SolarWinds ipMonitor

Administrator Guide

ipMonitor Administrator Guide v10

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 http://www.solarwinds.com
User Forums	http://www.thwack.com contains the community oriented user forums
Technical Support	support.solarwinds.net/support you need a customer account to access the Customer Support area of the website.

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.
Italics	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

ipMonitor Documentation Library

The following documents are included in the 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 the latest information about known issues, and updates. The latest Release Notes can be found at http://www.solarwinds.com.

Contents

Chapter 16

Chapter 17

Index

Chapter 1

Introduction

ipMonitor provides a proven agentless architecture as a backbone for a comprehensive feature set. Reliable data collection and tested ease of use makes ipMonitor the ideal network monitoring solution for your small to medium business.

ipMonitor not only provides the tools you need to proactively Monitor your network from end to end, it also includes the necessary alert types to notify you in the event of trouble and automatically recover critical applications, servers and infrastructure devices whenever possible.

Monitoring

ipMonitor proactively discovers your critical network resources and tracks their availability, responsiveness and performance quality. It monitors the health of:

- Business and web applications, such as SQL databases, web servers, commerce, and mail servers.
- Infrastructure equipment such as server computers, switches, routers and power back-up systems.
- Services including IP-based services and Windows services.

ipMonitor offers more than 55 different monitor types:

- User experience monitors that perform multiple transaction tests to measure response time and analyze results for critical applications and infrastructure equipment.
- Windows NT/2000/XP/2003/2008 system monitors specifically designed to monitor key systems, such as services and event logs.
- Resource monitors that monitor finite system resources, and then alert before consumption becomes critical.
- Availability monitors that support all popular OSI layer 7 (Application Layer) protocols based on IP networking.
- SNMPv2 trap support along with SNMPv1 traps.
- Exchange 2007 Monitor.
- WMI Generic Windows Monitor

Alerting

When quality of service degrades, thresholds are exceeded, or failures occur, ipMonitor provides a comprehensive suite of alerting tools:

- Alert actions offer industry standard methods to alert responsible individuals:
  - by phone using email or SMS.
  - by numeric or alphanumeric pager.
  - by wireless device using email or net broadcast.
- Integration actions allow for integration with other applications such as network management solutions, ticket systems, and custom recovery applications.
- Recovery actions allow you to automatically initiate recovery procedures.

Recovery

Each monitor supports the ability to set operating environment variables. Alerts use these variables when a problem is detected. During a failure, corrective action is taken immediately using ipMonitor's recovery actions:

- Restart failed applications, perform diagnostics, back up files, run scripts, and so on.
- Reboot the server or workstation.
- Restart a list of services on a specific remote machine, including services with dependencies.

Reporting

ipMonitor offers in-depth visual analysis of your monitor statistics. Detailed reports allow you to see equipment performance:

- Dashboard and Network Operation Center (NOC) views that provide at-a-glance reports for all personnel who manage the network.
- Configurable data analysis reports in both graphical and tabular formats.
- Quick reports offer instant access to statistics data recorded by any monitor or group.
- Zoomable reports allow you to explore deep into the ipMonitor database of test results to easily identify the error messages that triggered alerts.
- Email reports offer distribution to single or multiple recipients.

ipMonitor thwack integration

- Provides the most recent thwack community forum posts and file uploads for ipMonitor.

Chapter 2

Installing SolarWinds ipMonitor

The following sections help you ensure you have the appropriate system requirements, and then guide you through installing ipMonitor.

System Requirements

The following minimum system requirements must be met to successfully run ipMonitor:

Software	**Requirements**	
Operating System	A 32-bit version of one of the following: Windows Vista (IPv4 mode only) Windows XP SP2 or later Windows Server 2003 SP1 and R2 Windows 2008	
Web Browser	Microsoft Internet Explorer 6 or later Firefox 1.5 or later.	
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

Optional System Requirements

Some advanced features of ipMonitor have additional requirements as follows:

Optional Feature	Requirements
Modem and Telephony	For Simple beeper, SMS TAP, and SMS UCP alert actions: • Hayes-compatible 1200 baud or faster hardware modem. • Dedicated telephone line or a telephone system that is always able to free up an outbound telephone line on demand. For SMS GSM alert actions: • Hayes-compatible GSM/GPRS modem • GSM Mobile Network subscription
SSL Certificates	Valid certificates: • Self-signed certificates • CA certificates such as VeriSign • Microsoft Windows 2000 certificate services Note: After installed, available certificates are selected from the Local Machine certificate store.
ADO and ADO User Experience monitors	MDAC Version 2.6 SP2.or later

Installing ipMonitor

The following procedure guides you through install 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 install file, click the exe.

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 EULA and then click **Next**.

6. Provide a user name and organization name and then click **Next**.

7. To select a different install location, click **Change** and navigate to the desired destination folder and then click **Next**.

8. Click **Install** on the Ready to Install Program window.

9. Click **Finish** to launch the ipMonitor Configuration Program.

Note: It is recommended that you do not install ipMonitor on a domain controller. To take full advantage of ipMonitor's security features, we suggest that you create an account specifically for the ipMonitor Service to run under that applies the minimum tokens required by the ipMonitor Service to operate successfully. However, when ipMonitor is installed on a domain controller, the Credential Manager cannot be enabled to impersonate Windows accounts with elevated permissions. There is no allowance for trust relationships outside of the domain, resulting in limited access to many ipMonitor features.

After installing the software through the setup wizard and completing the Configuration Wizard, you are prompted to enter the license activation key for your product. If you do not have an activation key, the product runs in a time-limited evaluation mode.

To evaluate the software without a license:

Click **Continue Evaluation**.

Licensing ipMonitor

To license the software on a server with Internet access:

1. Click **Enter Licensing Information**.
2. Select **I have internet access and an activation key**.
3. Click the http://www.solarwinds.com/customerportal link to access the customer portal on the SolarWinds web site.
4. Log on to the portal using your SolarWinds customer ID and password.
5. Click **License Management** on the left navigation bar.
6. Navigate to your product, choose an activation key from the **Unregistered Licenses** section, and then copy the activation key.
7. ***If you cannot find an activation key in the Unregistered Licenses section,*** contact SolarWinds customer support.
8. Return to the Activate ipMonitor window, and then enter the activation key in the **Activation Key** field.
9. ***If you access Internet web sites through a proxy server,*** click **I access the internet through a proxy server**, and enter the proxy address and port.
10. Click **Next**.
11. Enter your email address and other registration information, and then click **Next**.

To license the software on a server without Internet access:

1. Click **Enter Licensing Information**
2. Select **This server does not have internet access**, and then click **Next**.
3. Click **Copy Unique Machine ID**.
4. Paste the copied data into a text editor document.
5. Transfer the document to a computer with Internet access.
6. On the computer with Internet access, complete the following steps:
7. Browse to http://www.solarwinds.com/customerportal/licensemanagement.aspx and then log on to the portal with your SolarWinds customer ID and password.
8. Navigate to your product, and then click **Manually Register License**.
9. If the **Manually Register License** option is not available for your product, contact SolarWinds customer support.
10. Provide the Machine ID from Step 5, and then download your license key file.
11. Transfer the license key file to the server.
12. Return to the Activate ipMonitor window, browse to the license key file, and then click **Next**.

Maintaining Licenses with License Manager

SolarWinds License Manager is an easily installed, free utility that gives you the ability to migrate Orion licenses from one computer to another without contacting SolarWinds Customer Service. The following sections provide procedures for installing and using License Manager.

Installing License Manager

Install License Manager on the computer from which you are migrating currently licensed products.

Note: You must install License Manager on a computer with the correct time. If the time on the computer is off by as little as 5 minutes, in either direction, from Greenwich Mean Time (GMT), you will be unable to reset licenses without calling SolarWinds Customer Service. Time zone settings do not affect and do not cause this issue.

To install License Manager:

1. Navigate to http://support.solarwinds.com/support/default.cfm.
2. Provide your SolarWinds Customer ID and password, and then click **Login**.
3. Click **Downloads & Updates** in the left navigation pane.
4. Locate the Download Licensed Software section of the page, and click **SolarWinds License Manager**.
5. Unzip the downloaded file, and then run `LicenseManager.exe`.

Using License Manager

You must run License Manager on the computer where the currently licensed SolarWinds product is installed before you can move licenses to a new installation. The following procedure deactivates currently installed licenses that can then be transferred to a new installation.

To deactivate currently installed licenses:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.
2. Check products to deactivate on this computer, and then click **Deactivate**.
3. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

   Note: Deactivated licenses are now available to activate on a new computer.

When you have successfully deactivated your products, log on to the computer on which you want to install your products, and then begin installation. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is then assigned to the new installation.

Configuring ipMonitor

The ipMonitor Configuration program helps you configure several key parameters for the `ipmonitorsrv` ipMonitor service:

- Entering an IP address and port number on which the web interface listens.
- Selecting an SSL certificate for secure communication.
- Changing the Windows Service account context.

First Run Mode

After you first install ipMonitor, the Configuration program automatically runs in "First Run" mode:

- Gets you up and running quickly.
- Runs once.
- Automatically provides default parameters.
- Requires you to configure an ipMonitor administrator account.

This initial configuration process allows you to set up the following default Monitors, allowing you to begin testing your system resources immediately:

- CPU usage monitor
- Memory usage monitor
- Drive Space monitor

In addition, the First Run mode creates a default group, alert, and email action, and associates them with the new Monitors.

Running the ipMonitor Configuration Program

To start the ipMonitor Configuration program, click **Start > All Programs > SolarWinds ipMonitor > Configure ipMonitor**. If the ipMonitor Service is not running, you are prompted to **Launch the ipMonitor Service**. Click **Yes** to start the Service.

The Configuration Program is not used to add or configure monitors, alerts, or actions. The addition or modification of ipMonitor elements is done through the ipMonitor Web Interface.

Using Express Discovery

Express Discovery assists in adding commonly used monitors in a quick and easy wizard-driven user interface. For new installs the Express Discovery will begin after the initial web interface login.

By default the most common monitors are added; CPU Usage, Memory, Usage, Drive Space, Bandwidth Usage, Ping, HTTP, HTTPS, Windows, Exchange Server 2000/2003, Exchange Server 2007, SQL Server, Active Directory.

To enable the Express Discovery:

1. Log on to the ipMonitor web interface with your administrator account username and password.
2. Click **Devices** and then select **Discovery Express Scan**
3. Select which applications and resources to monitor and then click **Next**.
4. Enter IP Ranges. In the **Start Address** and **End Address** text boxes, type the start and end of an IP address range to scan for devices and click **Next**.

   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.

5. ***If you have Windows network credentials you want to use for discovering Windows network resources***, complete the following procedure:

   a. Click **Next** 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**.

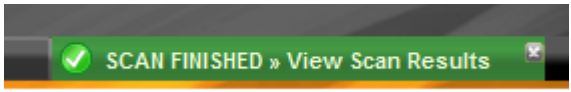
   g. Click **Apply**.

   . ***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** to begin Discovery Scan and then wait for the device scan to finish.
7. Wait for a few scans to finish. Scans are finished when the device state changes from **Scanning device** to **Scanning Complete**.
8. Click **Add All Scanned Devices**.
9. A tab appears on the Dashboard containing the scan results summary.



10. Select **Show Alert List** to review the added alerts.

11. Click **Go to Dashboard**. The Dashboard page appears, summarizing the current network state.

Note: User experience monitors must be added manually because critical information in each monitor is specific to each network environment

Adding ipMonitor Administrator Accounts

The Administrator Account window is used to add administrator accounts to ipMonitor. Accounts added here are strictly internal to the ipMonitor software, and are not associated with Windows local machine or domain accounts.

The first Administrator Account must be created from the ipMonitor Configuration program. The following rules apply to Administrator accounts:

- Administrator accounts cannot be deleted until they are demoted within the ipMonitor Administration web interface to a general user.
- There must always be at least one administrator account.
- Administrator accounts cannot delete themselves, nor can they demote themselves.

To create a new Administrator account

- Click **Add Account**.

Note: All account information is stored internally using RSA 512/1024 bit encryption.

Communications: Web Server Ports

From this window, you can:

- Configure the IP Address and Port combinations for the ipMonitor web interface to listen on.
- Set the IP Address and Port combination ipMonitor uses to listen for incoming SNMP Traps.

HTTP Server TCP Settings

ipMonitor requires that one or more IP Address and Port combinations be assigned to it in order to enable communication via the HTTP and HTTPS protocols. These are the protocols you use to log in and administrate ipMonitor.

Use the **Communications: Web Server Ports** window to enter any number of Port combinations for ipMonitor to listen on. The **Delete** button may be used to remove an entry, while the **Edit** button allows you to make modifications to an entry. Click the **Add** button to add additional IP Address and Port combinations.

For each HTTP entry:

- Type an IP Address and Port combination that is not used by any other server application.

For each HTTPS entry:

1. Type an IP Address and Port combination that is not used by any other server application.
2. Select the **Enable SSL** check box. This option requires an SSL Server Certificate to be assigned to your ipMonitor installation.

To have ipMonitor listen on all IP Addresses bound to the host machine on a specific Port, enter an IP Address of 0.0.0.0. For example, a value of [0.0.0.0][8080] makes ipMonitor listen on every IP Address assigned to the machine on port 8080.

Note: If other HTTP Services are installed on the ipMonitor host machine, verify that their IP Address and Port settings do not conflict with ipMonitor Port settings. For example, another HTTP Service might use the default port 80.

ipMonitor is a stand-alone HTTP server. It does not integrate into or require other web server Services such as IIS (Internet Information Server).

You can generate and assign a Self-Signed Certificate using the **Secure Socket Layer Certificate** options in the Configuration program. Self-signed certificates are free.

Configuring the SNMP Trap Listener

Any SNMP Trap Monitors created in ipMonitor uses the IP Address and Port combination entered in the **SNMP Trap Listener** section to listen for incoming SNMP Traps.

The SNMP - User Experience Trap monitor is an event-based, non-polling monitor. The monitor listens for SNMP Traps sent to it by any number of SNMP agents on the network. Each incoming Trap is parsed and compared to the settings of the existing SNMP Trap monitors to determine whether an Information alert action should be triggered.

To listen to all IP Addresses on a specific port, type an IP address of 0.0.0.0. ipMonitor listens to every IP Address on that port.

For example: [0.0.0.0][162]

Port 162 is the standard SNMP listening port.

Note: Any SNMP agents that are expected to send Traps to ipMonitor must be configured to send Traps to the IP address and port specified here.

If the **SNMP Trap Listener** is not enabled, SNMP Trap Monitors do not work, even if the Monitor itself is enabled.

Note regarding Windows SNMP Trap Service:

If the Windows SNMP Trap service is enabled on the ipMonitor host computer, it is very likely to conflict with ipMonitor's SNMP Trap Listener. Both are bound by default to port 162.

To resolve conflicts with the Windows SNMP trap service:

- Change ipMonitor's SNMP Trap Listener port to one that is unused, then also change the outbound port of all the SNMP agents sending Traps to ipMonitor.
  -or-
- Disable the Windows SNMP Trap Service from the Windows Control Panel/Services interface. There are no adverse effects to disabling the Windows SNMP Trap service unless you are running another SNMP solution on the ipMonitor server that requires use of the Windows SNMP Trap service.

Communications: Lockout

The **Communications: Lockout** dialog box is used to specify the IP addresses that ipMonitor communicates with.

IP Access Filters are an optional security feature that allow you to either:

- Limit communications to a set of IP Addresses or ranges of IP Addresses.
- Exclude a list of IP addresses or ranges of IP addresses from communicating with ipMonitor.

Click the **Add** button to add a new entry. Your entries may consist of single IP addresses or ranges of IP addresses. The **Delete** button may be used to remove an entry, while the **Edit** button allows you to make modifications to an entry.

To enter a single IP address:

- Enter the same IP address into the **Starting IP Address** and **Ending IP Address** boxes.

To enter ranges of IP addresses:

1. Enter the first IP address in the range into the **Starting IP Address** box.
2. Enter the last IP address in the range into the **Ending IP Address** box.

If needed, you can add additional IP address or ranges of IP addresses at any time by clicking the **Add** button.

Note: For more information regarding security features, see “Security Model” on page 209.

Communicating Using SSL Certificates

The **Communications: SSL** dialog box is used to install or select an SSL certificate. ipMonitor uses SSL to provide the secure exchange of data across non-secure networks, such as the Internet.

The following methods are supported for acquiring an SSL certificate:

- Generate and install a Self-Signed Certificate.
- Acquire a certificate from a trusted Certificate Authority.
- Request a certificate using the Microsoft Windows 2000 Certificate Services Web interface.
- Request a certificate from an enterprise certification authority using the MMC Certificates snap-in.

This section discusses installing a Self-Signed Certificate, which represents the easiest installation method with no cost involved.

Note: The ipMonitor Credentials Manager feature requires that you log in over an SSL-secured connection. If you log in through a non-secure channel, the Credentials Manager:

- Permits only limited viewing of credentials
- Prohibits any changes to credential configuration

Note: For information regarding other methods of installing certificates, see “SSL” on page 213.

Generating a Self-Signed Certificate

To create a Self-Signed Certificate:

1. Access the Communications: SSL window.
2. Select the **Self-Signed** option from the SSL Certificate Mode drop-down menu
3. Click the **Create New Self-Signed Certificate** button.
4. Enter the fully qualified domain name of your ipMonitor server into the **Common Name** text box.

After clicking the **Create** button, information regarding the newly generated Self-Signed Certificate is displayed, and the certificate is created in the Local Machine certificate store.

Important: Click **OK** to accept the SSL Certificate. You have to specifically accept the Certificate; otherwise it is simply added to the store and not assigned to ipMonitor.

Note: After the SSL certificate has been installed, it is necessary to configure ipMonitor to listen for HTTPS traffic. This can be accomplished in the ipMonitor Configuration program by changing the "Communications: Web Server Ports" options.

Trusting a Self-Signed Certificate

The ipMonitor Web Interface Internet shortcut, located on the Windows Start menu under the SolarWinds program group, automatically adjusts to use the HTTPS protocol when you assign an SSL certificate.

The first time you log in to the ipMonitor SSL interface, your web browser displays a security alert.

To install a certificate using Internet Explorer

1. Click **View Certificate**.
2. Click **Install Certificate** button to start the Certificate Import Wizard. This creates trust by copying the certificate to the Trusted Root Certification Authorities store.
3. Select the **Automatically select the certificate store based on the type of certificate** option.
4. After the certificate is added to the store, the self-signed certificate is trusted. You will not receive any further Security Alerts.

Using a Certificate from the Local Machine Store

Certificates that are installed in the Local Machine Store can be accessed from the **Manual Selection (advanced)** menu option.

