp-device-variables 216
- SNMP-enabled 157, 411
 - MIB 157
- SNMP-speaking 44, 52, 381, 736
 - address 44
 - finding 739
- SNMP Community 229, 380
 - Enter 380
 - setting 228
 - Specify 379
- SNMP Community String 229
- SNMP Console 743
- SNMP Get-Next-Requests 737
- SNMP Get-Request 735
- SNMP GetRequest 46, 383
- SNMP ID 738
- SNMP Information 734
- SNMP MIB 602, 736
- SNMP MIB-II 410
- SNMP MIB file 350
 - Imports 350
- SNMP Preferences 228
 - Setting 228
- SNMP Read-only 229, 382, 591, 736
 - enter 591
- SNMP Read-only Community 229, 736
- SNMP Read-Only Community String 736
- SNMP Read-Write 229
- SNMP Server Settings Pane 230
- SNMP Set-Request 736
- SNMP SysContact 390

- SNMP SysDescr 390
- SNMP SysLocation 390
- SNMP SysName 390
- SNMP sysUptime 160
- SNMP Table 354
- SNMP Trap 140, 230, 736
 - InterMapper 229
 - Listen 231
- SNMP Trap Community 141
- SNMP Trap Community String 141
- SNMP Version 228
- SNMP Version dropdown 591
- SNMP Watcher 735, 743
- SNMPv1 229, 591, 602
 - Selecting 591
- SNMPv1-2c Community 230
- SNMPv1-v2c 229
- SNMPv1-v2c-speaking 229
 - strings 229
- SNMPv2 591
- SNMPv2c 229, 591
- SNMPv3 229, 591
 - Selecting 591
- SNMPv3 Authentication 230
- Snmpwalk 405
- Snooze Alarm 217
- SNPP 106, 132
- SNPP-based 133
- SNPP Port 132
- SNPP Server 132
- Sort submenu 359
- Sound 120
- Sound Name 120
- Sound Notifier 120
 - Configuring 120
- Special Characters 679
 - Encoding 679
- Special Group 253
- Specific Device 186, 188, 231
- Specific folders 618
- Specifying 41, 43, 54, 73, 106, 122, 235, 382, 646, 734
 - Address 643
 - DNS 235
 - e-mail 106
 - Map's Default Notifiers 73
 - OID 735

- Port 56
- SMTP 122
- SNMP 44, 590
- SNMP Community 380
- Spreadsheet-style Import file 633, 643
- Spreadsheet/database 631
- Ss DOWN 693
- Ss DOWN-ACK 693
- SSL 283
- SSL Certificates 283
- SSL/TLS 288
- SSLCACertificateFile 288
- SSLCertificateFile 288
- SSLCertificateKeyFile 287
- SSLv3/TLS 259
- Star 94, 98, 385
 - command - using 94
 - illustrated 385
- Start 41, 213, 258, 260, 740
 - appName 213
 - Telnet Server 260
 - Web Server 258
 - Your Map 41
- Start InterMapper 595
- Start New Log File 233
- Stat 690, 696
- State 9, 120, 621
 - InterMapper 9
 - InterMapper Settings 621
 - None 120
- State/color 179
- Status 154, 167, 399
- Status Bar 31
- Status window 158-159, 175, 179, 363, 745
 - Customizing 159
 - hide 159
 - Open 363
 - Viewing 159
- Stdin 707
- Stdout 707
- Stop 9, 44, 214, 254, 258, 260
 - Auto-discovery 44, 378
 - InterMapper 9, 592
 - InterMapper daemon 9
 - InterMapper RemoteAccess 214
 - Remote Server 253

- Telnet 214
 - uses 731
- Telnet Server 260
 - value 743
- Web Server 258
- Strings 229, 734
 - SNMPv1-v2c-speaking 229
- STRIPPED_MESSAGE 136
- Style 200
- Style submenus 385
- Sub-Dividers 197, 244
- Sub-maps 54
 - Creating 54
- Subdirectory 137
- Submap 55
 - add 55
- Submenu 194, 350, 356, 360, 364, 398, 402, 632
- Submit Bug Report window 402
- Subnet 43-44, 52, 86, 100, 103, 157, 159, 381, 686, 736
 - attribute 731
 - Enter 103
 - indicate 743
 - scanning 739
 - see 743
 - uses 731
 - value 743
- Subnet 192.168.1.0 41
- Subnet List 391
- Subnets 46, 52, 86, 391
- Subscriber 125
- Subscriber dropdown menu 130
- sudo lsof 604
- Sum 693
 - pkts 696
- Sum In 686
- Sum In/Sum Out 160
- Sum Out 686
- Summary Information 690
- Suspend Sounds 22
- Switch Ports 99
 - Connecting Devices 99
- Switches 102, 631
 - IP 631
 - Map 102
- Synchronizing 594
 - Users 594
- SysContact 390

