

SolarWinds

ipMonitor

QuickStart Guide

Copyright© 1995-2008 SolarWinds.net, Inc. all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds ipMonitor™, SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, and Windows 2003 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

QuickStart Guide 01.09.2008 version 9.0

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	1.866.530.8100 www.solarwinds.com
Technical Support	www.solarwinds.com/support
User Forums	http://www.thwack.com/

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

SolarWinds ipMonitor Documentation Library

The following documents are included in the SolarWinds ipMonitor documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for every window in the ipMonitor user interface
QuickStart Guide	Provides installation, setup, and common scenarios for which ipMonitor provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com .

Contents

<i>About SolarWinds</i>	<i>iii</i>
<i>Contacting SolarWinds</i>	<i>iii</i>
<i>Conventions</i>	<i>iii</i>
<i>SolarWinds ipMonitor Documentation Library</i>	<i>iv</i>

Chapter 1

Installing SolarWinds ipMonitor	7
<i>Licensing ipMonitor</i>	<i>7</i>
<i>System Requirements</i>	<i>7</i>
<i>Installing SolarWinds ipMonitor</i>	<i>7</i>
<i>Configuring SolarWinds ipMonitor</i>	<i>8</i>
<i>Installing the Self-Signed Certificate</i>	<i>8</i>

Chapter 2

Getting Started	11
<i>Discovering Your Network Devices and Adding Monitors</i>	<i>11</i>
<i>Monitoring Your Network</i>	<i>13</i>
<i>Adding Web Resources</i>	<i>13</i>
<i>Re-arranging Web Resources</i>	<i>13</i>
<i>Inspecting Devices in the Dashboard</i>	<i>13</i>
<i>Organizing Your Network</i>	<i>14</i>
<i>Creating Groups</i>	<i>14</i>
<i>Creating SmartGroups</i>	<i>14</i>
<i>Drawing Maps</i>	<i>15</i>
<i>Understanding Alerts</i>	<i>17</i>
<i>Generating Reports</i>	<i>18</i>

Chapter 1

Installing SolarWinds ipMonitor

ipMonitor provides a simple, wizard-driven installation process.

Licensing ipMonitor

ipMonitor can collect data and detailed information from any of your Windows or SNMPv2-enabled devices, including routers, switches, firewalls, and servers. You license ipMonitor by the number of monitored services: 100, 250, 500, 1000, 1500, or 5000 monitors.

System Requirements

System requirements for ipMonitor vary based upon the number of monitors. The following table represents the minimum system requirements.

Software	Requirements	
Operating System	A 32-bit version of one of the following: - Windows Vista (IPv4 mode only) - Windows XP Professional SP2 or later - Windows Server 2003 SP1 and R2	
Web Browser	Microsoft Internet Explorer 6 and up, Firefox 1.5 and up, Opera 9 and up.	
Hardware	~500 monitors	~5000 monitors
CPU Speed	Single core 2.0 GHz	Dual core 2.0 GHz
Hard Drive Space	240MB	2.4GB
Memory	512MB	1 GB

Note: 500 monitors require approximately 1.5MB of hard drive space per day for storing statistics.

Installing SolarWinds ipMonitor

Complete the following procedure to install ipMonitor:

1. Log on to the server on which you want to install ipMonitor.
2. **If you downloaded the product from the SolarWinds website**, navigate to your download location and launch the executable.
3. **If you received physical media**, browse to the executable file, and then launch the executable.
4. Review the Welcome text, and then click **Next**.

5. Accept the terms of the license agreement on the License Agreement window, and then click **Next**.
6. Provide your name and organization, and then click **Next**.
7. Provide an installation destination folder on the Destination Folder window, and then click **Next**.
8. Click **Install** on the Ready to Install the Program window.
9. Click **Finish** on the InstallShield Wizard Completed window to launch the ipMonitor 9.0 Configuration Program.