All Certificates in the Local Machine Store are listed and may be selected for use with ipMonitor.

Service Settings

The Service Settings window is used to assign a Windows account for the `ipmonitorsrv` service to run under.

When choosing an account, you must take into consideration the Credentials Manager, a key element of our security model. The `ipmonitorsrv` service is intended to run under an account with minimum permissions. The Credentials Manager impersonates accounts with elevated permissions when required to execute monitors, alerts, and features such as the:

- Drive Space monitor.
- File monitor.
- Server/Workstation control.
- Reboot Server action.

Note: For more information regarding credentials, see “Credentials” on page 217. For information regarding security, see “Security Model” on page 209.

The LocalSystem Account

The LocalSystem account is the default Windows account assigned to the "ipmonitorsrv" Service when the software is installed.

Although continuing to use the LocalSystem account is an option, it should be noted that the privilege level of the LocalSystem account on the local machine is greater than the privilege level required by the "ipmonitorsrv" service.

If you wish to adhere to a stricter security model, we suggest creating a Local User account specifically for the "ipmonitorsrv" service to run under, as discussed below.

If assigning either the LocalSystem account or a low privileged Local User account, you need to use the Credentials Manager for features that need to access Windows file system objects or services via the network.

Creating an Account for the "ipmonitorsrv" Service

Browse Button

The **Browse** button can be used to select an account from either the local computer account container or from the domain account container.

Startup Type

By default, the "ipmonitorsrv" service is set to the Automatic startup type. Under normal circumstances, this default should not be changed. The same options you can select from the Windows Services manager (Automatic, Manual, and Disabled) are available here.

The following table outlines the minimum permission requirements for any Windows Account assigned to the "ipmonitorsrv" service:

Folder Name	Permissions
\ipMonitor\	READ + WRITE + EXECUTE
\ipMonitor\config*	READ + WRITE
\ipMonitor\db*	READ + WRITE if storing Monitor Statistics
\ipMonitor\historic*	READ + WRITE if storing Monitor Statistics
\ipMonitor\internal*	READ ONLY
\ipMonitor\logs\	READ + WRITE
\ipMonitor\state	READ + WRITE
\ipMonitor\wwwroot*	READ ONLY

Do I Need to Use the Credentials Manager?

Although ipMonitor can function without using the Credentials Manager feature, we do not recommend it for security reasons.

If you choose not to use the functionality provided by the Credentials Manager, you likely need to assign a Domain Administrator class account to the "ipmonitorsrv" service. In the event of a security breach, however, this scenario potentially exposes all the resources the high privileged account has access to.

The Credentials Manager may also be used to impersonate non-Windows accounts. For example, an HTML/ASP monitor may need to authenticate to a web server challenging with the Digest Authentication scheme. As this example illustrates, it is difficult to leverage the full capabilities of ipMonitor without using the Credentials Manager.

Note: ipMonitor uses RSA 512/1024 bit encryption to internally store all sensitive parameters and data.

Chapter 3

Dashboard Views

The Dashboard and Dashboard View consolidate a variety of small reports (called web resources) into a summary page that shows status information for any device, group or monitor. Each monitor, device, and group has a dashboard view that you can customize with different resources to show as much or as little information as you want.

From here you can:

- change the layout of the web resources using drag-and-drop editing
- show the top devices by bandwidth use, ping time, cpu utilization, and other criteria

The dashboard for the **My Network** group is unique, and does not share its dashboard layout with any other group. All other groups, devices, and monitors share a common dashboard layout with other dashboards of the same kind.

Dashboard Layouts are Shared Between Object Types

ipMonitor displays dashboard information using four different dashboard layouts. Each type of layout is shared by all objects of that same type. For example, Monitor dashboards all use the same monitor dashboard layout, and so on

- **Monitors**. Used to display information about monitors.
- **Devices**. Used to display information about devices.
- **Groups**. Used to display information about groups, smartgroups, and subnets
- **My Network**. Used to display information about the entire network. This is the dashboard information you see when you click the Dashboard tab.

Changing the Layout of Dashboard Views

Dashboard templates are shared between types, so making a change to the layout of one dashboard type makes the same change to all dashboards of the same type. For example, adding a map to the dashboard of a group adds that same map to the dashboard of all groups.

To change the column layout:

1. Click **Change Columns**. The Change Columns dialog box appears.
2. ***If you want to insert a column***, click the **Add Column** button in the column to the left of the desired column position.
3. ***If you want to delete a column***, click the **Delete Column** button in the column you want to delete.
4. ***If you want to change the width of a column***, type a new value in the **Width** textbox of the column whose width you want to change. Width values are in pixels.
5. Click **OK**.

To add a new web resource to a layout:

- From the **Add Web Resource** menu, click the web resource you want to add.

To move web resources within the layout:

- Drag the title text (not the title bar) of any dashboard web resource to the desired location.

Web Resource Types

You can add many different types of web resources to a dashboard.

Web Resources for Group Dashboards and the My Network Dashboard

- **Map**. A specific map, or the default group map.
- **My Reports**. A list of report templates that apply to this group.
- **Getting Started**. A list of common tasks to help get you started.
- **Device Tree, by properties**. A hierarchal device list, organized by properties you choose.
- **Monitor Tree, by properties**. A hierarchal monitor list, organized by properties you choose.
- **Dependency States**. A list of all dependencies for the group and their status.
- **Devices with Down Monitors**. A list of all devices with monitors in a down state.
- **Group Contents**. A list of all explicitly defined group contents, sorted by status.
- **Monitor States**. A list of all monitors in the group, even those included inside other groups or monitors, sorted by status.

- **Summary Counts**. A numerical summary of the objects that belong to this group
- **Tag Details**. A list of all tags defined for this group.
- **Top XX Devices by Property** (availability, bandwidth use, battery, CPU use, disk use, humidity, memory, ping, response time, temperature). A list of the devices with the most marginal values for the selected property.

Web Resources for Device Dashboards

- **Map**. A specific map, or the default group map.
- **My Reports**. A list of report templates that apply to this group.
- **Dependency States**. A list of all dependencies for the device and their status.
- **Device Contents**. A list of the monitors that belong to the device, sorted by status.
- **Device Details**. A list of the device properties.
- **Monitor States**. A list of the monitors that belong to the device and their last test results, sorted by status.
- **Tag Details**. A list of all tags defined for this device.
- **CPU Utilization**. Gauges showing current CPU utilization for the device.
- **Disk Utilization**. Gauges showing current disk utilization for the device.
- **Memory Utilization**. Gauges showing current memory utilization for the device.

Web Resources for Monitor Dashboards

- **My Reports**. A list of report templates that apply to this monitor.
- **Monitor Details**. A list of the monitor properties.
- **Tag Details**. A list of all tags defined for this monitor.
- **Performance Chart**. Graphs that plot the last 23 hours of statistics for this monitor (availability, uptime, downtime, response time, battery capacity, SNMP value, SNMP delta value, free drive space, used drive space, free memory, used memory, CPU usage, traffic in, traffic out, download speed, humidity, temperature, file size, downloaded rows).
- **Performance Gauge**. Gauges showing current statistics for this monitor (availability, response time, used memory, used drive space, CPU usage, humidity, battery capacity, temperature, traffic in & out).

Chapter 4

Managing Devices

The Devices tab contains views that allow you to classify, organize, and see the status of the devices and monitors in your network.

- Details View. The Details View provides a tree view representation of your network hierarchy.
- Map View. The Map View provides a graphical representation of your network hierarchy.
- **Dashboard View**. The Dashboard View consolidates a variety of small reports into a summary page that shows status information for any device, group or monitor.
- NOC View. The Network Operations Center (NOC) view provides at-a-glance status reports for IT personnel and network operations groups who manage the network around the clock.

Details View

The Details View provides a tree view representation of your network. From here, you can:

- explore the status of devices and monitors
- organize your devices and monitors into groups, smartgroups, and subnets
- modify device and monitor properties and descriptions either individually or as a group
- add custom information tags
- disable or suspend monitors and devices

Add menu

- **Add New Group**. Add a new group to the tree.
- **Add New Smartgroup**. Add a new smartgroup to the tree.
- **Add New Subnet**. Define a new subnet within the Subnet group.
- **Add New Device**. Add a new, unscanned device to a group.
- **Add Existing Device**. Add a previously scanned device to a group.
- **Add New Monitor**. Add a new monitor to a device.

- **Add Scanned Monitors**. Add a previously scanned monitor to a device.
- **Add Existing monitors**. Add an existing monitor to a group.
- **Add Dependency**. Create a dependency in a device or group.
- **Add Alert**. Associate an alert with a group, device, or monitor.
- **Add column**. Add another column of data to the Details view.

Discovery menu

- **Scan Network**. Launch the Device Discovery Wizard to scan for new device.
- **Previous Scan Results**. Show the results of the last network scan so that you can add monitors that you chose to skip after the last scan.

Clone command

Make a copy of the selected object or objects.

Monitors can be cloned to quickly add new monitors to your network. After you clone a monitor, simply change only the parameters you need (such as the Monitor Name or IP address) to put the new monitor into service.

Cloned monitors are disabled by default, and have the [cloned] label applied to the Monitor Name.

If you need consistent custom tags in every monitor, cloning allows you to duplicate this information instantly. The importance of the tag remains the same upon cloning, so you can quickly discern which monitors have important information or require further tag configuration.

Move command

Move the object to another group. You cannot move monitors out of their parent group.

Edit menu

- **Properties**. Edit the properties of the selected object.
- **Tags**. Edit the tags of the selected object.
- **Mass Edit Monitor Properties**. Perform text substitutions and other large scale changes within the property fields of a group of objects.
- **Mass Edit Monitor Tags**. Perform text substitutions and other large scale changes within the tags of a group of objects.

Enable command

Resume testing previously disabled monitor selections.

Disable command

Stop testing the selected monitors.

Suspend menu

- **Suspend for xx minutes**. Temporarily pause testing of the selected monitors for the stated number of minutes. Ideal for periods of unscheduled network or server maintenance.
- **Suspend for xx hours**. Temporarily pause testing of the selected monitors for the stated number of hours.
- **Unsuspend immediately**. Resume testing of the selected monitors. You can reset the testing cycle for a monitor by suspending it, and then immediately unsuspending it. This can be used to promptly reapply new configuration parameters.

Delete menu

- **Delete**. Permanently delete the selected object or objects from your network. If the selected object is a group, you are asked in a subsequent dialog box whether you want to delete only the group, or delete the group and all its contents.
- **Remove from Group**. Removes the selected objects from the current group.

Creating Groups

ipMonitor supports the ability organize individual monitors and devices together under a group. A group does not contain the actual monitors and devices, but merely references them as members. In this way, monitors and devices can belong to several different groups.

You can create dependency relationships between critical resources and the entire group. This prevents multiple alerts from being sent when only a single alert can suffice.

To create a group:

1. Click the **Devices** tab.
2. Select a group in the tree where you want to create the new group.
3. From the **Add** menu, click **Add New Group**.
4. In the **Group Name** text box, type the name of the group, then click **OK**.

As with monitors, a good naming strategy can greatly improve working with groups. For example, you might choose names based on:

- Level of importance
- Purpose
- Location
- Responsibility
- Department

To add monitors and devices to a group:

1. Select the group.
2. From the **Add** menu, click **Add Existing Monitors** or **Add Existing Devices**.
3. Select the check boxes next to the monitors or devices you want to add, then click **Continue**.

You can add both monitors and devices to the same group.

Creating SmartGroups

SmartGroups are dynamic groups whose contents are determined by a filter that you create. 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.

To create a SmartGroup:

1. Click the **Devices** tab.
2. From the **Add** menu, select **Add New SmartGroup**.
3. Create the filter rules that define the SmartGroup, and then click **OK**.

Example of Creating a SmartGroup

In this example, we create a Smartgroup that contains all our devices manufactured by Cisco Systems.

1. Select the **My Network** group in the devices tree.
2. From the **Add** menu, select **Add New SmartGroup**. This takes us to the Edit SmartGroup page.

3. In the **Name** text 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 that can compare the Device Vendor property of each device.
   a. Click the arrow after "**devices, where**", and then select **Property** from the list.
   b. Click **Click here to Select a Property** to open the property menu.
   c. From the box at the bottom of the menu, select **Device Properties**.
   d. From the list, click the **Device Vendor** property, and then click the **Close** button to exit the menu.
7. Use the regex wizard to create a regular expression for the **Matches regular expression** text box that matches the case-sensitive string "Cisco".
   a. Click **RegEx Wizard** to open the Regex Wizard dialog box.
   b. In the **Match begins with** text box, type `Cisco`.
   c. Scroll to the bottom of the dialog box, and then copy the text `\iCisco.*?$` that has been created in the **Regular Expression you have built** text box.
   d. Click **Close** to return to the Edit SmartGroup page.
   e. Paste `\iCisco.*?$` into the **Matches regular expression** text box.
8. Click **Preview** to preview the contents of the new SmartGroup.
9. Click **OK** to create the SmartGroup.

Creating Subnets

A subnet is an IP address range within your network. In ipMonitor, adding a new subnet creates a group that contains references to devices within the subnet. ipMonitor creates these references automatically when you create the subnet. You do not manually add devices to a subnet.

To create a subnet:

1. Click the **Devices** tab.
2. Click the **Subnets** group in the tree.
3. From the **Add** menu select **Add New Subnet**.
4. Enter the name and IP address range of the subnet, and then click **OK**.

Map View

A map is a graphical representation of your network devices and monitors. Maps allow you to visualize the effects of a failing device or monitor.

ipMonitor creates default maps for each group and device in your network. These maps provide a graphical representation of your network. From the Map view, you can:

- change the layout and scale of a map
- add background images and change icons
- connect network items with lines that represent monitor status
- see more details about items on the map by clicking the items

To view a map of a device or group:

1. Click the **Devices** tab.
2. Select the group or device from the tree.
3. Click the **Map** button.

To resize the map:

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

To add a map to the main dashboard:

1. Click the **Dashboard** tab.
2. From the **Add Web Resource** menu, select **Map**. This adds a new, default map resource to the Dashboard.
3. From the **Edit** menu of the new map resource, click **Select Map**. The Select Map dialog box appears.
4. From the **Select map to display** list, click the specific device or group map that you want to display.
5. ***If you want to display the default map***, from the **Select map to display** list, click **Default Group for Dashboard**.
6. Click **Save**, and then confirm the change.
7. The new map replaces the default map in the dashboard.

Editing Maps

You can change the layout and scale of any map using the map editor.

Basic Map Editing Tasks

To edit a map:

1. Click the **Devices** tab.
2. In the Details view, click the device or group whose map you want to edit.
3. Click the **Map** button.
4. Click **Edit Map**.

To move map objects within the map:

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

To add a background to the map:

1. From the **Change Background** menu, click **Upload Background**.
2. Click **Browse**, and then select a **JPG**, **PNG**, or **GIF** format image file.
3. Click **Upload**.

To change the icon of a map object:

1. Click the object. A bounding box appears around it
2. Click the **Icons** list, and then select an icon category.
3. Click an icon.
4. The object changes to that icon.

To resize an object:

1. Click the object. A bounding box appears around it.
2. Drag any handle on the bounding box to resize.

To save the changes made to a map:

- Click **Save** to save the map.

Connecting Lines and Assigning Monitors

Between any two objects, we can create logical connections that represent the status of a monitor. For example, we can draw a line between two devices and assign a bandwidth monitor to that connection. If the monitor goes into a down state, it will be reflected in the map.

To create a connection between two objects.

1. From the **Drawing Tools** palette, click the line drawing tool.
2. Drag a line from one object to another.
3. A connection is created between the two objects.

To assign a monitor to a connection.

1. From the **Drawing Tools** palette, click the selection tool.
2. Click on an existing connection to select it.
3. Click **Assign Monitor**.
4. Select a monitor, and then click **OK**.
5. A monitor status indicator appears over the line.

Note: Within the Map Editor, the monitor status indicators are not active. To see the true status of the monitor, you must exit the Map Editor.

NOC View

The Network Operations Center (NOC) view provides at a glance status reports for IT personnel and network operations groups who manage the network around the clock.

The NOC View uses color codes to prioritize individual Monitors within a Group. When ipMonitor detects a problem, the resource color changes from green to amber, and may then progress to red and then to dark red as ipMonitor detects successive failures.

As this process occurs, the interface is reflowed to move the failing Monitor(s) to the top of the list. At a glance, you will know where to direct your troubleshooting efforts even before ipMonitor begins the Alerting process. With web browser sounds enabled, you can also be alerted audibly.

Chapter 5

Viewing Reports

Reports make it easy to view detailed monitoring data in both graphical and tabular formats.

This section describes these topics:

- My Reports
- Report Templates
- Quick Device and Group Reports
- System Status
- Scheduled Reporting Tasks

My Reports

My Reports are configurable reports that make it easy to view detailed monitoring data in both graphical and tabular formats. In addition to displaying Response Time, Uptime and Downtime for specified time periods, you can leverage historical data to view long-term and short-term performance trends, identify problems, and report operational efficiency for individual monitors and for monitor groups.

Extensive customization options make it possible to:

- Use the data sources available to display data averages for CPU, Memory, Battery, Temperature, Humidity, Hard Drive and Bandwidth Usage Monitors in graphical or tabular format.
- Arrange Monitor data for display in line graphs, vertical bar graphs, horizontal bar graphs, area graphs, or in tables.
- Display data spanning multiple time periods in one Report.
- Display statistics data for multiple Monitors in one Report, even if the Monitors do not belong to the same Group.
- Generate yearly, quarterly, monthly, weekly, daily or hourly Reports, as well as Reports for custom time periods.

To create a configurable Report using the Add Report Wizard

1. Click the **Reports** tab.
2. In the **My Reports** column, click **Add New Report**.

The Add Report Wizard is designed to help you create a Report with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to create new Reports quickly and efficiently.
- The Add Report Wizard allows you to test the selected customization options by previewing the appearance of the Report before saving it.

To edit a configurable report:

1. Click the **Reports** tab.
2. In the **My Reports** column, pause your mouse pointer over the configurable report.
3. Click the arrow that appears next to the configurable report to open the shortcut menu.
4. Select a command from the shortcut menu: **View Report**, **Edit Properties**, **Edit Tags**, **Clone**, or **Delete**.

Report Templates

After a Configurable Report has been created using the Add Report Wizard, the Edit Report page allows you to further customize the Report template to display data accumulated over a period of time in a wide variety of formats. The ability to create Reports based on reoccurring time selections makes Report Templates ideal for creating customized Service Level Agreement (SLA) Reports.