SysDescr 390
SysLocation 390
Syslog 106, 139, 233
 address 107
 Main Logger 107
 send 139
Syslog Notifier 139
 Configuring 139
Syslog Server 233
SysName 390
System Preferences 604
System Tray icon 9
System Version 226
System/Library/Sounds 121
SysUpTime 123, 601-602, 690, 696
SysUpTime.0 221

T

Tab-Delimited TEXT File 349
Tab key 359
TAP 106, 124
Task Bar Menu 41
TBytes 690, 696

TCP 159, 187, 216, 254, 259, 261, 390, 409, 737
 accept 410
 access 214
 Enter 254, 259, 261
 number 409
TCP-based 160, 390, 410
TCP Check 409
TCP Port 390
TcpConnState OID 734
TDis 690, 696
Telelocator Alphanumeric Protocol 124
Telnet 66, 212, 214, 234, 252, 254, 260, 271, 276, 359, 693
 access 252, 267, 272
 End 695
 stopping 214
Telnet Server 260, 693
 access 261
 start 260
 stop 260
 use 261
Telnet Server Command Reference 693

- Telnet Server firewall 261
 - addresses 261
- Telnet Server Messages 216
- Telnetting 743
- Terminal application 604
- Terminal window 65
- TErr 690, 696
- Test IP 741
- Test Notifier 117, 135
- Tests 117
- TEXT 38, 123, 199, 378, 385
 - Editing 123
 - Use 378
- Text-msg 217
- Thawte 287
- The ImProbe URL 677
- The Simple Times 738
- Threshold-condition 212
- Thresholds 181
 - Setting 181
- Thresholds>Device 185
- Thresholds>Traffic 157, 186, 188
- Time Axis Tab 198
- Time Interval 244
- Time Interval dropdown menu 195
- Time Interval Menu 195
- Timed acknowledgement 175
- TimeOut 410, 589
 - Set 363
- Timestamp 123, 141, 212, 605
- TimeStr 218
- Title Bar 24
- TInt TELNET 216
 - TInt Starting telnet 214
 - TInt Stopping telnet 214
- Tools->Folder Options 592
- Tools subdirectory 135
 - InterMapper Settings 137
- Top 386
- Top Err 160
- Top Left 392
- Top Right 392
- Top Rx 160
- Top Tx 160
- TotalErrors 603
- TotalPkts 603

- TPkt 690, 696
- Traceroute 50, 380
- Traditional 82
- Traffic 72
- Traffic Thresholds 181
- Transition 123
 - particular device state sends multiple notifiers 123
- Transmit bytes/second 599
- Transmit packets/second 602
- Transmit Statistics 686
- TRAP 114, 140, 154, 212
- Trap-Related Messages 217
- Trap - Plays 120
- Troubleshooting 599, 741, 746
 - InterMapper 741
 - InterMapper RemoteAccess 746
 - Network 599
- TTL 733
- TXT 233
- U**
- UCD-snmp 736
- UDP 231, 410, 604, 733
- UDP Port 162 Check 228
- Un-Acknowledge 178, 363
- Un-hiding Detail 105
- UNAC 212
- Unacknowledge 177, 179
- Undo 355
- Undo/Redo 357
- Unencoded 679
- Unencrypted 229
- Uninstall 741
- Uninstaller 741
- Unix 128, 139, 235, 708
 - Unix/Linux 65, 592
 - Unix/Linux/Mac OS 621
- Unknown HTTP Command 220
- Unknown HTTP Version 220
- Unmanaged Hubs 102
 - Adding 102
- Unselected - Invert 355
- UP/OK 114
- Update Address 374
 - Resolve Name 374
- Update Name 374
 - Resolve Address 374

- Upgrade 739
- Uploading 287
 - Signed Certificate 284
- Upper Bounds 197, 244
- Uptime 690
- UpTimeNow 220
- UpTimePrev 220
- URL 39, 61, 66, 260, 648, 677
 - Enter 39, 66, 259
 - handle 61
 - importing 677
 - Including 61
- URL-encoded 677
- URLESCAPE 137
- USB 128
- User 237, 249, 266, 272, 277, 279, 593
 - enter 236
 - Managing 270, 275
 - Removing 270, 275
 - set 249
 - Synchronizing 594
- USER 707
- User-settable 157
- User Access 280
 - Controlling 279
- User Information 268, 270, 273, 275
 - Editing 270, 275
- User Information dialog 270, 275
- User list 270, 275
- User Name 56, 139, 230
 - Enter 56
- Userhome/Library/Preferences/InterM
apper Remote 746
- Username 217, 252-253, 260, 593, 677
 - change 677
 - match 596
 - prompted 594
 - prompts 252
 - replacing 677
 - supplies 252
- Username/password 229, 252, 277
 - provide 277
 - request 252
- Users Panel 267, 272
- USGS Aerial 638
- Using 94, 643, 679, 682
 - Arrange Commands 94