Configuring SolarWinds ipMonitor

Complete the following procedure to configure a 21-day evaluation of ipMonitor:

1. In the Configuration Program, click **Next** on the Software Licensing window.
2. Click **Next** on the First Run Service Settings window.
3. Click **Next** on the First Run HTTP Server Settings window.
4. Add a new administrator account:
 - a. Enter the user name for the account in the **User Name** box.
 - b. Enter the password for the account in the **Password** and **Confirm Password** boxes.
 - c. Click **Add Account**.
5. Click **Next** on the First Run Administrator Account window.
6. In the **Administrator's Email Address** box, type an email address.
7. Click **Next** on the First Run Default ipMonitor Serving Settings window.
8. Click **Finish** to complete the configuration steps and launch ipMonitor.

Installing the Self-Signed Certificate

Complete the following procedure to install the self-signed certificate and allow secure ipMonitor sessions:

1. ***If you are using Firefox as your web browser***, you see a **Website Certified by an Unknown Authority** dialog box. Complete the following step:
 - Select the **Accept this certificate permanently** option, then click **OK**.

2. *If you are using Internet Explorer 6 as your web browser*, you will see a **Security Alert** dialog box and must complete the following steps:
 - a. Click **View Certificate**.
 - b. Click **Install Certificate** to launch the Certificate Import Wizard.
 - c. Click **Next**.
 - d. Select the **Automatically select the certificate store based on the type of certificate** option, and then click **Next**.
 - e. Click **Finish**.
 - f. Click **Yes** to install this certificate.
 - g. Click **OK** to close the Certificate Import Wizard dialog box.
 - h. Click **OK** to close the Certificate dialog box, and then click **Yes**.
3. *If you are using Internet Explorer 7 as your web browser*, you will see a certificate error and must complete the following steps:
 - a. Click **Continue to this website (not recommended)**.
 - b. Click the **Certificate Error** on the address bar to view the security report.
 - c. Click **View Certificates**.
 - d. Click **Install Certificate** to launch the Certificate Import Wizard.
 - e. Click **Next**.
 - f. Select the **Automatically select the certificate store based on the type of certificate** option, and then click **Next**.
 - g. Click **Finish**.
 - h. Click **Yes** to install this certificate.
 - i. Click **OK** to close the Certificate Import Wizard dialog box.
 - j. Click **OK** to close the Certificate dialog box.

The self-signed certificate is now trusted for secure ipMonitor sessions.

Chapter 2

Getting Started

A wealth of information can be collected about your network using the powerful tools that comprise ipMonitor. The following section steps you through some common use cases. By stepping through this quick introduction, you learn how to discover devices on your network and monitor them, keep your network organized using smartgroups and maps, create alerts and associate them with monitors, generate reports, and display network status using the Dashboard and the Network Operations Center (NOC) views.

1. Discovering Your Network Devices and Adding Monitors
2. Monitoring Your Network
3. Organizing Your Network
4. Drawing Maps
5. Understanding Alerts
6. Generating Reports

Discovering Your Network Devices and Adding Monitors

As this is the first time you have run ipMonitor, ipMonitor takes you to the Getting Started Wizard after you log on. Complete the following procedure to discover your networked devices.

To discover devices on your network:

1. Log on to the ipMonitor web interface with your administrator account username and password.
2. Select **Yes** on the Getting Started page, and then click **Next**.
3. Select **IP Range**, and then click **Next**.
4. ***If you have Windows network credentials you want to use for discovering Windows network resources***, complete the following procedure:
 - a. Click **Select** to open the Credentials window.
 - b. Click **New Credential** to launch the Credentials Wizard.
 - c. In the **Credential Name** text box, type a name for the credential, and then click **Next**.

- d. Type the details of your Windows network credential in the **Account**, **Password**, and **Confirm Password** text boxes, then click **Next**.
 - e. Click **Credential may only be used by my Account**, and then click **Next**.
 - f. Click **Finish**.
 - g. Click **Apply**.
5. *If you have SNMP community strings you want to use for discovering SNMP devices and resources*, complete the following procedure:
- a. In the **SNMP Credential** text box, type the SNMP community string.
 - b. *If you want to specify additional SNMP community strings*, click **Add SNMP Community** to create additional entries.
6. Click **Next**.
7. In the **Start Address** and **End Address** text boxes, type the start and end of an IP address range to scan for devices.
- Note:** Scanning a large IP address range may take a long time. In the interest of providing you with a quick start, please select only a small IP address range of 100 addresses or less for your initial scan.
8. Click **Begin Discovery Scan**, and then wait for the device scan to finish.
9. Select **All found devices**, then click **Next**.
10. Wait for a few scans to finish. Scans are finished when the device state changes from **Scanning device** to **Scanning Complete**.
11. Click **Add All Scanned Devices**.