In addition to displaying Response Time, Uptime and Downtime for specified time periods, you can leverage historical data to view long-term and short-term performance trends, identify problems, and report operational efficiency for individual Monitors and Groups of Monitors.

Extensive customization options make it possible to:

- Use the data sources available to display data averages for CPU, Memory, Battery, Temperature, Humidity, Drive Space and Bandwidth Usage Monitors in graphical or tabular format.
- View data averages for CPU, Memory, Battery, Temperature, Humidity, Drive Space and Bandwidth Usage Monitors using resource icons, which provide a visual representation of the information.

- Arrange Monitor data for display in line graphs, horizontal bar graphs, vertical bar graphs, area graphs, or in tables.
- Display data spanning multiple time periods in one Report.
- Display statistics data for multiple Monitors from multiple Groups in a single Report.
- Generate yearly, quarterly, monthly, weekly, daily or hourly Reports, as well as Reports for custom time periods.
- Create numerous presentation-quality Report styles by fully controlling the design and layout of each Report.
- Add custom logos or other graphics, and use CSS and HTML code to further customize the appearance of each Report.
- Add custom headers and footers to each Report.
- Assign permission levels to determine which Administrator or User Accounts can view a particular Report.

To access report templates for a previously configured report

1. Log in to the ipMonitor web interface.
2. Click the **Report** tab, then click **Manage all reports**.
3. Click a previously configured Report to launch the Edit Report page.

Quick Device and Group Reports

Device Reports and Group Reports make it easy to view specific monitoring data for a group or a device.

To view a Device Report or Group Report:

1. Click the **Reports** tab.
2. Click a report type from the **Device Reports** or **Group Reports** column.
3. Select the group or device you want to view, and then click **Continue**.

Note: You will see a blank report if you select a report type that does not exist for your selection. For example, you will see a blank report if you try to view the CPU Utilization report for a device that does not have a CPU monitor.

You cannot edit the report parameters of a device or a group reports, but you can save an editable copy to your My Reports. After saving a quick report to My Reports, you can edit and tweak it as you would any other Customizable Report.

To save an editable version of a Quick Report

- When viewing a Quick Report, click **Save to My Reports**.

System Status

The **System Status** report allows you to view details about the server that ipMonitor is installed on, as well as the ipMonitor installation itself.

In the event that you need to contact ipMonitor technical support, details such as the ipMonitor version and build number, free hard disk space, physical memory available on the server and other relevant information found here can be particularly useful for troubleshooting purposes.

Monitoring Services Information

- **Version.** The ipMonitor Major Version and Build number.
- **Uptime.** The total running time of the ipMonitor 8 Service.
- **CPU Utilization.** The total processor time used by the ipMonitor Service since it was started.
- **License.**The number of Monitors available on the installation and the number of Monitors configured.
- **Support Policy.**The Support Policy ID associated with your installation.

Reporting Services Information

- **Version.** The ipMonitor Major Version and Build number.
- **Connected.** The current connection state of the ipMonitor Report Service.
- **Uptime.** The total running time of the ipMonitor Report Service.
- **CPU Utilization.** The total processor time used by the ipMonitor Report Service since it was started.
- **Last Report.** The date and time the last Report was generated by the ipMonitor Report Service.
- **Time Taken.** The length of time it took the ipMonitor Report Service to generate the Report.
- **Records Seen.** The number of data records gathered during the process of creating the last Report.

System Information

- **OS.** The current Operating System and Service Pack level.
- **OS Version.** The numeric operating system version and build number.
- **Processor Type.** A description of the ipMonitor server processor.

- **Processor Speed.** The processor speed, in MHz or GHz.
- **Processors Active.** The number of processors detected on the ipMonitor server.
- **MDAC.** The version number of Microsoft Data Access Components currently installed on the system.

System Vitals

- **Physical Memory**. The amount of Physical Memory on the ipMonitor server, shown in megabytes (MB) and/or gigabytes (GB). Gray bars indicate available memory, while green bars indicate allocated physical memory on the server. When available memory reaches 10% or less, the color of the available memory area changes from green to red.
- **Commit Charge Memory.** The amount of Virtual Memory on the ipMonitor server, shown in megabytes (MB) and/or gigabytes (GB). Gray bars indicate available memory, while green bars indicate allocated physical memory on the server. When available memory reaches 10% or less, the color of the available memory area changes from green to red.
- **Drive x.** The amount of Drive Space on the hard drive / partitions located on the ipMonitor server, shown in megabytes (MB) and/or gigabytes (GB). The gray area indicates available drive space, while the green area indicates allocated drive space. If the remaining available drive space is dangerously low, the color of the used Drive Space area changes from green to red.

Scheduled Reporting Tasks

Scheduled Reporting Tasks allow you to:

- Email your Configurable Reports and Quick Reports to a predefined list of recipients at scheduled intervals.
- Save your Configurable Reports and Quick Reports to disk.

In addition to displaying Response Time, Uptime and Downtime for specified time periods, you can leverage historical data to view long-term and short-term performance trends, identify problems, and report operational efficiency for individual Monitors and Groups of Monitors.

Report Publisher features include:

- The ability to email Reports on a daily or weekly basis.
- The ability to email Reports to multiple recipients.
- Control over the format of the images included in the Report.
- Full control over the file name of the Report saved to disk.

- The ability to specify the directory where the Report will be saved.

Email Report Publishers

Email Report Publishers make it easy to schedule your Reports to be emailed to a list of recipients at regular intervals.

To configure an Email Report Publisher:

1. Log in to the ipMonitor web interface.
2. Click the **Configuration** tab, and then click **Scheduled Reporting Tasks**.
3. Click the **Add Email Report Publisher** button.

Disk Report Publishers

Disk Report Publishers allow you to save your reports to the location of your choice.

To configure a Disk Report Publisher:

1. Log in to the ipMonitor web interface.
2. Click the **Configuration** tab, and then click **Scheduled Reporting Tasks**.
3. Click the **Add Disk Report Publisher** button.

Chapter 6

Configuration

The configuration page provides access to all the items and settings in ipMonitor that can be configured. This includes alerts, user accounts, credentials, and scheduled reports. It also contains tools to help you administrate your network.

Settings

If you want to…	Then select…
Change user access permissions	Account List
Create a schedule for generating reports	Scheduled Reporting Tasks
Create or modify alerts	Alert List
Create or modify ipMonitor accounts and passwords	Account List
Disable monitors during scheduled maintenance	Scheduled Maintenance Tasks
Import and export XML ipMonitor data	System Settings
Log ipMonitor activity	System Settings
Manage credentials	Credential List
Manage the settings of the ipMonitor server	System Settings
Manage the settings of your account	My Settings

Tools

If you want to…	Then select…
Add a new device to ipMonitor	Add New Device
Browse the MIB database	SNMP Tree
Share notes with other ipMonitor users	Notes
Create regular expressions	Regex Wizard
Monitor the status of an SNMP object	SNMP Monitor Wizard
Reboot a windows server or workstation	Server/Workstation Control
Search for an entry in the MIB database	SNMP Search
Stop or restart a remote windows service	Server/Workstation Control
Update ipMonitor to the latest version	Updates
View all the devices discovered by ipMonitor	Scan Results
View the log files	Log Files
View who is currently logged into ipMonitor	Sessions

Updates

The Updates command allows you to query the ipMonitor update service regarding the latest Upgrades, Updates and Fixes available under the Service Plan.

Click the Scan for Updates button to begin the query process.

Protocol

Choose between the HTTPS / SOAP and HTTP / SOAP protocols. Outbound HTTP or HTTPS access is required to check for updates.

Site

The update service engine connects to ipmsupport.solarwinds.com. This location does not require authentication.

Force communication through a Proxy Server

Select this option if your organization connects to the Internet through a proxy server.

Any new updates that have been released but not applied to the current ipMonitor will be listed when you click **Continue**. Information includes:

- Importance level.
- Date of release.
- Build Number.
- List of fixes and enhancements.
- Link to download the Upgrade, Update or Fix.

Before you select this option, ensure that you have correctly set up the **Client HTTP Settings** to permit communications with your proxy server. You can access the Server Settings from the **Configuration** tab.

Note: This feature does not run automatically; it can only be initiated by clicking the **Scan for Updates** button.

Sessions

The Sessions tab allows you to view Administrators and Users currently logged in to your ipMonitor installation.

Last Access

The last time the Administrator or User accessed the installation.

Session Age

The length of time that has passed since the Administrator or User logged in.

Guest?

This column indicates whether the account is a Guest Account.

Notes

The Notes feature is ideal for IT departments that have a team of people accessing and using the Administration interface at various times.

Notes can be used to post messages for other ipMonitor Administrators and Users, such as: configuration settings, policy information, problem resolution, tips and tricks, and so on.

Using Notes to Share Information

If you plan to use Notes to share information with your team, each Administrator and User Account should:

1. On the **Configuration** page, click **My Settings**.
2. From the **Start Page** list, select **Notes**.

The Notes page will then be the first page Administrators and Users see after logging in. Like a message board, new messages will be located at the top of the page.

Deleting Messages

To delete a message, check the box adjacent to the message, and then click the **Delete** button.

To delete all messages, check the box adjacent to the **Delete** button, and then click **Delete**.

Note: Administrators can delete any message that is posted. Users are only able to delete messages that they post. Check boxes are only displayed for messages posted by that User.

Adding Messages

To add a new message, click the **Add Note** button.

Adding Format Styles to Messages

Messages can be posted in plain text, or Tags can be used to format text. Formatting requires an opening tag and a closing tag. For example, to write **Bold Text**, you would type: [B]Bold Text[/B].

Tags can be inserted using the various format options shown below. Alternatively, you can type opening and closing tags directly into the message.

Tag	Function
[B] [/B]	Insert bold font.
[I] [/I]	Insert Italic font.
[U] [/U]	Underline font.
[S] [/S]	Strike through a word or a line of text.
[CENTER] [/CENTER]	Center text or an image.
[CODE] [/CENTER]	Set a fixed width font.
[URL] [/URL]	Insert an active URL link.
[FONT] [/FONT]	Set the size, style and color of your preferred font.
[EMAIL] [/EMAIL]	Insert an active email address link.
[IMAGE] [/IMAGE]	Insert an image into your message. Type the URL to the location of the image within the tags.

Click the **Preview** button to view the way your message will appear after it has been properly formatted.

Note: Administrators have full control over whether Users can view and / or post messages. The Security / Accounts menu is used to configure Notes Permissions for User Accounts.

thwack Resource

ipMonitor thwack tab

- Provides quick access to the most recent thwack community forum posts and file uploads for ipMonitor. Search for ipMonitor related content directly from the web interface.

Chapter 7

Relations

The Relations page offers a top-down look at the way the essential elements of your network interrelate with one another, making it easy to spot associations.

Understanding the relationships between your monitors, groups, and dependencies is a key factor in properly configuring an ipMonitor installation. Likewise, the relationship between monitors, alerts, and actions is critical to ensuring the right people are notified when a problem is detected. Without these components working together, actions may not be triggered, or they may not reach the intended destination.

Using the Relations pop-up page, you can display any of the following individual configuration components and their associations:

- Monitors
- Groups
- Alerts
- Actions
- Configurable Reports
- Report Publishers
- Maintenance Schedules
- Credentials

Accessing the Relations Pop-Up Window

The Relations pop-up window is accessible from the Edit page of any individual configuration element listed above.

For example, you may wish to view all ipMonitor configuration components associated with a particular Monitor using the following procedure:

1. Click the Monitors menu option.
2. Click on the name of the desired Monitor to enter Edit mode.
3. From the submenu bar, click the Relations icon.

Navigating the Relations Pop-Up Window

- **Links.** Each configuration element listed in the Relations pop-up window is linked to its own Relations page. For example, the Relations pop-up window for a particular Monitor may display Groups, Dependencies, Alerts, Actions, Configurable Reports and Report Publishers. Clicking on the name of any of these individual elements will automatically direct you to the Relations page corresponding to that component.
- **Previous Relations.** The Previous Relations drop-down selector allows you to return to the Relations page of any individual configuration element already accessed. A maximum of ten previously accessed configuration elements are retained for selection, allowing you to quickly navigate to a particular Relations page at any time.
- **Edit.** To make configuration changes to the settings of any individual component displayed in the Relations pop-up window, click the Edit button adjacent to the desired element to access it in Edit mode.

  For example, you may choose to change the time intervals associated with an enabled Alert related to a specific Monitor. To do so, you can simply click the Edit button, make the required changes, and then click OK. After the configuration changes are complete, you can click the Relations button located on the submenu bar to open the Relations pop-up window for the alert, and then display any other features that will be affected by the timing change.

Relationship Types

Individual ipMonitor features can be associated with other essential configuration elements. The types of relations displayed in the Relations pop-up window depend on the feature being edited.

Monitors

A Monitor is a background process that continuously tests a target resource on timed intervals. ipMonitor includes a comprehensive suite of Monitors that are used to watch system resources, applications, infrastructure equipment, servers and essential services around-the-clock.

Monitor Relations can include:

- Any Dependency Monitor that affects whether or not Alerts will be triggered for this Monitor when a problem is detected.
- Any Group that contains the Monitor as a Member.
- Any Group that contains the Monitor as a Dependency.
- Any Alert to which the Monitor belongs.

- Any Action that is part of an Alert to which the Monitor belongs.
- Any Maintenance Schedule that regulates scheduled downtime for the Monitor.
- Any Configurable Report customized to include statistics data gathered by the Monitor.
- Any Report Publisher containing a Configurable Report customized to include statistics data for the monitor.
- Any Credential assigned to the Monitor.

Groups

ipMonitor supports the ability to group together multiple individual Monitors for the purposes of assigning them Dependencies. Properly configured Groups and Dependencies act as an Alert suppression system in ipMonitor. When a critical resource fails, ipMonitor limits Alerts to the Monitors defined as a Dependency rather than triggering Alerts for every member Monitor in the Group.

Group Relations can include:

- Any Monitor designated as a Dependency of the Group.
- Any Monitor designated as a Member of the Group.
- Any Alert to which the Group belongs.
- Any Action that is part of an Alert to which the Group belongs.
- Any Maintenance Schedule that regulates scheduled downtime for the Group.
- Any Configurable Report customized to include statistics data gathered by the Group.
- Any Report Publisher containing a Configurable Report customized to include statistics data for the group.

Alerts

An Alert is a collection of actions. Each alert can act on behalf of a set of Monitors. Alerts determine what Monitors specific Administrators and departments watch, as well as when and how they are alerted.

Alert Relations can include:

- Any Monitor assigned to the Alert.
- Any Group assigned to the Alert.
- Any Actions belonging to the Alert.

Actions

The comprehensive suite of Actions provide various notification methods, integration options, and recovery actions.

Alert Relations can include:

- Any Monitor associated with the Alert to which the Action belongs.
- Any Group associated with the Alert to which the Action belongs.
- Any Credential assigned to the Alert.
- The Alert to which the Action belongs.

Configurable Reports

Configurable Reports make it easy to view detailed monitoring data in both graphical and tabular formats. In addition to displaying Response Time, Uptime and Downtime for specified time periods, the ability to leverage historical data allows you to view long-term and short-term performance trends, identify problems and report operational efficiency for individual Monitors and Groups of Monitors.

Configurable Report Relations can include:

- Any Monitor included in the Configurable Report.
- Any Group included in the Configurable Report.
- Any Report Publisher that contains the Configurable Report.

Report Publishers

Report Publishers allow you to save Configurable Reports to disk or email them to a predefined list of recipients at scheduled intervals.

Report Publishers can include:

Any Configurable Report included in the Report Publisher.

Maintenance Schedules

Maintenance Schedules allow Administrators to temporarily disable monitoring of certain resources, for example to perform data back-ups or Service restart actions.

Maintenance Schedule Relations can include:

- Any Monitor affected by the Maintenance Schedule.
- Any Group affected by the Maintenance Schedule.
- Any Credential assigned to the Maintenance Schedule.

Credentials

In order for ipMonitor to be fully functional, various Monitors, Alerts and management features require access to Windows file system objects or Services via the network. Instead of running the ipMonitor Service under an Administrator account at all times, Credentials are used to apply elevated permissions only when required.

Credential Relations can include:

- Any Monitor that uses the Credential for monitoring purposes.
- Any Recovery Action that uses the Credential for recovery purposes.
- Any Alert that uses the Credential for alerting purposes.
- Any Maintenance Schedule that uses the Credential to perform routine actions.
- The Manual Backup action to which this Credential is assigned.
- The Recurring Internal Maintenance Backup action to which this Credential is assigned.

Chapter 8

Monitors

ipMonitor includes a comprehensive suite of Monitors that are used to watch system resources, applications, infrastructure equipment, servers and essential services around-the-clock:

- Quality Assurance Monitors perform result analysis testing for critical applications such as SQL servers, commerce solutions and dynamic web applications.
- SNMP polling and Trap Monitors provide industry standard methods for monitoring devices such as routers, switches and load balancers.
- Windows NT/2000/XP/2003/2008 Monitors test key aspects of Windows operating systems.
- Resource Monitors test finite system resources and alert before consumption becomes critical.
- Uptime Monitors test availability of popular TCP/IP protocol based application-layer protocols such as HTTP, HTTPS, SNMP, and so on.

DNS Names Require Lookup Time

As a general rule, conservative use of DNS names is recommended for TCP/IP based Monitors. Service level responsiveness can be timed more accurately by removing the DNS lookup from the equation. Monitor response must be completed within a specified number of seconds. This includes the time taken to perform a DNS lookup.

Some exceptions apply for Monitors that require access to the Windows files system, and HTTP-based Monitors. These are noted in the Help pages for individual Monitors.

If your network uses a DHCP (Dynamic Host Configuration Protocol) server to dynamically assign IP addresses, type an IP address only if it is "reserved", otherwise type a Domain Name. If a Monitor is configured to use an IP address, and that IP address was to be dynamically assigned to another resource, the Monitor would no longer be able to successfully monitor the target resource.

If you assign a DNS Name to a Monitor, timing parameters may be affected by the additional time required to perform the DNS lookup. Although the default timing parameters for testing should allow for the time it takes to perform the DNS lookup, timing is a variable you need to consider when aggressive testing times are used.

Dependencies

In cases where many monitored resources depend on one or more critical resources to function, Groups can be created and assigned Monitor Dependencies. This effectively prevents redundant Alerts from triggering for each Member Monitor in the Group when only a single Alert for a Dependency Monitor would suffice.

Maintenance Schedules

Maintenance Schedules allow you to temporarily suspend monitoring for individual Monitors or Groups of Monitors during planned maintenance periods.