- Command Line Interface 643
- Web Server 679, 682
- Using Auto-discover 43
- Using Background Images 85
 - Tips 85
- Using Charts 192
- Using Default Values 65
- Using Double-Click Actions 65
- Using Geographic Coordinates 634, 647
- Using Group Notifiers Intermapper 123
- Using Helper Applications 61
- Using Intermapper Remote Access 345
- Using Notification Dependencies 114
- Using SNMP Version 591
- Using WINS 739
- Usr/bin/java 708
- Usr/local/bin 619
- Util 220, 691
- Utilization
 - Interface 603

V

V.34 128

- Value 213, 743
 - sysUpTime.0 221
- Vantage Point 23, 114, 364
 - move 115
 - Removing 115
 - set 114
- Varbind 231
- Varbinds 231
- Verisign 287
- Version 123, 226
 - Use 226
- Vertex 633, 660
 - applies 634, 643
 - Use 660
- Vertex Attributes 633, 660
- Vertical Axis Tab 196
- Vertical Dividers 201
- Vertices 634, 643
- View 50, 62, 68, 108, 159, 167, 194, 279, 347-348, 401, 684, 688
 - Chart dropdown menu 194
 - Chart menu 194
 - Client 403

- Helper Applications Customize window 62
- Information 688
- Interfaces window 167
- Log 348-349
- Map Settings Window 68
- Notifier List 108
- Select Probe window 50
- Status Windows 159
- Summary Information 690
- View as
 - Map 359
- View Menu 347-348, 359
 - Use 347-348, 359
- VLAN 99
- Vlans 745
- W**
- WAN 132
- WARN 114, 141, 154
- Warning 29, 71, 106, 112, 121, 156, 410
 - Alarm 108
 - generate 71
- WAV 121, 623
- Web 252, 277, 279, 359
- Web-based Service 638
- Web Device List 692
- Web Page 623, 680, 682
 - Customizing 682, 684
 - Reloading 681, 683
- Web Server's Stop button 258
- Web Server firewall 259
 - addresses 259
- Web Server Messages 219
- Web Servers 84, 258, 679, 682
 - access 259
 - Connecting 260
 - start 258
 - stop 258
 - use 259
 - Using 679, 682
- Week 198, 244
 - Show Day 198, 244
- Weekend Pager 117
- Whitespace 50, 380
- Wildcards 250

- Window
 - Edit Device Label 387
 - Window System Tray 10
 - Window>Logs submenu 222
 - Window>Logs>Debug menu 405
 - Windows 9, 43, 52, 61, 121, 128, 235, 249, 378, 385, 407, 592, 621, 693
 - Windows 2003 10
 - Windows CA 287
 - Windows menu 193-194, 205, 211, 222, 231, 347-348, 397
 - Charts submenu 194
 - Logs submenu 231
 - Use 347-348
 - Windows Networking 595
 - Windows NT 592
 - running 592
 - Windows NT Services Probe 592
 - Windows Only 138
 - Windows OS 592
 - Windows popup window 9
 - Windows Server 2003 595
 - Windows XP 10
 - running 592
 - Windows, Unix 407
 - WINDOWS/Profiles/user/IMRemote 746
 - Windows/Unix 76
 - WinPopup 138
 - WINS 45, 50, 235, 739
 - Comma-separated list 236
 - use 235, 739
 - WINS Preferences 236
 - Setting 235
 - WINS Scope 236
 - Enter 235
 - leave 236
 - WINS/NetBIOS 236
 - Wire 241, 386
 - Wire icon 385
 - Wire item 387
 - Wrong Community 737
 - Wrong DNS name/IP 736
- X**
- X-axis 244
 - XCoordinate 647
 - XML 42, 629
 - XML file 353

XP 592

XP Home

running 592

Y

Y-axis 197

YCoordinate 647

Z

Zoom 155, 398

Choose 398

In On 155

Contacting Fortra

Please contact Fortra for questions or to receive information about Intermapper. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the [Fortra Support Portal](#).

Customer Portal

For additional resources, or to contact Technical Support, visit the Intermapper Community Portal at <https://community.fortra.com/>.

For additional resources, or to contact Technical Support, visit our website at <https://www.fortra.com/support>.

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.