A new browser window or tab appears, containing the monitor summary.

12. Scroll down to the end of the monitor summary, and then click **Add Now**.
13. Select **Use an existing alert**, and then click **Next**.
14. Click **Modify Alert & go to Dashboard**.

The Dashboard page appears, summarizing the current network state.

Monitoring Your Network

The Dashboard page you are viewing contains a sampling of small reports called Web Resources that show you the current status of your network devices and monitors.

Adding Web Resources

Complete the following procedure to add another Web Resource to the Dashboard:

1. On the **Add Web Resource** menu, click **Top XX Devices by Availability**.
2. Click **OK**.

The web resource appears in the dashboard.

Re-arranging Web Resources

Complete the following procedure to change the layout of the Dashboard:

1. Move the pointer over the web resource title **Top 10 Devices by Availability**.

The pointer changes shape to a four-pointed arrow.

2. Drag the title to a new location.

Inspecting Devices in the Dashboard

Complete the following procedure to examine devices in the dashboard.

1. In the **Top 10 Devices by Availability** web resource, click **ipMonitor Host**.
You are now seeing the Dashboard page for this device.
2. In the **Monitor states for ipMonitor Host** web resource, click **ipMonitor [CPU-Processor Total]**.

You are now seeing the Dashboard page for this monitor.

Organizing Your Network

The Devices tab contains views that allow you to classify, organize, and see the status of the devices and monitors in your network. One way you can classify and organize your devices and monitors is by creating groups.

Creating Groups

A group is a collection of devices, monitors, and potentially other groups. You may create groups inside other groups, and monitors and devices may be members of multiple groups. Complete the following procedure to create a group:

1. Click the **Devices** tab.
2. In the **Groups** tree, select the **My Network** group.
3. On the **Add** menu, click **Add New Group**.
4. In the **Group Name** box, type `Important Devices`, and then click **OK**.
Your new group, Important Devices, appears in the Groups tree list.
5. In the **Groups** tree, select the **Important Devices** group.
6. On the **Add** menu, click **Add Existing Devices**.
7. From the device list, select at least one device that you consider important, and then click **Continue**.

Creating SmartGroups

A SmartGroup is a dynamic group whose contents are determined by parameters that you set. Unlike regular groups, whose contents never change, the contents of a SmartGroup automatically keep track of changes in your network. Some examples of SmartGroups include:

- a group of all your network devices located in Texas.
- a group of all the offline monitors in your network.
- a group of all the Cisco devices in your network.

Complete the following procedure to create a SmartGroup that contains all the Cisco devices in your network:

1. In the **Groups** tree, select the **My Network** group.
2. On the **Add** menu, click **Add New SmartGroup**.
3. In the **Name** box, type `All Cisco Devices`.
4. In the **SmartGroup Contains** box, select **Devices**.

5. In the **Start With** box, select **No Devices**.
6. Add a rule to add devices with the string “Cisco” in the Device Vendor property to the SmartGroup
 - a. Click the arrow in the box after “devices, where”, and then select **property** from the list.
 - b. Click **Click here to Select a Property** to open the property window.
 - c. In the box at the bottom of the window, select **Device Properties**.
 - d. In the list, click **Device Vendor**, and then click the Close button to exit the window.
 - e. Click **RegEx Wizard** to open the Regex Wizard window.
 - f. In the **Match begins with** text box, type `Cisco`, and then press TAB.
 - g. Scroll down to the bottom of the window, and then copy the text `\iCisco.*?$` that has been created in the **Regular Expression you have built** box.
 - h. Click **Close** to return to the **Edit SmartGroup** page.
 - i. Paste `\iCisco.*?$` into the **Matches regular expression** box.
7. Click **Preview** to preview the contents of the new SmartGroup.
8. Click **OK** to create the SmartGroup.