Mass Edits

When ipMonitor installations range into hundreds or thousands of Monitors, manually changing common configuration settings can be time consuming. The Mass Edit feature makes it easy to quickly apply large-scale changes to configuration fields across any number of Monitors using a rule-based system.

How It Works: Monitors

A Monitor is a background process that continuously tests a target resource on timed intervals. Testing methods depend on the capabilities of the Monitor, and the Test Parameters you specify during Monitor configuration.

Flexible timing parameters provide the ability to intensify or lessen testing during each of the four operational states of a monitor. Each time a Monitor test fails, the sequential failure count is incremented and checked against the configured Number of failures allowed before Alerting takes place. A successful test at any point resets the sequential failure count to zero.

When a Monitor reaches its maximum number of test failures, it will trigger an Alert causing the following series of events to take place:

1. Each alert is scanned to see if the monitor belongs to it.
2. If so, action parameters and action schedules are checked for actions within the alert.
3. Any active actions are carried out.

Monitor States

Monitors have five operational states, as well as a disabled state.

Icon	Monitor State	Description
Green	Up and Listening	The device is responding as expected or ipMonitor is listening for inbound SNMP Traps.
Amber	Warn	Indicates an unexpected result. Testing is in progress, but no alerts have been triggered.
Light Red	Down	Alerts are being sent. A Monitor will progress from a Fail state to a Lost state when the maximum number of Alerts has been processed.
Dark Red	Lost	The monitored resource continues to be in an error state. All configured alerts have been sent.
Light Gray	Suspended or in Maintenance	The Monitor is disabled or in Maintenance mode.
Dark Gray	Uninitialized	The monitor has not yet been initialized. No testing has occurred.

You can view the State of a Monitor using any of the following options:

- Access **Live Reports** within the Admin Dashboard. Monitors are sorted and color-coded based on their State.
- Access the **Monitors List** within the Configuration interface by clicking the Monitors menu option. The Monitor State is displayed under the Status heading.
- Access the **Edit Monitor** page by clicking on the **Monitor Name** from the **Monitors List**. The Monitor Status is displayed at the top of the page.

Scanning the Network

ipMonitor includes a Device Discovery Wizard that seeks out devices on uyour network and recommends resources to monitor.

Potential Monitors that can be added are based on the types of resources detected. Although recommended Monitors can be summarily added to an installation, further customizations can also be made by using the Add Device Wizard directly from within the Device Discovery feature.

To start the Device Discovery Wizard:

1. Click the **Devices** tab.
2. From the **Discovery** menu, click **Scan Network**.

The Device Discovery Wizard makes it easy to:

- Quickly add all recommended Monitors to your installation.
- Pick and choose individual Monitors to add to your installation.
- Add entire Groups of Monitors to your installation.

Features include:

- Control over the discovery methods ipMonitor uses to perform the Network Scan.
- Control over the range of IP addresses that will be scanned.
- The ability to add non-standard ports to the list of ports that ipMonitor will probe.
- The ability to navigate through the list of returned items using the tree-like structure of the Add Device Wizard that provides a visual representation of the device.
- The ability to use cached scan results to add Monitors and Groups to your installation over a period of time.
- The ability to exclude servers, workstations and devices from the list of resources that will be scanned when the Network Scan Wizard recommends Monitors to add to your installation.

Device Discovery Wizard

- **IP Range**. Scans IP address ranges for devices
- **Network Neighborhood**. Scans the Active Directory for devices.
- **DNS Zone**. Initiates a DNS zone transfer from a DNS server and scans the list for devices.
- **Host File Import**. Scans a list of IP addresses for devices.

Monitors List

The Monitors List displays every Monitor configured for your ipMonitor installation is displayed in this one list no matter what other groups individual Monitors have been assigned to.

Depending on your licensing tier, the Monitors List can range from 500 to 5000 Monitors, making it difficult to locate individual Monitors with any degree of efficiency.

To help you manage the large number of Monitors with relative ease, the Monitors List comes equipped with broad search capabilities and various management features:

- Sort the lists by name, status, or type
- Filter the list by name, address, tag, ID, type, or status..

The Monitors List shows all configured Monitors by Name, State and Type.

Controlling List Size

Use the Items per page drop down menu to control the number of Monitors displayed per page. The default is 25 monitors per page.

Filtering the List

Use the **Filter Text** drop down menu to apply a Filter to the Monitors list.

General Monitor Settings

All Monitor types available in ipMonitor have the following configuration options in common:

- Monitor Submenu
- Monitor Status
- Identification
- Timing
- Notification Control
- Recovery Parameters

These common options are discussed in this single location to avoid repeating the same information throughout each Monitor Type document.

The Test Parameters and Analysis of Test Results sections are detailed on a per-Monitor basis throughout the documentation available in the Monitor Types section.

Note: Monitors can be disabled during scheduled maintenance periods. This ability is controlled by the Maintenance Schedules.

In ipMonitor installations with hundreds or thousands of Monitors, manually changing common configuration settings can be time consuming. The Mass Edit feature makes it easy to quickly apply large-scale changes to configuration fields across any number of Monitors using a rule-based system.

Monitor Submenu

The Monitor Submenu located at the top of each Edit Monitor page makes it easy to perform maintenance actions, configure a Downtime Simulator, view a Report, access the Relations page, or pop up a new window to display the configuration settings of the monitor in XML format.

Cancel / Back

Return to the Monitors List.

Disable

Instruct ipMonitor to stop testing the target resource indefinitely. A confirmation prompt will be displayed before Monitors are disabled.

Delete

Permanently remove a Monitor from the ipMonitor system. A confirmation prompt will be displayed before Monitors are deleted.

Suspend

Temporarily pause testing. This ability is ideal for periods of unscheduled network or server maintenance. Type an integer value to suspend monitors for "x" number of minutes or hours. Fractional values are not allowed.

Force Test

Reset the testing cycle for a Monitor. This option allows you to promptly reapply new configuration parameters.

Clone

Duplicate the current Monitor. After a Monitor is cloned, simply change only the parameters you need, such as the Monitor Name or IP address, to put the new Monitor into service.

Cloned Monitors appear in the Monitors List. They are disabled by default and have the "[cloned]" label applied to the Monitor Name.

Downtime Simulator

Perform pre-rollout testing for a Monitor. The Downtime Simulator demonstrates the Alerting process for a Monitor by illustrating Alert coverage at a specific time of day, for any day of the week.

View Report

Access Quick Reports for an individual Monitor. Quick Reports are ideal for troubleshooting problems as they happen and for identifying short-term and long-term performance trends at a glance.

Relations

Display the associations to other ipMonitor components, such as Groups, Alerts, Actions, Maintenance Schedules, Configurable Reports, Report Publishers and Credentials.

Popup XML

Display the current configuration settings for the monitor in an XML format within a new browser window. The XML template can be saved as a .txt file.

Monitor Status

The Monitor Status section shows the current operational state of the Monitor. The data displayed is based on the Status settings configured in the NOC View section of the Real Time Status Reports.

Status

The result of the last test performed by the Monitor. Different Monitor types generate specific Test Results and Error Codes in accordance with the technical capabilities for the Monitor. Please refer to the specific Monitor section for a detailed explanation of the Test Results and Error Codes reported.

Availability

The percentage of time the Monitor has been available. This calculation is based on Coverage time.

Coverage

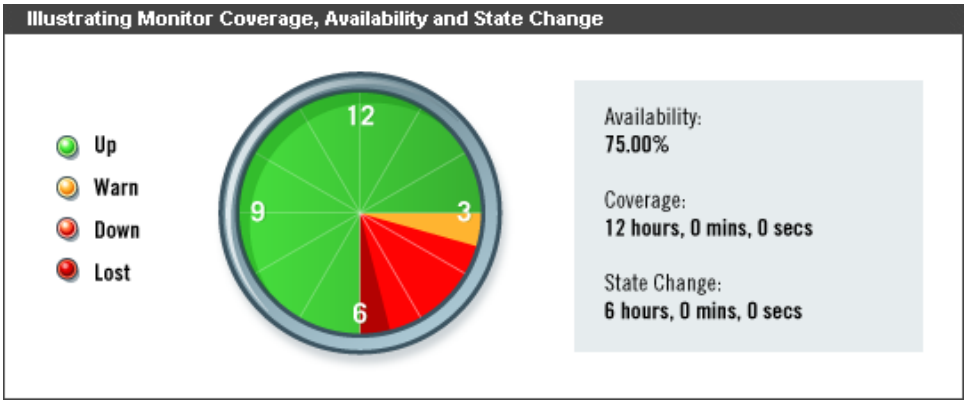
The total length of time ipMonitor has been monitoring the resource. Coverage specifically excludes any period while the Monitor is suspended, disabled, or in maintenance mode. This value is reset when ipMonitor is restarted.

State Change

The length of time since the Monitor changed operational states. This includes time elapsed since scheduled maintenance.

Example of Availability, Coverage, and State Change

The following diagram illustrates how ipMonitor calculates Availability, Coverage, and State Change.



Assuming that it is now 12:00 PM and the Monitor was first enabled at 12:00 AM, the above diagram tells us that:

- The Monitor has been enabled for 12 hours. During that time, it was not suspended or placed in maintenance. This total is recorded in the Coverage column.
- During the time the Monitor was enabled, it was in a Warn state for approximately 35 minutes, Down for approximately 2 hours and Lost for approximately 25 minutes. When totaled, these periods amount to 25% (3 hours) of the entire Coverage time recorded (12 hours). The Availability column, then, shows that the Monitor was available for 75% of the time.
- The Monitor recovered at 6:00 o'clock, exactly 6 hours ago. Since that was the last time ipMonitor recorded any change in the monitor status, this length of time is appropriately recorded in the State Change column.

Note: You can choose which Monitor details to display by accessing the **NOC View** page from the **Real-Time Status Reports** interface. Click the top bar of the NOC View page to bring up the configuration menu, and select the desired data to display. Refresh the Edit Monitor page to view the newly selected status details.

Downtime Simulator

The Downtime Simulator is used to perform pre-rollout testing for a Monitor. The Downtime Simulator:

- Demonstrates the alerting process for a monitor
- Illustrates the alert coverage of a monitor at a specific time of the day, for any day of the week

The Downtime Simulator runs a synthetic failure by:

1. Applying the configuration parameters of the monitor.

2. Scanning each alert to find any associations with the monitor.
3. Checking Range parameters and Schedules for actions within the alert.
4. Carrying out any active actions.

Configuring the Downtime Simulator

Enter Edit mode for the specific Monitor you want to test, then click the **Downtime Simulator** button located on the submenu bar.

Downtime Duration

Enter the number of downtime minutes to simulate. Be sure to allow enough time for the Monitor simulation to progress through to its Lost state (dark red).

Downtime Start Time

Enter the day and start time to test Alert coverage for the Monitor.

Average Test Duration

Enter the time to allot for each test in the simulation. This is shown in the Time column.

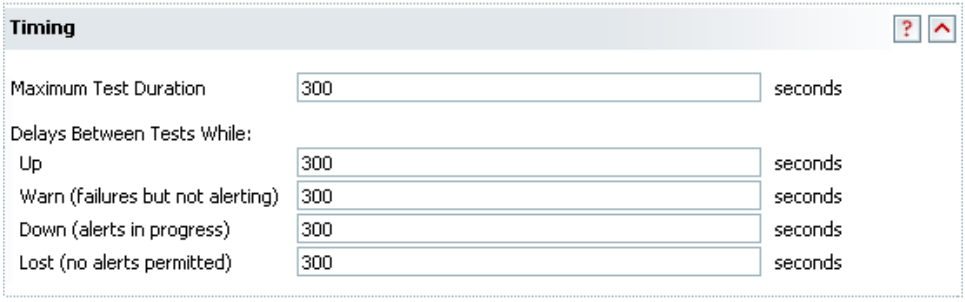
If you make any changes to the Simulation Settings, click the Update button to refresh the Simulation Results.

How it Works: Downtime Simulator

The Downtime Simulator is easy to understand if you know how the **Timing** and **Notification Control** parameters are used to control the failure and alerting process for each monitor.

You may want to review the Alerting Process topic, which displays a sample test failure count and the action taken based on elapsed time.

The Downtime Simulator example that follows uses these Monitor Timing and Notification Control parameters:



Notification Control

Accumulated Failures per Alert	3
Maximum Alerts to Send	3

Time	State
Sat, 09:00:00	Testing ... FAILED
Sat, 09:00:10	Waiting 5 mins, 0.00 secs ...
Sat, 09:05:10	Testing ... FAILED
Sat, 09:05:20	Waiting 5 mins, 0.00 secs ...
Sat, 09:10:20	Testing ... FAILED
Sat, 09:10:30	Notification #1 (Alerts Sent, 2 more Notifications may be used)

Alert Name	Queued?	Enabled?	Availability OK?	Range OK?
Restart IIS	**NO**	**YES**	**YES**	**NO**
XYZ Admin Email Alert	YES	YES	YES	YES

Sat, 09:10:30	Waiting 5 mins, 0.00 secs ...
Sat, 09:15:30	Testing ... FAILED
Sat, 09:15:40	Waiting 5 mins, 0.00 secs ...
Sat, 09:20:40	Testing ... FAILED
Sat, 09:20:50	Waiting 5 mins, 0.00 secs ...
Sat, 09:25:50	Testing ... FAILED
Sat, 09:26:00	Notification #2 (Alerts Sent, 1 more Notifications may be used)

Alert Name	Queued?	Enabled?	Availability OK?	Range OK?
Restart IIS	YES	YES	YES	YES
XYZ Admin Email Alert	YES	YES	YES	YES

Sat, 09:26:00	Waiting 5 mins, 0.00 secs ...
Sat, 09:31:00	Testing ... FAILED
Sat, 09:31:10	Waiting 5 mins, 0.00 secs ...
Sat, 09:36:10	Testing ... FAILED
Sat, 09:36:20	Waiting 5 mins, 0.00 secs ...
Sat, 09:41:20	Testing ... FAILED
Sat, 09:41:30	Notification #3 (Alerts Sent, 0 more Notifications may be used)

Alert Name	Queued?	Enabled?	Availability OK?	Range OK?
Restart IIS	**NO**	**YES**	**YES**	**NO**
XYZ Admin Email Alert	YES	YES	YES	YES

Sat, 09:41:30	Waiting 5 mins, 0.00 secs ...
Sat, 09:46:30	Testing ... FAILED
Sat, 09:46:40	Waiting 5 mins, 0.00 secs ...
Sat, 09:51:40	Testing ... PASSED
Sat, 09:51:50	Notification (Recovery)

Alert Name	Queued?	Enabled?	Availability OK?	Range OK?
Restart IIS	**NO**	**NO**	**YES**	**YES**
XYZ Admin Email Alert	YES	YES	YES	YES

Sat, 09:51:50	Waiting 5 mins, 0.00 secs ...

The following table explains the Alerting process. Three failed tests must accumulate before each Alert is sent. The **Maximum Alerts to Send** value is set to 3.

FAILURE	TIME	COLOR	STATE	ACTION
1st	Sat 09:00:00	YELLOW	WARN	
2nd	Sat 09:05:10	YELLOW	WARN	
3rd	Sat 09:10:20	RED	DOWN	**FIRST ALERT SENT**
4th	Sat 09:15:30	RED	DOWN	
5th	Sat 09:20:40	RED	DOWN	
6th	Sat 09:25:50	RED	DOWN	**SECOND ALERT SENT**
7th	Sat 09:31:00	RED	DOWN	
8th	Sat 09:36:10	RED	DOWN	
9th	Sat 09:41:20	RED	DOWN	**THIRD ALERT SENT**
10th	Sat 09:46:30	DARK RED	LOST	**NO MORE ALERTS WILL BE SENT**

Looking at the Time values in the table, you will notice that the interval between each test is a combination of the **Delay Between Tests While: UP** value of the monitor and the **Average Test Duration** value of the simulator. In this example, it is ten seconds.

To completely understand the **Time** column of the Downtime Simulator, you must look at the **Timing** parameters for the monitor. In this example, we have used the default setting of 300 seconds for each Monitor State, but the time of each test increments by 310 seconds (5m10s). This is easily explained by the following arithmetic::

- 10 second **Average Test Duration**
  -plus-
- 300 second **Delay Between Tests**

The **Average Test Duration** is used to override the **Maximum Test Duration** timing parameter.

Please note that in a real world scenario, the numbers in the **Time** column would be much more variable and subsequently more difficult to understand. Variables such as the monitor type, network topology, network load, hardware, carrier, and latencies all affect the time it takes to perform tests Some tests may return values in a few hundred milliseconds, while others may not return values for several seconds.

What the Downtime Simulator Reports

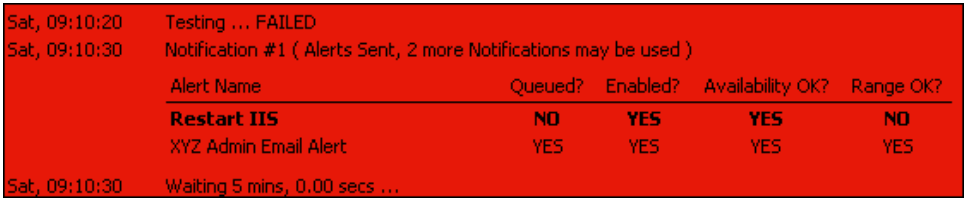
The primary purpose of the Downtime Simulator is to test Alert coverage for a Monitor at a specific time of day during any day of the week. It does this by processing every Action that can be triggered by the Monitor across all Alerts. The following text columns help pinpoint problems:

- **Queued?**. Indicates whether an Action will be attempted or triggered.
- **Enabled?**.Indicates whether the Action has the appropriate **Send Failure Notifications** or **Enable Recovery Action** message "checked on".
- **Availability OK?**. Indicates whether the alert schedule permits the action to be triggered during the Day and Time period selected for the Downtime Simulator.
- **Range OK?**.Indicates whether the Alert Range setting corresponds to or includes the Alert count number sent by the failing Monitor. Configurable Alert Ranges allow you to receive all or only some Alerts when a problem occurs.

Simulator Example of an IIS Restart

Background for this example:

- We are monitoring an IIS web server using an HTTP Monitor
- An Email Action notifies the web administrator
- A Restart Service Action automatically restarts the IIS Service

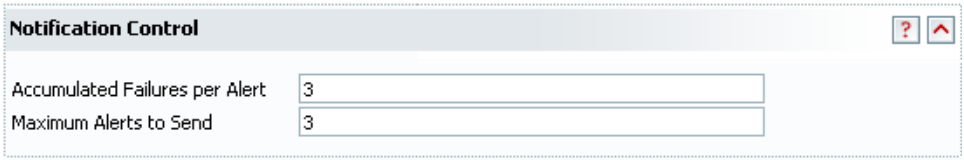


Alert Ranges can be used to escalate an action to another administrator or to automatically take corrective action when a problem is not resolved quickly enough. In this example:

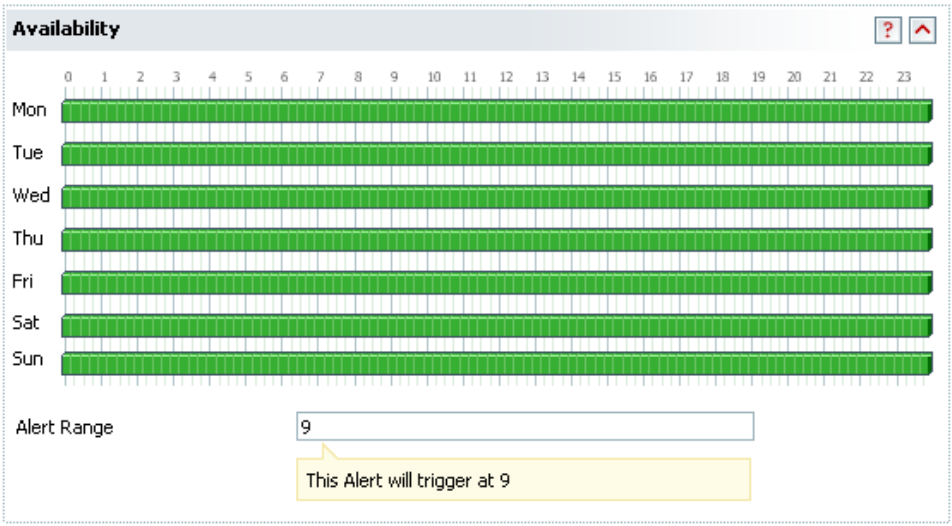
- ipMonitor sends an email to notify the web administrator of the problem
- If the administrator does not respond quickly enough, the IIS Service is automatically restarted
- With **Send Recovery Notifications** enabled for the email Action, the administrator will receive an email indicating if the web server has recovered.

Bold text indicates that there is a problem with the action. Looking at each of the three Failure Notifications sent by the Monitor in this simulation, you can see that the Restart IIS action is displayed in bold.. The Action has the **Enable Recovery Action** box checked, and is scheduled for Availability at this time. The Action is not **Queued**, however, due to the fact that its **Alert Range** value is out of bounds.

The Monitor states the **Maximum Alerts to Send** is 3.



The problem lies in the **Alert Range** for the Restart IIS Alert. It is set to 9.



In order for the proper Alert escalation to take place, the Monitor's **Maximum Alerts to Send** would also have to be set to 9.

Downtime Simulator Tips

- If you specify a **Downtime Duration** for the Downtime Simulator that is too long, you will see more than one and possibly many dark red Lost tests. If you specify a duration that is too short, you will not see any Lost tests, and the Warn and Down states may also be truncated.

The Up (green) state shown at the bottom of the Downtime Simulation shows Alert information when the monitored resource recovers.

The Downtime Simulator configuration parameters can be saved for your account upon logging out. Simply hold down the Shift key and click either **Logout this session** or **Logout all sessions**.

Mass Edit: Monitor Properties

When ipMonitor installations range into hundreds or thousands of Monitors, manually changing common configuration settings can be time consuming. The Mass Edit feature makes it easy to quickly apply large-scale changes to configuration fields across any number of Monitors using a rule-based system.

The Mass Edit feature for Monitor Properties supports:

- Filtering the Monitor List to isolate and edit only specific Monitors.
- Setting any configuration field to a specific value.
- Replacing text in a configuration field.
- Replacing numerical values in a configuration field.
- Using Regular Expressions pattern matching to search and replace.
- Appending numerical or textual strings to any existing value.
- Previewing changes before committing to them.
- Cancelling unwanted changes before they can affect your installation.

Using the Mass Edit feature, you can:

- Add a prefix string, such as an IP address or machine name, to Monitor Names.
- Change the timing parameters of all Monitors, or only of Monitors in a filtered subset.
- Quickly update the configuration settings of Monitors created using the Network Scan.
- Enable or disable Monitor statistics.

Accessing the Mass Edit Feature for Monitor Properties

To access the Mass Edit feature for Monitor Properties:

1. Log in to the ipMonitor web interface.
2. Click the **Devices** tab.
3. Select two or more monitor check boxes.
4. From the **Edit** menu, select **Monitor Properties**.

Mass Edit: Tags

When ipMonitor installations range into hundreds or thousands of Monitors, manually changing Custom Tags attached to each Monitor can be time consuming. The Mass Edit feature makes it easy to quickly apply large-scale changes to Custom Tags across any number of Monitors using a rule-based system.

The Mass Edit feature for Monitor Tags supports:

- Filtering the Monitor List to isolate and edit only Tags attached to specific Monitors.
- Renaming Tags.
- Using Regular Expressions pattern matching to search and replace Tag content values.
- Appending numerical or textual strings to any existing Tag content value.
- Previewing changes before committing to them.
- Cancelling unwanted changes before they can affect your installation.

Accessing the Mass Edit Feature for Monitor Tags

To access the Mass Edit feature for Monitor Tags:

1. Log in to the ipMonitor web interface.
2. Click the **Devices** tab.
3. Select two or more monitor check boxes.
4. From the **Edit** menu, select **Monitor Tags**.

Chapter 9

Group Dependencies

ipMonitor supports the ability to group together multiple individual Monitors for the purposes of assigning them Dependencies. Properly configured Groups and Dependencies act as an Alert suppression system in ipMonitor. When a critical resource fails, ipMonitor limits Alerts to the Monitor defined as a Dependency rather than triggering Alerts for every member Monitor in the Group.

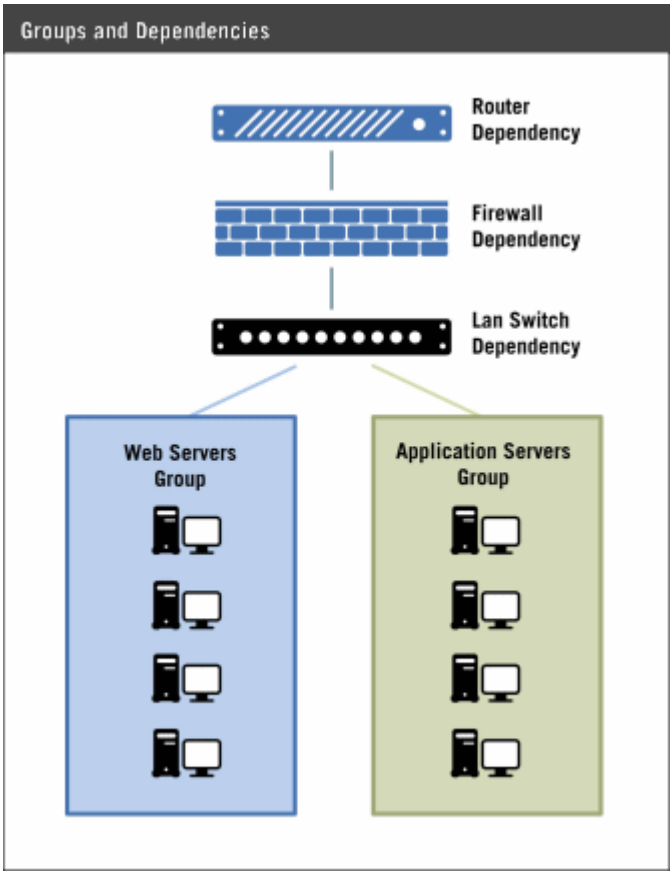
- Group **Members** are Monitors that make up the Group.
- Group **Dependencies** are Monitors that must remain available for all Members to function correctly.

Dependencies define the relationship between critical resources and those resources that depend on them for all or part of their functionality. A router, switch, server computer or stable path to another network would all be valid Dependencies.

Defining Dependency relationships:

- Minimizes the number of redundant Alerts.
- Helps isolate the root cause of the problem.
- Prevents configured Recovery Alerts from attempting to restart services and applications if such an action is not required.

As an example, consider a web solution that is made up of various individual components. It would be practical to Group them together and assign certain Dependencies to the Group.



A logical Dependency would be the network switch. If the switch were to become unavailable or fail, all of the Member Monitors for both Groups would be affected and many Alerts would be generated.

By defining the switch Monitor as a Dependency, only the switch failure would trigger an Alert. This helps greatly in isolating the root-cause of the problem, prevents you from being inundated with a large number of unnecessary Alerts, and ensures that Recovery Alerts are not triggered for services and applications that do not need to be restarted.

Dependency Monitors must reach the Down state for ipMonitor to disable alerting for Group Members. If the Dependency Monitor is Up, the ability of individual Group Members to trigger Alerts remains unaffected. For example, Alerts will be processed if hard disk space runs low, an SNMP trap is received, the SQL server produces an unexpected query result, and so on.

Note: After a Dependency Monitor reaches the Down state, Members that are currently in an Up or Warn state will not reach Down or Lost. When all Dependencies return to an Up state from a Down state, all alerting functionality is restored.

Groups

Monitors can be assigned to Multiple Groups

For example, a PING Monitor that traverses a network switch could be assigned as a Dependency to many Groups that depend on the availability of the switch.

How Monitor State applies to Groups

A Group will inherit the most critical state of any Monitors, including Dependency Monitors, it has been assigned. For example:

- If the State of a single Monitor within a Group changes to Warn, the state of the entire Group becomes Warn.
- If the state of that Monitor progresses to Down, the state of the entire Group becomes Down.

The All Managed Devices Group

The **All Managed Devices** group is a system group that serves as the parent object and container for all ipMonitor devices.

- All newly created devices are automatically added to the **All Managed Devices** group.
- The **All Managed Devices** group cannot be deleted, nor can ipMonitor be configured to operate without it.
- The **All Managed Devices** group is required for ease of management, and acts as the parent for all network devices.

ipMonitor Installations with More Than 50 Monitors

Typically, the **All Managed Devices** group is never assigned to an alert. It is the master list and only used to add members to the groups you create. These are then assigned to alerts.

ipMonitor Installations with Less Than 50 Monitors

The **All Managed Devices** group may be the only group you require. Dependencies can be applied to this group and an alert in order to prevent unnecessary actions and help pinpoint problems quickly.

The Orphaned Objects Group

The **Orphaned Objects** group is a system group that serves as temporary container for monitors and groups that do not have valid parent objects. Monitor and groups can become orphans when they are imported into ipMonitor with missing or invalid XML data.

To assign an orphaned monitor to an existing device:

1. Select the orphaned monitor.
2. Click **Move**.
3. Select a device from the **Destination Device** list and then click **Continue**.
4. The monitor is moved and assigned to the destination device.

To assign an orphaned group to an existing group:

1. Select the orphaned group.
2. Click **Move**.
3. Select a group from the **Destination Group** list and then click **Continue**.
4. The group is moved and assigned to the destination group.

Chapter 10

Monitor Types

ipMonitor contains many different types of monitors. We list them here in alphabetical order:

Active Directory	IRC
Bandwidth Usage	Kerberos 5
Battery	LDAP
CPU Usage	Link – User Experience
DNS User Experience	Lotus Notes
DNS TCP	MAPI – User Experience
DNS UDP	Memory Usage
Directory	Network Speed
Drive Space	NNTP
Event Log	NTP
Exchange Round-Trip Email Wizard	Ping
Exchange Server 2000/2003/2007	POP3
External Process	POP3 – User Experience
Fan	RADIUS
File Property	RWHOIS
File Watching	Service
Finger	SMTP
FTP	SNMP
FTP User Experience	SNMP – User Experience
Gopher	SNMP Trap – User Experience
HTML/ASP	SNPP
HTTP	SQL: ADO
HTTP User Experience	SQL: ADO – User Experience
HTTPS	SQL Server
Humidity	TELNET
IMAP4	Temperature
IMAP4 – User Experience	WHOIS
ipMonitor	Windows

Active Directory

Active Directory is the directory Service offered in Windows 2000, Windows 2003 and Windows Vista. It is used to provide a centralized location to store information about networked devices, Services and users, as well as a means to securely add, modify, delete, and locate data in the directory store.

Microsoft's Active Directory resolves domain object names to object records through Lightweight Directory Access Protocol (LDAP) search or modify requests.

The Active Directory Monitor:

1. Establishes a connection to the Active Directory service
2. Sends a Bind Request indicating that it is making a LDAP v2 request
3. Sends a Search Request asking which LDAP versions the Active Directory Service supports
4. Sends an Unbind Request for the Active Directory server to close the TCP connection

Use the Active Directory Monitor to test that:

- An Active Directory client can open a connection with an Active Directory server
- The server adheres to the Active Directory protocol by responding with the correct codes
- The server responds within a required number of seconds
- **Note**: The Active Directory Monitor supports LDAP version 2, which is the most commonly supported version.

Bandwidth Usage

The Bandwidth Usage Monitor uses RPC or SNMP communication to measure the amount of inbound and outbound traffic traveling through a network interface on:

- The local machine
- A remote computer running Microsoft Windows NT, 2000, XP or 2003
- An SNMP-enabled device

It effectively ensures that:

- The bandwidth rate is tested over time in order to distinguish between a steady increase in network usage and a sudden data spike.
- Heavy bandwidth utilization is detected before performance can be affected.
- Administrators are alerted if bandwidth usage exceeds a specified threshold.
- The amount of traffic a resource uses on the network can be determined.

The Bandwidth Usage Monitor Wizard is designed to help you configure a Bandwidth Usage Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Bandwidth Usage Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Test Results

When the Monitor is in an Up state, test results are reported as shown in the example below:

- **in**. This value indicates the inbound data received by the server, displayed in Kilobytes (KB).
- **out**. This value indicates the outbound data sent by the server, displayed in Kilobytes (KB).
- **KB/s**. This value indicates the current amount of bandwidth consumption, displayed in KB/s (1024 bytes per second).
- **KB/s-avg**. This value indicates the average amount of bandwidth consumption, displayed in KB/s (1024 bytes per second). This calculation is based on the tests performed during the length of time specified in the Sample Size field.

- **kb/s**. This value indicates the current amount of bandwidth consumption, displayed in kb/s (1000 bits per second).
- **kb/s-avg**. This value indicates the average amount of bandwidth consumption, displayed in kb/s (1000 bits per second). This calculation is based on the tests performed during the length of time specified in the Sample Size field.

When the Monitor is in a Warn, Down, or Lost state, the Last Result field indicates the problem encountered.

Battery

The Battery Monitor uses SNMP communication to test the remaining charge in a UPS battery. The Monitor's ability to retrieve and analyze data allows an Administrator to:

- Be notified when a power outage occurs.
- Stay aware of the remaining charge in the battery.
- Obtain an accurate picture of battery health and current operational conditions.

In order to extend the running time of necessary servers or components, critical decisions can be made using this information.

Test Results

When the Monitor is in an Up state, test results are reported as shown in the example below:

- **capacity**. This value indicates the current capacity of the UPS battery being monitored, shown as a percentage.

When the Monitor is in a Warn, Down, or Lost state, the Last Result field indicates the problem encountered.

CPU Usage

The CPU Usage Monitor uses Local or SNMP communication to test the amount of processor capacity available on:

- The local machine
- A remote computer running Microsoft Windows NT, 2000, XP or 2003
- A remote computer running a Unix-Based Operating System such as Linux, Solaris, HP-UX, and so on.
- An SNMP-enabled device

It effectively ensures that:

- Heavy, sustained CPU utilization is quickly detected before performance can be affected.
- Administrators are alerted if the CPU utilization exceeds the specified threshold.

Test Results

When the Monitor is in an Up state, test results are reported as shown in the example below:

- **usage**. This value indicates the CPU load currently on the system, represented as a percentage (%).
- **usage-avg**. This value indicates the average CPU load on the system, represented as a percentage (%). It is based on the tests performed during the length of time specified in the Sample Size field.

DNS User Experience

The DNS User Experience Monitor tests the ability of a Primary and the Secondary DNS server to respond to a record query, as well as its level of responsiveness.

This monitor uses the Universal Datagram Protocol(UDP), which is the primary method of communication with DNS servers. The monitor alternately queries both the Primary and the Secondary DNS server for a Domain Name until one of the DNS servers responds, or the "Maximum Test Duration" time expires.

The results of the Domain Name resolutions are compared against a list of expected IP addresses. Results are verified in one of two ways:

- The result set must include all of the IP addresses in the "expected" list
- The result set must have at least one of the IP addresses in the "expected" list

The monitor considers the test to have failed:

- If the above noted tests fail
  -or-
- If both DNS Servers fail to respond within the "Maximum Test Duration"

The monitor tests:

- That at least one DNS server is "up and running"
- That the Primary DNS server, Secondary DNS server or both are able to respond to a Domain Name Query, perform a lookup and resolve a hostname
- That the results of the resolved Domain Name correctly corresponds to the IP address you expect
- That the complete round trip time until the response is received is within a specific number of seconds

DNS TCP

The DNS TCP Monitor tests a DNS Server's ability to respond to a record query, as well as its level of responsiveness.

This monitor uses the Transmission Control Protocol (TCP), which is the secondary method of communication for DNS Servers. As TCP establishes a connection, guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent, it is considered less efficient for the purpose of DNS. TCP is typically used only when the response data size exceeds 512 bytes, or for such tasks as zone-transfer request in DNS over TCP (AXFR).

The monitor measures round trip time by sending a query for thea root server A Record, `a.root-servers.net`, to the specified DNS Server and then waiting for a response.

The Monitor test will pass if the Monitor receives a valid positive or negative response within the required timeout period.

The DNS TCP Monitor tests that the:

- DNS Server is "up and running"
- DNS Server is able to process and respond to a query
- Response makes a complete round trip within a specific number of seconds

DNS UDP

The DNS UDP Monitor tests a DNS Server's ability to respond to a record query, as well as its level of responsiveness.

The DNS UDP Monitor uses the Universal Datagram Protocol, which is the primary method of communication with DNS Servers.

ipMonitor measures round trip time by sending a query for the root server A record, `a.root-servers.net`, to the specified DNS Server and then waiting for a response.

The Monitor test will pass if the Monitor receives a valid positive or negative response within the required timeout period.

The DNS UDP Monitor tests that the:

- DNS Server is "up and running"
- DNS Server is able to process and respond to a query
- Response makes a complete round trip within a specific number of seconds

Directory

The Directory Monitor detects modifications to a directory's basic structure and alerts you when changes outside of specified bounds are detected. The Monitor tests various properties of a given directory, making it ideal for:

- Verifying the existence of a directory.
- Determining whether files have been added to or removed from a directory.
- Determining whether the size of a directory has changed.
- Monitoring subdirectories for modifications to their overall size or file count.