Drawing Maps

A well-drawn map allows you to better visualize the effects of a failing device or monitor. ipMonitor creates default maps for each group and device in your network, but you will get the most benefit from your maps if you customize them by creating connections between devices and adding background images.

Complete the following procedures to customize the map for the Important Devices group:

1. View the map of the Important Devices group:
 - a. Click the **Devices** tab.
 - b. In the **Groups** tree, select the **Important Devices** group.
 - c. On the **view** menu, click the **Map** button.

2. Resize your view of the map:

- Move the **Scale** slider left to zoom in and right to zoom out.
- or -
- Click **Fit To Screen** to automatically size the map to the full extent of the area.

3. Click **Edit Map**.

4. Change the icon of a map object:

- a. Click the object. A bounding box appears.
- b. Click the **Icons** list, and then select an icon category.
- c. Click an icon. The object changes to that icon.

5. Resize a map object:

- a. Click the object. A bounding box appears.
- b. Drag a handle on the bounding box to resize it.

6. Create a connection between two map objects:

- a. Click the line drawing tool from the **Drawing Tools** palette.
- b. Drag one object to the other to draw a line.

7. Assign a monitor status to the connection:

- a. Click the selection tool from the **Drawing Tools** palette.
- b. Click a line to select it.
- c. Click **Assign monitor**.
- d. Select a monitor option and click **OK**. A monitor status indicator appears over the line.

8. Change the layout of the map:

- Select an object and drag it to a new location.
-or-
- On the **Auto Layout** menu, click a layout type:
 - Circular
 - Organic
 - Tiled

9. Add a background to the map:
 - a. On the **Change Background** menu, click **Upload Background**.
 - b. Click **Browse**, and then select a JPG, PNG, or GIF format image file.
 - c. Click **Upload**.
10. Click **Save** to save the map.
11. Click **Close** to exit the map editor.

Understanding Alerts

An alert is a configurable response to a change in the status of a monitor. One of the many strengths of ipMonitor is the ability to alert on almost every aspect of your network. You can trigger responses when an alert is generated and when it is resolved; you can create simple or complex conditions under which an alert is triggered or reset; you can suppress alerts when a set of simple or complex conditions exist; you can create an escalation path that triggers when an alert remains unresolved.

The triggering of an alert and the resetting of an alert can trigger any number of the following types of actions:

- Send an email, page, or beeper message.
- Send an SNMP trap.
- Send a Windows “Net Send” broadcast message
- Log alerts to a file or to the Windows event log.
- Run an external program.
- Reboot a server or restart a service.

Complete the following procedure to create an alert that watches for changes in the Important Devices group, and that escalates the issue to management if the down state persists after the third alert:

1. Click the **Configuration** tab.
2. Click **Alert List**.
3. Add a new alert:
 - a. Click **Add Alert**.
 - b. In the **Alert Name** box, type `Notify techs then escalate`.

4. Add an action to notify technicians:
 - a. On the **Add Action** menu, click **Simple Email**.
 - b. In the **Action Name** box, type `Send email to techs`.
 - c. In the **Send an Email Message To** box, type a local email address.
 - d. Click **OK**.
5. Add an action to notify managers after three alerts:
 - a. On the **Add Action** menu, click **Simple Email**.
 - b. In the **Action Name** box, type `Send email to manager`.
 - c. In the **Alert Range** box, type `3-`
 - d. In the **Send an Email Message To** box, type a local email address.
 - e. Click **OK**.
6. Associate this alert with a group of devices:
 - a. Click **Add Groups**.
 - b. Select the **Important Devices** group, and then click **Continue**.
7. Click **OK**.

Generating Reports

Reports make it easy to view detailed, historical monitoring data about devices and monitors in both graphical and tabular formats.

Complete the following procedure to generate a quick disk utilization report of the ipMonitor host:

1. Click the **Reports** tab.
2. From the **Device Reports** list, click **Disk Utilization**.
3. From the **Select Device** list, select **ipMonitor Host**, and then click **Continue**.
4. Click **Cancel / Back** to return to the Reports tab.