The Directory Monitor tests the structure and content of a directory at regular intervals to detect any changes outside the boundaries you define. When a change is encountered, the Monitor can trigger:

- A Failure Notification Alert.
- An Information Alert.
- Both a Failure Notification Alert and an Information Alert.

Configuring Information Alerts is an optional process. Separating Information Alerts from Monitoring actions and Failure Notifications allows you to instruct the Monitor to send an Information Alert but remain in an Up state even if a change is detected. This gives you maximum flexibility to configure each Directory Monitor to meet your specific needs for every directory being tested.

This Monitor is particularly useful for tasks such as:

- Monitoring allotted storage space in a user directory.
- Detecting whether critical files have been removed from a directory.
- Ensuring required backups are always completed.
- Monitoring files that could potentially grow large enough to impact disk space.
- Monitoring directories containing files that are likely to grow and multiply at a rapid rate.

Drive Space

The Drive Space Monitor uses RPC or SNMP communication to test the amount of available drive space on a specified drive, share or mount. If less available space than specified is detected, a failure state occurs.

Using the RPC communication method, the Drive Space Monitor can monitor any host machine running:

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003

Using the SNMP communication method, the Drive Space Monitor can monitor any SNMP-enabled host machine running:

- Windows NT/2000/XP/2003
- UNIX and UNIX-like Operating Systems such as Linux, Solaris, HP-UX, and so on

Common uses of the Drive Space Monitor are:

- Ensuring critical resources do not run out of drive space.
- Automatically taking Recovery actions to free up drive space.

Note1: For Windows NT, comparison is made in relation to the drive size that hosts the UNC share. For Windows 2000, comparison is made in relation to the drive size that hosts the UNC share unless a disk space quota has been set for the share. In this case, comparison is made relative to the size of the quota.

Note2: The Drive Space Monitor Wizard allows you to configure Drive Space Monitors quickly and easily. However, if you prefer greater control over the process, you can Clone an existing Drive Space Monitor and make any required configuration changes manually.

Test Results

- **space**. The current available space on the share being monitored. Available space is reported in gigabytes (gb) and megabytes (mb).
- **avail**. The current available space on the share being monitored, reported as a percentage (%) of the entire drive.

Event Log

The Event Log Monitor can be used to locate information within Error, Warning, Information, Success Audit and Failure Audit events that are recorded in the Windows event logs.

For any Server or Workstation version of Windows:

- Application log
- Security log
- System log

Additional logs for computers running as a Domain Controller:

- Directory service log
- File Replication service log

Additional logs for computers running as a Domain Name System Server:

- DNS server log

The Event Log Monitor uses header information to locate specific events, however, the Description is often the most useful piece of information, as it indicates what occurred or the significance of the event.

As the format and contents of the event description vary depending on the event type, the Event Log Monitor requires a Regular Expression to filter specific details from the description field. This can be a simple RegEx that captures the entire contents of the description field, or a more sophisticated RegEx to filter only specific parameters.

The events table only shows ipMonitor events relating to the status of the monitor. It does not display the events captured by the Windows Event Log monitor.
If you need to see a history of the events captured by the Windows Event Log monitor, you can create a Text Log action to record the Information Messages that the monitor generates.
To add a Text Log action to an alert:

1. Click the **Configuration** tab, and then click **Alert List**.
2. Click an alert.
3. Click **Text Log** from the **Add Action**menu.
4. Type Text Log Action in the **Action Name**field.

5. Type the file name and directory for the log file in the **File Name** and **Directory** fields. For example:
   eventlog.txt
   C:\
6. Check **Send Information Messages**
7. Click **OK**.

Note 1: Tests on Event Log Monitors Differ from other Monitors

When creating a new Event Log Monitor, note that the Monitor starts searching forward from the time of creation; it does not search historical content already in the Event log file.

When configuring Monitors, suspending and then unsuspending a Monitor is often used to force an immediate test. This will not work with the Event Log Monitor as its pointer will be reset to its current time or, essentially, the end of the log file. A real Event will need to occur for the Monitor to send an Information Alert.

The Preview test, however, does search the Event Log's existing content, making it ideal for configuration and troubleshooting purposes.

Note 2: Recommended Default Timing Interval

We recommend using the default timing intervals of 300 seconds between scans. This is because the Event Log Monitor queries the Event Log via the WMI Service, and this Service may consume a considerable amount of resources on the target machine. 300 seconds between scans allows for a balance between the length of time it takes to query the Event Log and the load placed on the target machine's CPU.

IMPORTANT! Setting the timing intervals to a value lower than 180 seconds can cause problems related to security and authentication, particularly in scenarios where multiple Event Log Monitors target a single machine using a Credential impersonating a Domain Account.

Exchange Round-Trip Email Wizard

The Exchange Round-Trip Email Wizard is designed to help you configure an IMAP4, POP3, or MAPI User Experience Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Exchange Round-Trip Email Wizard allows you to test all the parameters you enter along the way to make sure that the new Monitor will work as expected immediately upon being enabled to go live in a production environment.

IMPORTANT! Before creating a MAPI User Experience Monitor using the Exchange Round-Trip Email Wizard, please note that the monitor requires:

- Access to the messaging subsystem of Microsoft Outlook.
  Note: A full version of Microsoft Outlook that supports the MAPI protocol must be installed on the ipMonitor server for this purpose. However, the Microsoft Outlook application itself does not need to be running in order for the Monitor to function correctly.
- A Microsoft Outlook Email Account to exist under the default Mail Profile of the Windows User Account impersonated by the Monitor.

Exchange Server 2000/2003

The Exchange Server 2000/2003 Monitor opens a connection to the specified Exchange server and tests the performance of its subsystems to determine the server's general health. The overall performance of the server is typically dictated by its weakest performing subsystem.

The Monitor's ability to retrieve and analyze data allows an Administrator to:

- Use preconfigured performance counters made available by the Windows Management Instrumentation service to test multiple Exchange Sever subsystems at once.
- Quickly identify any performance degradation in critical Exchange Server components.
- Determine the exact point of failure.
- Take corrective action before email outages occur.
- **Note**: There is a separate monitor type for Exchange Server 2007.

Exchange Server 2007

The Exchange Server 2007 Monitor opens a connection to the specified Microsoft® Exchange 2007 server and tests the performance of its subsystems to determine the server's overall health.

The Monitor's ability to retrieve and analyze data allows an Administrator to:

- Use preconfigured performance counters made available by the Windows Management Instrumentation service to test multiple Exchange Sever subsystems at once.
- Quickly identify any performance degradation in critical Exchange Server components.
- Determine the exact point of failure.
- Take corrective action before email outages occur.

Available performance counters:

Aggregate Delivery Queue Length (All Queues)

Aggregate Delivery Queue Length (All Queues) is the number of items queued for delivery in all queues..

Active Non-SMTP Delivery

Active Non-SMTP Delivery Queue Length is the number of items in the active Non-SMTP queues.

Active Mailbox Delivery

Active Mailbox Delivery Queue Length is the number of items in the active mailbox queues.

Active Remote Delivery Queue Length

Active Remote Delivery Queue Length is the number of items in the active remote delivery queues.

Messages Queued for Submission

The Messages Queued for Submission performance counter indicates the number of messages in the mailbox store that are ready to be sent and are waiting to be submitted to a transport server.

Poison Queue

The Poison Queue Length performance counter measures the number of messages currently in the poison queue. Messages in the poison message queue are in a permanently suspended state.

Replication Receive Queue Size

The Replication Receive Queue Size performance counter indicates the number of public folder replication messages waiting to be processed.

The larger the replication queue becomes, the more out of synchronization the content in the folders becomes. When replication queues grow, there is an increased load on resources as the messages in the replication queue are processed. Also, growing replication queues indicate that public folder content on the server is outdated.

Retry Remote Delivery

The **Retry Remote Delivery Queue Length** performance counter measures the number of messages currently in the retry remote delivery queue. Messages in this queue are in a retry state because there an issue prevented their delivery. If the issue is transient, a subsequent reattempt to send the message may be successful.

Messages that cannot be successfully delivered are subject to various retry, resubmit, and expiration deadlines based on the message's source and destination. The message is said to "time-out", or expire, after all delivery efforts have failed during a specified period of time. After a message expires, the sender is notified of the delivery failure. Then the message is deleted from the queue.

Submission Queue Length

The Submission Queue Length performance counter measures the number of messages currently in the submission queue. Messages in this queue are in a retry state because an issue prevented their submission to the categorizer. If the issue is transient, a subsequent attempt to submit the message may be successful.

Unreachable Queue Length

The Unreachable Queue Length performance counter measures the number of messages currently in the retry mailbox delivery queue. Messages in this queue are in a retry state because an issue prevented their delivery. If the issue is transient, a subsequent attempt to send the message may be successful.

WMI Requirements

In order for the Exchange Server Monitor to be able to properly monitor an Exchange Server, Windows Management Instrumentation (WMI) must be enabled and functioning properly. In addition, the remote server must be accessible through an RPC connection in order to run the WMI queries.

Counters are tested in the order that they appear. In the event of multiple counter failures, only the first counter error encountered will be reported.

The Exchange Server Monitor's built-in internal sampling helps combat counter spikes. The Monitor will issue the WMI query five times, once every second, and then calculate an average based on the query results.

Troubleshooting WMI

1. As remote WMI connections use RPC, the RPC Service must be enabled and started on the remote system
   a. Logon to the remote system.
   b. Open the Windows Services list on that system.
   c. Ensure that the "Remote Procedure Call (RPC)" service is enabled and started.
2. As WMI also uses DCOM to communicate with the remote system, it must be enabled and configured correctly on the remote system.

a. Log on to the target server with an administrator account.

b. Navigate to Start > Control Panel > Administrative Tools > Component Services. You need to switch to the Classic View of the Control Panel to use this navigation path.

c. Expand Component Services > Computers.

d. Right-click **My Computer**, and then select **Properties**.

e. Select the **COM Security** tab, and then click **Edit Limits** in the Access Permissions grouping.

f. Ensure the user account you want to use to Monitor resources over WMI has Local Access and Remote Access, and then click **OK**.

g. Click **Edit Default**, and then ensure the user account you want to use to Monitor resources over WMI has Local Access and Remote Access.

h. Click **OK**.

i. Click Edit Limits in the Launch and Activation Permissions grouping.

j. Ensure the user account you want to use to Monitor resources over WMI has Local Launch, Remote Launch, Local Activation, and Remote Activation, and then click **OK**.

k. Click **Edit Default**, and then ensure the user account you want to use to Monitor resources over WMI has Local Launch, Remote Launch, Local Activation, and Remote Activation.

l. Click **OK**.

3. Verify WMI Security to ensure that the account used by the ipMonitor Credential can access the CIMV2 namespace.

a. Log on to the computer you want to monitor with an administrator account.

b. Navigate to **Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Services and Applications**. You need to switch to the Classic View of the Control Panel to use this navigation path.

c. Click **WMI Control**, and then right-click and select **Properties**.

d. Select the **Security tab**, and then expand **Root** and click **CIMV2**.

e. Click **Security** and then select the user account used to access this computer and ensure you grant the following permissions:

- -Enable **Account**
- -Remote **Enable**

f. Click **Advanced**, and then select the user account used to access this computer.

g. Click **Edit**, select This namespace and subnamespaces in the Apply to field, and then click **OK**.

h. Click **OK** on the Advanced Security Settings for CIMV2 window.

i. Click **OK** on the Security for Root\CIMV2 window.

j. Click Services in the left navigation pane of Computer Management.

k. Select Windows Management Instrumentation in the Services result pane, and then click Restart.

4. If you are monitoring a target in a workgroup, you need to disable remote User Account Control (UAC). This is not recommended, but it is necessary when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

Warning: The following procedure requires the modification or creation of a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Consider backing up your registry before making these changes.

a. Log on to the computer you want to monitor with an administrator account.

b. Click **Start > Accessories > Command Prompt.**

c. Enter `regedit`.

d. Expand the following registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\`

e. Locate or create a DWORD entry named *LocalAccountTokenFilterPolicy* and provide a DWORD value of 1.

Note: To re-enable remote UAC, change this value to 0.

5. If the target computer has Windows Firewall enabled, it must have a Remote WMI exception to allow remote WMI traffic through (http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx).

a. Click **Start**, click **Run**, type *cmd* and then press **ENTER**.

b. Type *netsh* firewall set service *RemoteAdmin* enable at the command prompt, and then press **ENTER**.

c. Type *exit* at the command prompt, and then press **ENTER**.

External Process

The External Process Monitor launches an external program or script. It can also launch a script via an executable program, such as:

- PuTTY Link `plink.exe`
- Windows `cscript.exe`

Any required command line parameters can be passed to the third party executable on startup.

The External Process Monitor is very versatile and typically used by administrators to:

- Simplify routine or repetitive tasks.
- Create custom Monitors to work with ipMonitor.

The External Process Monitor supports two modes of operation:

- **Process Return Value.** The third party executable reports an "exit" code to the ipMonitor process in the form of a numeric value.
- **Environment Variable**. The third party executable sets the value of an "environment variable" to be read by the Monitor.

When configured using **Process Return Value** mode, the test passes if:

- The program finishes executing within the **Maximum Test Duration** timeout interval.
- The "exit" code returned matches the **Expected Return Value**.

When configured using **Environment Variable** mode, the test passes if:

- The program finishes executing within the **Maximum Test Duration** timeout interval.
- The Monitor was able to read the **Environment Variable** in question and determined its value is correct.

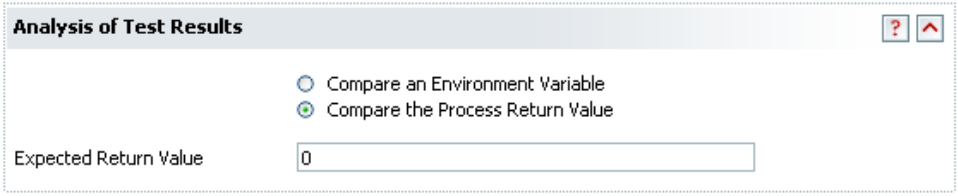
Analysis of Test Results

The External Process Monitor supports two modes of operation:

- Analyze a Process Return Value
- Analyze an Environment Variable

Process Return Value

The third party executable reports an "exit" code to the ipMonitor process in the form of a numeric value.



When the third party executable or script is created, it must be designed to produce an exit code when it shuts down.

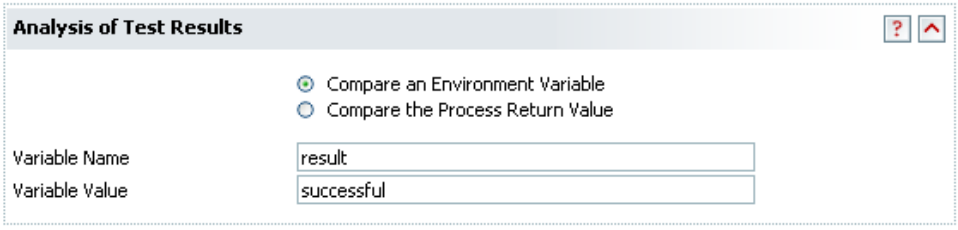
Although exit codes can be any number you choose in your program design, "0" is a standard Success exit code used when an executable returns the expected value.

In our example, if the target log file did not exist we would return "1" to the ipMonitor process on exit. This result would not match the Expected Return Value, therefore causing the External Process Monitor test to fail.

Alternatively, if a "0" was returned, the result would be a match and the External Process Monitor would continue in an Up state.

Environment Variable

The third party executable sets the value of an Environment Variable, which is subsequently read by the External Process Monitor.



Environment Variables allow for greater flexibility in the information that can be passed, especially when the content must contain file paths, or special characters such as less than or greater than symbols.

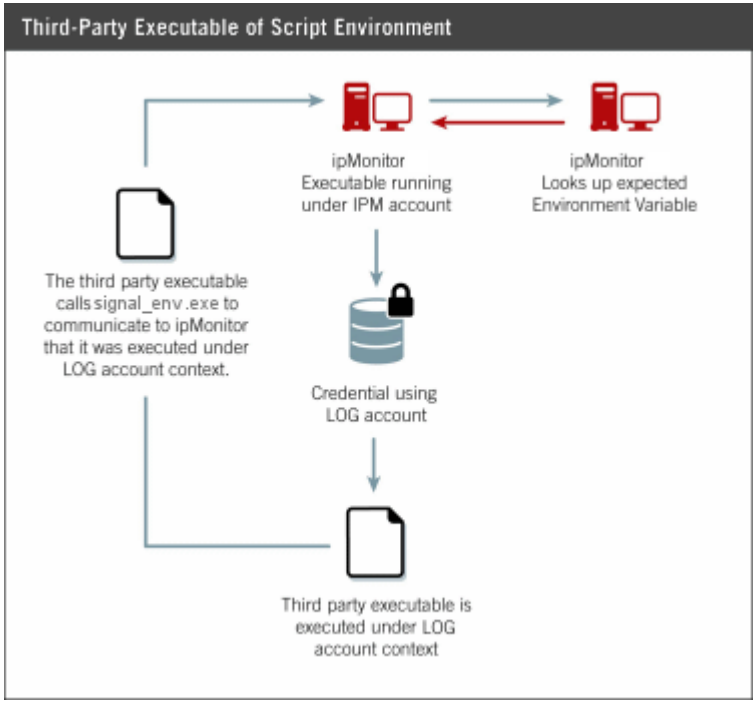
After setting the value of the Environment Variable, the third party executable or script must call `signal_env.exe` in order for the variable to be available to the ipMonitor process.

The signal_env.exe tool is located in the root folder of the ipMonitor installation. These steps describe how `signal_env.exe` works:

1. The application or script being monitored is run.
2. During execution, the application sets the necessary Environment Variable and then calls `signal_env.exe`.
3. The External Process Monitor reads the Environment Variable and performs a comparison based on the Monitor configuration.

In this example, ipMonitor expects "`result`" to equal "`successful`" for the test to pass. Any other text string will cause the test to fail.

The following diagram shows the third party executable or script environment:



The diagram illustrates that:

- The ipMonitor executable is running under the IPM account.
- A Credential named LOG was created to impersonate an account with the necessary permissions.
- ipMonitor impersonates the LOG Account to run the third party program.
- When the third party executable runs, it calls signal_env.exe to communicate back to ipMonitor that it was run under the LOG account context.
- ipMonitor retrieves the LOG environment variables for comparison.

In the Windows NT, 2000, XP, 2003 and Vista Operating Systems, Environment Variables are grouped internally into four categories:

- **SYSTEM Variables** define the behavior of the global operating system environment. These apply to all users of the machine and are recorded in the Registry at: HKLM\System\CurrentControlSet\Control\Session Manager\Environment.
- **PROCESS Variables** define the environment in which a process runs. These apply to the current process, and may be passed on to child processed. PROCESS variables are not stored in the Registry.
- **USER Variables** are only available when the user is logged on to the machine. Local variables set in the HKEY_CURRENT_USER hive are valid only for the current user. These are recorded in the Registry at HKCU\Environment.
- **VOLATILE Variables** are created during logon script execution. These apply to the current logon session and are recorded in the Registry at HKCU\VolatileEnvironment.

Note: ipMonitor is able to set only **PROCESS** Environment Variables to launch a script or executable via the External Process Monitor or External Process Alert.

The External Process Monitor can be configured to determine test success or failure by reading a PROCESS Environment Variable rather than basing its status on the script or executable's exit code.

Note1: If the third party executable or script fails to finish within the **Maximum Test Duration** interval, ipMonitor will terminate the process.

Note2: We recommend that the third party executable be located on the same machine that hosts ipMonitor. The third party executable or script runs in the memory space and environment of the ipMonitor host machine. Even if it is called across the network using a UNC path, it still runs locally.

Test Results

- **return**. The numeric "exit code" reported by the third party executable.

Fan

The Fan Monitor uses SNMP communication to test the current status of a fan. The Monitor's ability to retrieve and analyze the response received from a fan allows an Administrator to:

- Be notified when the fan is not functioning as expected.
- Ensure that server temperature remains within safe operating limits.
- Obtain an accurate picture of current fan health.

Using this information, fan degradation can be immediately detected and dealt with in a timely manner before it can impact critical servers or other network components.

The Fan Monitor Wizard is designed to help you configure a Fan Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Fan Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Note1: The Humidity, Temperature, Battery and Fan Monitors' default **Delays Between Tests While: Up**, **Warn**, **Down** and **Lost** settings are slightly different from those of other Monitor types. Due to the high potential for disaster when abnormal conditions are detected, these default settings have been lowered from 300 seconds to 60 seconds between tests.

Note2: The Fan Monitor Wizard allows you to configure Fan Monitors quickly and easily. However, if you prefer greater control over the process, you can Clone an existing Fan Monitor and make any required configuration changes manually.

File Property

The File Property Monitor detects modifications made to a file and alerts you when changes outside of specified bounds are detected. The Monitor tests various properties of a given file, making it ideal for:

- Verifying the existence of a file.
- Determining whether a file has been modified.
- Determining whether the size of a file has changed.
- Detecting changes in a file's checksum value.

The File Property Monitor tests the existence and properties of a file at regular intervals to detect any changes outside the boundaries you define. When a change is encountered, the Monitor can trigger:

- A Failure Notification Alert.
- An Information Alert.
- Both a Failure Notification Alert and an Information Alert.

Configuring Information Alerts is an optional process. The separation of Alerting actions from Monitoring actions allows you to instruct the Monitor to send an Information Alert but remain in an Up state even if a change is detected. This gives you maximum flexibility to configure each File Property Monitor to meet your specific needs depending on the type of file being tested.

Test Results

- **size**. The current available space on the share being monitored. Available space is reported in gigabytes (gb) and megabytes (mb)..

File Watching

The File Watching Monitor reads file content one line at a time, making it ideal for locating various types of information recorded in application or server log files, such as errors, events and notices.

Syslog files, which are sent across the network to a Syslog Server rather than being recorded locally, can also easily be monitored using the File Watching Monitor.

The File Watching Monitor scans the file you specify to locate any entries that match the regular expressions you have defined. Regular expression searching is ideal for filtering specific details from the lines in a file, because the format and contents in log files may vary significantly depending on the information recorded.

When a match is found, a Content Generator that you configure parses the information, and then an Information Alert is triggered.

The File Watching Monitor may be configured to only trigger a single Information Alert per scan, as opposed to one per match, which can significantly reduce the number of Alerts you receive.

The File Watching Monitor maintains a pointer to the file offset, ensuring that lines are only analyzed once. Should the log file be reset, the pointer will also be reset.

Note: When creating a new File Watching Monitor, note that the Monitor starts searching forward from the time of creation; it does not search historical content already in the file.

While configuring a Monitor, clicking the **Force Test** button will reset the testing cycle for the Monitor, allowing you to promptly reapply new configuration parameters. However, this will not work with the File Watching Monitor as its pointer will be reset to its current time or, essentially, the end of the file.

The **Preview** test, however, does search the file's existing content, making it ideal for configuration and troubleshooting purposes.

Example

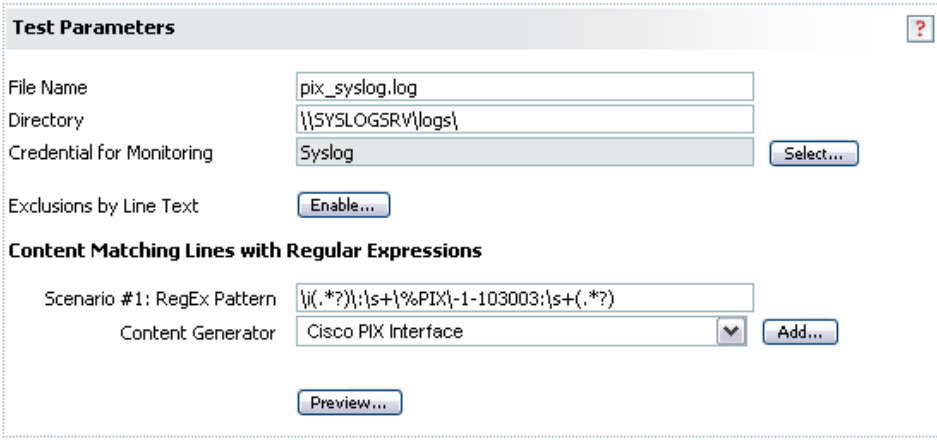
Most servers and server applications are capable of recording system errors to a log file. ipMonitor can be used to search through the contents of a log file for specific entries based on user-defined criteria, or a Regular Expression.

When a match is found, this information can be extracted from the file and formatted using a Content Generator before it is sent to an Information Alert.

Sample Line in Syslog :: Cisco PIX Firewall

```
Jul 29 2004 09:56:27: %PIX-1-103003: (Primary) Other firewall
network interface 4 failed.
```

Monitor Configuration Settings

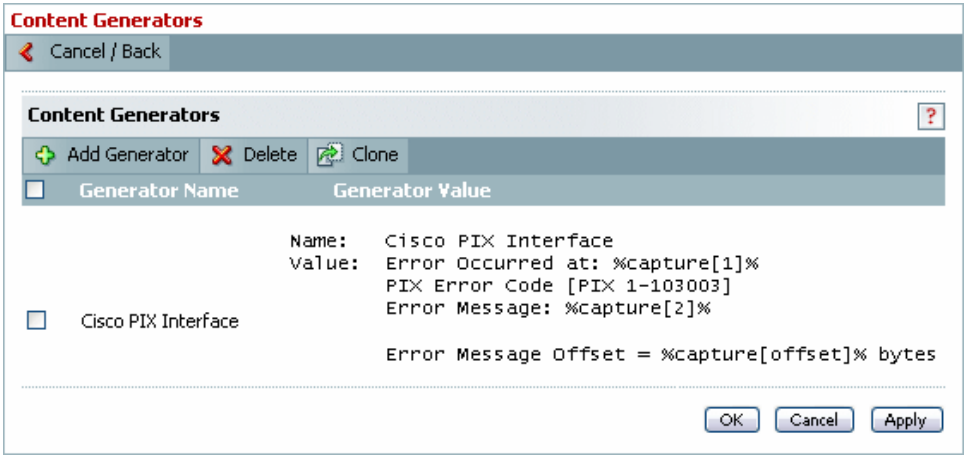



```
File Name: pix_syslog.log
Directory: \\SYSLOGSRV\logs\

Scenario #1: RegEx Pattern \i(.*?)\:\s+\%PIX\-1-103003:\s+(.*?)
```

Content Generator

After the configuration settings are applied, it will then be necessary to create a **Content Generator** to insert the results into an email message body or other action type when an action is triggered. A Content Generator is created in the **Alerts / Content Generators** section.



```
Name:  Cisco PIX Interface

Value: Error Occurred at: %capture[1]%
       PIX Error Code [PIX 1-103003]
       Error Message: %capture[2]%

Error Message Offset = %capture[offset]% bytes
```

After the Content Generator has been created and saved, it will then be necessary to assign the newly created Content Generator to the File Watching Monitor. This selection is made in the **Information Alert Content** drop-down box located in the Monitor configuration page.

Information Alert Results

The following is a sample of the formatted result when ipMonitor finds an entry in the file matching the Regular Expression.

```
Error Occurred at: Jul 29 2004 09:56:27
PIX Error Code [PIX-1-103003]
Error Message: (Primary) Other firewall network interface 4
failed.

Error Message Offset = 23698 bytes
```

Finger

The Finger Monitor is used to test a remote RUIP host for availability and its level of responsiveness.

The Finger protocol provides an interface to a remote user information program (RUIP), which works by taking an email address as input and returning information, such as whether the user is currently logged on.

The Finger Monitor:

1. Connects to the service, performs a blind query (CRLF) and waits for a response
2. Considers the test successful if a valid response is returned within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the opening message.
4. Considers the test to have failed if the Finger server fails to respond or responds with an error code indicating that the Service is not available.

Use the Finger Monitor to test that:

- A Finger client can open a connection with a Finger server
- The server adheres to the Finger protocol by responding with the correct codes
- The server responds within the required number of seconds

FTP

The bandwidth light FTP Monitor opens a connection to the specified FTP server and waits for the Server to respond with a standard "Service Ready for a new user" Code 220 message.

Upon receipt of the opening message, the FTP Monitor safely disconnects from the server by sending out a QUIT command to terminate the connection.

If the FTP server fails to respond, or if it responds with an error code indicating that the Service is not available, ipMonitor considers the test to have failed.

Use the FTP Monitor to test that:

- An FTP client can open a connection with a FTP server
- The server adheres to the FTP protocol by responding with the correct codes
- The server responds within a required number of seconds

If you perform log analysis on your FTP logs, the FTP Monitor may cause hits to be generated. Refer to your log analysis software for information regarding how to exclude ipMonitor from analysis.

If you need to test your FTP Server's ability to log in to a client or transmit a file, create an **FTP User Experience** monitor.

FTP User Experience

The FTP User Experience Monitor tests a FTP server's ability to accept incoming sessions, process user logons and then transmit the requested file.

Use the FTP User Experience Monitor to ensure that the FTP server can:

- Communicate with ipMonitor via the FTP protocol.
- Respond within a required number of seconds.
- Log on a user.
- Transmit a file that is an exact content match with the snapshot of the resource ipMonitor has on record.

FTP User Experience Monitor features:

- Automatically log in to an anonymous FTP server.
- Use a Credential to log in to a private FTP server.
- Supports either Active FTP or Passive FTP.
- Perform a CRC comparison on the downloaded file to verify its contents.

Gopher

The Gopher Monitor is used to test a Gopher server for availability, as well as its level of responsiveness.

As the Gopher system predates the World Wide Web, it has limited application in today's network environment. However, it is sometimes used to organize files in a hierarchically structured list.

The Gopher Monitor:

1. Connects to the Service, performs a blind query (CRLF) and waits for a response.
2. Considers the test successful if a valid response is returned within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the opening message.
4. Considers the test to have failed if the Gopher server fails to respond, or if it responds with an error code indicating that the Service is not available.

Use the Gopher Monitor to test that:

- A Gopher client can open a connection with a Gopher server
- The server adheres to the Gopher protocol by responding with the correct codes
- The server responds within a required number of seconds

HTML/ASP

The HTML / ASP Monitor tests a web server's ability to accept incoming sessions, generate a web page server-side, and then transmit the requested web page to ipMonitor.

The requested pages may be static HTML pages or dynamic pages such as Microsoft Active Server Pages, Cold Fusion pages or PHP Hypertext Preprocessor pages.

Typical uses of the HTML / ASP Monitor are:

- Monitoring web-based applications for sales and customer service.
- Accessing corporate databases and back-end applications.

Use the HTML / ASP Monitor to ensure that the web server can:

- Communicate with ipMonitor via the HTTP protocol.
- Respond within a required number of seconds.
- Run server side scripts, ActiveX components, access data sources, and so on to successfully construct the requested web page.
- Transmit the requested web page or resource.

HTML / ASP Monitor features include:

- Searching the delivered page for a specific text string.
- Using HEAD requests to save on bandwidth.
- Following redirections until a valid file is transmitted or until an error occurs.
- Transmitting account and password information if required by the web server.

Test Results

- **Kps**. Kilobytes Per Second. This value indicates the web server's transfer data rate.
- **http**. HTTP Status Code. Codes in the 200 to 399 range indicate success. Codes in the 400 to 599 range indicate an error.

HTTP

The lightweight HTTP Monitor tests a web server's ability to accept incoming sessions and conduct a transaction.

Use the HTTP Monitor to ensure that the web server can:

- Communicate with ipMonitor via the HTTP protocol
- Respond within a required number of seconds

HTTP Monitor features include:

- Using HEAD requests to save on bandwidth

Note: If you use log analysis or web analytics software, the HTTP Monitor may cause hits to be generated. Refer to your log analysis software for information regarding how to exclude ipMonitor from analysis.

If you require the ability to request a specific page on the website or to analyze test results, see “HTTP User Experience” on page 116 and “HTML/ASP” on page 114.

Test Results

- **http**. HTTP Status Code. Codes in the 200 to 399 range indicate success. Codes in the 400 to 599 range indicate an error.

HTTP User Experience

The HTTP - User Experience Monitor tests a web server's ability to accept incoming sessions and transmit a requested resource, such as a web page, or the results of a CGI script.

Use the HTTP - User Experience Monitor to ensure that the web server can:

- Communicate with ipMonitor via the HTTP protocol.
- Respond within a required number of seconds.
- Access the source files and/or resources required to construct a specified web page or resource.
- Transmit a specified web page or resource that is an exact content match with the snapshot of the resource ipMonitor has on file.

Note. This monitor can generate considerable bandwidth if aggressive timing parameters are applied. Therefore, we advise keeping the default timing intervals of 300 seconds intact.

If you use log analysis or web analytics software, this monitor may cause hits to be generated. Refer to your log analysis software for information regarding how to exclude ipMonitor from analysis.

Test Results

- **Kps**. Kilobytes Per Second. This value indicates the web server's transfer data rate.
- **http**. HTTP Status Code. Codes in the 200 to 399 range indicate success. Codes in the 400 to 599 range indicate an error.

HTTPS

The HTTPS Monitor tests a web server's ability to accept incoming sessions over a secure channel, generate a web page server side, and then transmit the requested web page to ipMonitor.

The requested pages may be static HTML pages or dynamic pages such as Microsoft Active Server Pages, Cold Fusion pages or PHP Hypertext Preprocessor pages.

Typical uses of the HTTPS Monitor are:

- Monitoring secure web-based applications for sales and customer service.
- Accessing corporate databases and back-end applications.

Use the HTTPS Monitor to ensure that the web server can:

- Communicate with ipMonitor via the HTTPS protocol.
- Respond within a required number of seconds.
- Run server side scripts, ActiveX components, access data sources, and so on to successfully construct the requested web page.
- Transmit the requested web page or resource.

HTTPS Monitor features include:

- Searching the delivered page for a specific text string.
- Using HEAD requests to save on bandwidth.
- Following redirections until a valid file is transmitted or until an error occurs.
- Transmitting account and password information if required by the web server.

Humidity

The Humidity Monitor uses SNMP communication to assess humidity levels in a specific area. The Monitor's ability to retrieve and analyze the response received from a humidity sensor allows an Administrator to:

- Be notified when abnormal humidity conditions are detected.
- Ensure that humidity levels in a specific area remain within safe operating limits.
- Obtain an accurate picture of current humidity levels.

High humidity levels lead to condensation, which in turn leads to corrosion. Low humidity is not desirable either, as it can cause problems with excess static electricity. Dealing with these issues in a timely manner ensures they will not impact critical servers or other network components.

The Humidity Monitor Wizard is designed to help you configure a Humidity Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Humidity Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Note1: The Humidity, Temperature, Battery and Fan Monitors' default **Delays Between Tests While: Up**, **Warn**, **Down** and **Lost** settings are slightly different from those of other Monitor types. Due to the high potential for disaster when abnormal conditions are detected, these default settings have been lowered from 300 seconds to 60 seconds between tests.

Note2: The Humidity Monitor Wizard allows you to configure Humidity Monitors quickly and easily. However, if you prefer greater control over the process, you can **Clone** an existing Humidity Monitor and make any required configuration changes manually.

Test Results

- **Humidity**. The humidity level response received from the humidity sensor, expressed as a percentage.

IMAP4

The bandwidth light IMAP4 Monitor opens a connection to the specified IMAP4 server and waits for the server to respond with a standard "Service Ready for a new user" Code 220 message.

Upon receipt of the opening message, the IMAP4 Monitor safely disconnects from the server by sending a LOGOUT command to terminate the connection.

If the IMAP4 server fails to respond, or responds with an error code indicating that the Service is not available, ipMonitor considers the test to have failed.

Use the IMAP4 Monitor to test that:

- An IMAP4 client can open a connection with an IMAP4 server
- The server adheres to the IMAP4 protocol by responding with the correct codes
- The server responds within a required number of seconds

IMAP4 – User Experience

The IMAP4 - User Experience Monitor tests the ability of your SMTP server to receive and distribute email, as well as the ability of your end-users to log in from an IMAP4 enabled email client and manage their email.

The IMAP4 - User Experience Monitor uses this process to simulate an email round trip and measure the time it takes for a series of transactions to occur:

1. Connects to port 25 of the SMTP server for the recipient address you specify to deliver an email.
2. Logs in to the IMAP4 mail server and selects the INBOX.
3. Searches for the test email it sent and flags it for deletion.
4. Sends a LOGOUT command.

If the SMTP mail server or IMAP4 server fails to respond, or responds with an error code at any time, ipMonitor considers the test to have failed.

Use the IMAP4 - User Experience Monitor to test that:

- The SMTP mail server can accept and distribute email.
- The IMAP4 mail server can authenticate users.
- The IMAP4 server can respond correctly to IMAP4 commands.
- The server responds within a required number of seconds.

Note: ipMonitor uses a message with a special subject line to test the send and receive ability of the IMAP4 Mail Server, similar to the following: "Subject: ipm8:imap4:guid:441991169".

ipMonitor

The ipMonitor Monitor can be used to monitor an external installation of ipMonitor on another computer.

The ipMonitor Monitor can be configured for two different purposes:

- It can be used to perform internal diagnostics of the ipMonitor installation you specify.
- It can be used to perform redundant monitoring and alerting on behalf of the ipMonitor installation you specify.

The ipMonitor Monitor can be used to test an ipMonitor installation's ability to:

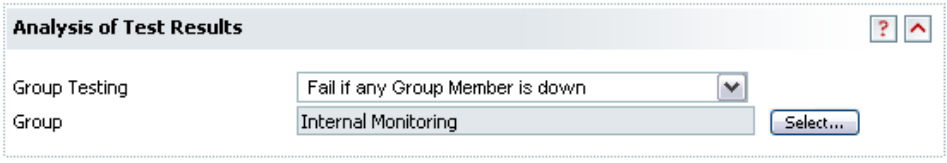
- Accept incoming sessions.
- Conduct transactions via the HTTP or HTTPS protocol.
- Respond within a required number of seconds.

The ipMonitor Monitor may optionally be used to perform redundant monitoring and alerting for the external ipMonitor installation when one of the following options is selected:

- Fail if any Group Member or Dependency Monitor is down
- Fail if any Group Dependency is down
- Fail if any Group Member is down

Creating Redundant Alerting

The ipMonitor Monitor can be used to perform a quick diagnostic or to perform redundant Alerting for an external ipMonitor installation.



Group Testing

The following options are used to specify which function the ipMonitor Monitor will perform:

- Do not obtain the status of a Group, just a quick diagnostic
- Fail if any Group Member or Dependency Monitor is down
- Fail if any Group Dependency is down
- Fail if any Group Member is down

Group

Click **Select** to specify the Group on the remote ipMonitor installation you want to monitor for a Down state.

Select...

Force an immediate connection to the remote ipMonitor installation to obtain a list of Groups that can be monitored. Select a Group from the list of Groups displayed.

If the Group list is not displayed, verify the validity of:

- IP address or Domain Name: Ping and/or perform a TraceRoute to the remote ipMonitor installation to verify the connection.
- Port: ipMonitor can be installed on many possible Ports.
- Account information: Log in to the remote ipMonitor installation to verify that the account you provided is valid and has Real-time Statistics list access.

Note: The test will fail and trigger an Alert when:

- The specified remote ipMonitor installation is unavailable.
- The diagnostic fails to complete within the Maximum Test Duration.
- Depending on the Group Testing option selected in the Analysis of Test Results section, a Member or Dependency Monitor in the selected Group has tried to trigger an Alert.

IRC

The Internet Relay Chat Monitor is used to test an IRC server's ability to accept incoming sessions, as well as its level of responsiveness.

IRC is a multi-person conversation system that allows users to join chatting channels and converse in real-time. The IRC server relays everything that is typed to those people who are in the channel.

The IRC Monitor:

1. Constructs both a user name and a "nick" name based on the current time, and then attempts to log in.
2. Safely disconnects from the server upon receipt of the opening message.
3. Considers the test successful if a valid response is returned within the specified Maximum Test Duration.
4. Considers the test to have failed if the IRC server fails to respond or responds with an error code indicating that the Service is not available.

Use the IRC Monitor to test that:

- An IRC client can open a connection with an IRC server
- The server adheres to the IRC protocol by responding with the correct codes
- The server responds within a required number of seconds

Kerberos 5

The Kerberos 5 Monitor tests an authentication server's ability to respond to a ticket request.

The Kerberos authentication protocol provides a mechanism for mutual authentication between a client and a server before a network connection is opened between them. In other words, authentication happens before permission to access network resources is granted.

The Kerberos 5 Monitor tests the ability of the Kerberos server to respond to a ticket request by:

- Sending a ticket request to the Authentication Service (AS). The ticket request contains the client identity `ipMonitor`, a session key, a timestamp, and other information, such as flags.
- Measuring the roundtrip time determine responsiveness of the service.

If the service does not respond within the specified Maximum Test Duration, the test fails.

LDAP

The Lightweight Directory Access Protocol (LDAP) Monitor can be used to access standalone LDAP directory services or directory services that have an X.500 backend.

LDAP runs directly over TCP. It is used to store information in a database structure about users, including the network privileges assigned to each user. Revoking or changing privileges can be done from one entry in the LDAP directory, rather than at many machines across the network.

The LDAP Monitor supports LDAP version 2, which is the most commonly supported version. Most LDAP version 3 servers will support LADAP version 2 client requests.

The LDAP Monitor:

1. Establishes a LDAP connection.
2. Sends a Bind Request indicating that it is making a LDAP v2 request.
3. Sends a Search Request asking which LDAP versions the LDAP server supports.
4. Sends an Unbind Request for the LDAP server to close the TCP connection.

Use the LDAP Monitor to test that:

- A LDAP client can open a connection with a LDAP server
- The server adheres to the LDAP protocol by responding with the correct codes
- The server responds within a required number of seconds

Link – User Experience

The Link - User Experience Monitor tests any HREF links it locates within a specified web page to ensure the links can be successfully accessed by your web site's visitors.

The requested page may be comprised of static HTML or dynamic pages, such as:

- Microsoft Active Server Pages
- Cold Fusion Pages
- PHP Hypertext Preprocessor pages

To simulate a customer session, the monitor:

1. Connects to the web server
2. Waits for a response within a required number of seconds
3. Receives the requested web page or resource
4. Analyzes the content of the web page to locate any internal or external links
5. Accesses each link on the page sequentially
6. Checks that the referenced link or resource is available

Typical uses of this monitor are:

- Verifying that any external links your website references are available
- Ensuring that important resources you link to are not removed or changed
- Ensuring that dynamically generated content references correct links

Features of the monitor include:

- Searching the delivered page for URLs
- Using HTTP HEAD requests and upgrading to GET if necessary when following links
- Controlling whether ipMonitor will connect to any or only a specific set of web servers
- Skipping specific resources to speed up analysis
- Transmitting account and password information if required by the web server

Test Results

- **links.** The total number of links that were checked during the last Monitor test.

- **blocked.** The total number of links that were not checked by the Monitor during the last test. This value is directly based on the settings configured in the Server Inclusions and Link Filtering fields.
- **kps.** Kilobytes Per Second. This value indicates the web server's transfer data rate.

Lotus Notes

The Lotus Notes Monitor is used to test the ability of a Lotus Notes mail server to accept incoming sessions, as well as its level of responsiveness.

The Lotus Notes Monitor:

1. Opens a connection to the specified Lotus Notes server and waits for the Service to respond.
2. Considers the test successful if a valid response is returned within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the opening message.
4. Considers the test to have failed if the Lotus Notes server fails to respond or responds with an error code indicating that the Service is not available.

Use the Lotus Notes Monitor to test that:

- A Lotus Notes client can open a connection with a Lotus Notes server.
- The server adheres to the Lotus Notes protocol by responding with the correct codes.
- The server responds within a required number of seconds.

MAPI – User Experience

The MAPI - User Experience Monitor uses this process to simulate an email round-trip and measure the time it takes for a series of transactions to occur:

1. The MAPI - User Experience Monitor connects to the SMTP server on port 25, and then sends an email message for the recipient address specified.
2. The monitor logs into the Exchange Server and uses the email account specified in the default Mail Profile to connect to an Exchange mailbox.
3. The monitor searches for the test email it sent and, if located, flags it for deletion.
4. The MAPI - User Experience Monitor sends a logout command to the Exchange Server.

ipMonitor considers the test to have failed if:

- The SMTP server fails to respond or returns an error code.
- The Exchange Server fails to respond or returns an error code.
- The MAPI - User Experience Monitor is unable to locate the sent email.

Use the MAPI - User Experience Monitor to test that:

- The SMTP mail server can accept and distribute email.
- The Exchange Server can authenticate users.
- The Exchange Server can respond correctly to MAPI commands.
- MAPI clients can receive their email.
- The Exchange Server responds within a required number of seconds.

Outlook Account Requirements of this Monitor

To operate correctly, this monitor requires the following Microsoft Outlook environment:

- Access to the messaging subsystem of Microsoft Outlook. A full version of Microsoft Outlook that supports the MAPI protocol must be installed on the ipMonitor server for this purpose. The Microsoft Outlook application itself does not need to be running.
- A Microsoft Outlook Email Account to exist under the default Mail Profile of the Windows User Account impersonated by the Monitor.

To set up a windows Mail Profile as required by this monitor

1. Log in to the ipMonitor server using the Windows Domain Account to be used by the MAPI - User Experience Monitor.
2. Install Microsoft Outlook.
3. Launch Microsoft Outlook.
4. Follow the steps outlined in the Outlook Startup Wizard to configure the default Mail Profile for the Domain Account.

When configuring the MAPI User Experience Monitor, the **Credential for Monitoring** should directly reference the Windows Account used to log in to the ipMonitor server

Contents of the Test Email Message

ipMonitor uses a message with a special subject line to test the send and receive ability of the IMAP4 Mail Server, similar to the following: "Subject: ipm8:imap4:guid:441991169".

Memory Usage

The Memory Usage Monitor uses a local API call or SNMP communication to test the amount of physical memory (RAM) available on:

- The local machine.
- A remote SNMP-enabled computer running Microsoft Windows NT, 2000, XP or 2003.
- A remote SNMP-enabled computer running a Unix-Based Operating System such as Linux, Solaris, HP-UX, and so on.
- An SNMP-enabled device.

It effectively ensures that:

- Memory leaks are detected before performance can be affected.
- The minimum amount of physical memory required by the system remains available.
- The total amount of physical memory allotted to the server is not exceeded.

The Memory Usage Monitor Wizard is designed to help you configure a Memory Usage Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Memory Usage Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

If you prefer greater control over the process, you can Clone an existing Memory Usage Monitor and make any required configuration changes manually.

Test Results

- **Avail**. These values indicate the amount of physical memory currently available on the system, in megabytes (MB), and as a percentage (%).
- **avail-avg**. This value indicates the average amount of physical memory on the system, based on the tests performed during the length of time specified in the Sample Size field.

Network Speed

The Network Speed Monitor is used to test the available bandwidth or the speed of a transaction between ipMonitor and another point on a network.

To perform this test, the Network Speed Monitor requires a Character Generator service to be installed on the target server.

ipMonitor opens a connection to the Character Generator Service, which then responds by sending a stream of data that continues until ipMonitor terminates the connection. The stream is typically a recognizable pattern of printable ASCII characters.

Note: We recommend that the Network Speed Monitor only be used in the safe zone of networks that are secured with a firewall. If the transaction between the Character Generator and ipMonitor traverses the firewall, it could be interpreted as a denial of service attack.

ipMonitor measures the length of time it takes to download the "Sample Size" you specify, and then performs a kilobytes per second calculation to determine if the test passes or fails.

Test Results

- **kb/s**. This value indicates the network's transfer data rate, displayed in kb/s (1000 bits per second).
- **KB/s**. This value indicates the network's transfer data rate, displayed in KB/s (1024 bytes per second).

NNTP

The Network News Transfer Protocol (NNTP) Monitor tests the ability of a News server to accept incoming sessions, as well as its level of responsiveness.

NNTP servers are used for the distribution, inquiry, retrieval, and posting of news articles. News articles are stored in a central database, allowing subscribers to select only those items they wish to read, and include the ability to index, cross-reference and expire messages.

The NNTP Monitor:

1. Opens a connection to the specified NNTP server and waits for the service to respond.
2. Considers the test successful if a valid Server Ready connection code is returned within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the Server Ready code. The NNTP server then sends a code indicating that it is disconnecting the socket.
4. Considers the test to have failed if the NNTP server fails to respond or responds with an error code indicating that the service is not available.

Use the NNTP Monitor to test that:

- A NNTP client can open a connection with a NNTP server
- The server adheres to the NNTP protocol by responding with the correct codes
- The server responds within a required number of seconds

NTP

The NTP Monitor is used to test the availability and responsiveness of a Network Time Protocol Service.

NTP is a vital part of some networks. Clusters and other parallel processing environments depend on accurate and synchronized time. If these servers become unsynchronized, older applications may behave unpredictably.

The NTP Monitor:

1. Opens a connection to the specified NTP server and waits for the Service to respond.
2. Considers the test successful if a valid Universal Time Coordinated (UTC) time value is returned within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the UTC time value.
4. Considers the test to have failed if the NTP server fails to respond or responds with an error code indicating that the Service is not available.

Use the NTP Monitor to test that:

- A NTP client can open a connection with an NTP server
- The server adheres to the NTP protocol by responding with the correct codes
- The server responds within a required number of seconds

Ping

The Packet INternet Groper (ping) Monitor is used to test the availability of a specific computer or device on the Internet.

ipMonitor measures round trip time by sending an Internet Control Message Protocol (ICMP) echo request to the specified IP Address and then waiting for a valid UDP packet to be returned.

The test will pass if the Monitor receives a valid return packet within the required timeout period.

The test will fail if the Monitor's specified timeout period expires.

The Ping Monitor tests:

- The route between ipMonitor's host machine and an IP-enabled computer or device.
- That the target computer or device is able to respond.
- That the packet makes the complete round trip within a specific number of seconds.

The Ping Monitor is often specified as a Dependency for a Group of Monitors. For example, a Web application Group could include a web server, SQL server, drive space, etc, and a Ping Monitor that monitors the availability of the server computer.

In this case, you could assign the Ping Monitor as a Dependency for the Web application Group. In the event that problems with the server occur, this configuration would prevent you from receiving Alerts for all the application Monitors and resource Monitors configured to watch the server computer.

Not only would this minimize the number of Alerts you receive, it would also help you quickly identify the source of the problem.

POP3

The bandwidth light POP3 Monitor opens a connection to the specified POP3 server and waits for the Server to respond with a standard "Service Ready for a new user" Code 220 message.

Upon receipt of the opening message, the POP3 Monitor safely disconnects from the server by sending a QUIT command to terminate the connection.

If the POP3 server fails to respond, or responds with an error code indicating that the Service is not available, ipMonitor considers the test to have failed.

Use the POP3 Monitor to test that:

- A POP3 client can open a connection with a POP3 server
- The server adheres to the POP3 protocol by responding with the correct codes
- The server responds within a required number of seconds

POP3 – User Experience

The POP3 - User Experience Monitor tests the ability of your SMTP server to receive and distribute email, as well as the ability of your end-users to log in from a POP3 enabled client and retrieve their mail.

The POP3 - User Experience Monitor uses the following process to simulate an email roundtrip, and measures the time it takes for the series of transactions to occur:

1. The monitor delivers an email to the SMTP server on port 25 for the recipient address you specify.
2. The monitor logs in to the POP3 Mail Server on port 110 and retrieves the LIST of queued mail.
3. The monitor locates and validates the email it sent, and sends a DELE command to delete the message.
4. The monitor disconnects from the server by sending a QUIT command to terminate the connection.

If the SMTP server or POP3 server fails to respond, or responds with an error code at any time, ipMonitor considers the test to have failed.

Use the POP3 - User Experience Monitor to test that:

- The SMTP mail server can accept and distribute mail.
- The POP3 mail server can authenticate users.
- The POP3 server can deliver mail to a POP3 client.
- The POP3 and SMTP servers respond within a required number of seconds.

Implementation

ipMonitor sends a message with a special subject to test the send and receive ability of the POP3 Mail Server, similar to the following: "Subject: ipm9:pop3:guid:141991169".

After ipMonitor logs into the POP3 server on port 110 and retrieves the LIST of queued mail, it will:

1. Retrieve up to a maximum of the 100 last emails.
2. Attempt to locate the email with the special subject line.
3. Make several attempts to retrieve the email before the test expires.
4. Delete the email after verifying the subject line to prevent email from accumulating on the POP3 Server.

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) Monitor tests an authentication server's ability to perform an internal database lookup and respond to an authentication request.

RADIUS is commonly used to provide authentication and authorization for dial-up, virtual private network, and wireless network access from a centralized server.

The RADIUS Monitor:

1. Tests the ability of the RADIUS server to respond to an authentication request.
2. Sends user credentials and connection parameters in a RADIUS message to the RADIUS server.
3. Waits for the RADIUS Server to authenticate and authorize the Access-Request.
4. Validates the RADIUS message response sent back.
5. Determines the responsiveness of the Service by analyzing roundtrip time.
6. Considers the test to have failed if the Service does not respond within the Maximum Test Duration.

Test Limitations

The RADIUS Monitor tests the RADIUS server to verify its availability and responsiveness. It does not perform a full login to the RADIUS server using the account information provided during configuration. It simply tests an authentication server's ability to perform an internal database lookup and respond to an authentication query.

Depending on your RADIUS solution, you may not need to provide account information or a 'secret'. When invalid account information is provided, your authentication solution may send negative responses instead of quietly discarding requests. If this occurs, ipMonitor will accept that the service is available.

RWHOIS

The RWHOIS Monitor is used to test a Remote WHOIS server for availability, as well as its level of responsiveness.

The RWHOIS protocol extends the WHOIS protocol by providing a decentralized means of storing and retrieving information related to network information systems and the individuals associated with those systems.

The RWHOIS Monitor:

1. Connects to the Service and waits for the Service to respond.
2. Considers the test successful if the RWHOIS server responds indicating that it is available within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the opening response.
4. Considers the test to have failed if the RWHOIS server fails to respond or responds with an error code indicating that the service is not available.

Use the RWHOIS Monitor to test that:

- A RWHOIS client can open a connection with a RWHOIS server.
- The server adheres to the RWHOIS protocol by responding with the correct codes.
- The server responds within a required number of seconds.

Service

The Service Monitor uses RPC or SNMP communication to test whether a specified Service is running on:

- The local machine
- A remote SNMP-enabled computer running Microsoft Windows NT, 2000, XP or 2003
- A remote SNMP-enabled computer running a Unix-Based Operating System such as Linux, Solaris, HP-UX, and so on.

Common uses of the Service Monitor:

- Ensuring that a critical Service is not unexpectedly stopped.
- Monitoring the state of Dependency Services that must be running for a critical Service to function.
- Automatically taking Recovery actions to Restart the Service or Reboot the computer in the event that a Service is unexpectedly stopped.

The Service Monitor works with any host machine running:

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003

The Service Monitor Wizard is designed to help you configure a Service Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Service Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Windows Recovery options for Services

The Windows Control Panel / Administrative Tools / Services / Recovery dialog can be used to set recovery options that will automatically Restart the Service, Run a File or Reboot the Computer.

The purpose of the Windows recovery options for Services is very similar to ipMonitor's Recovery Alerts. There are some differences to consider:

- ipMonitor can Alert you by email or phone if the Service stops, and escalate to automatic Recovery Actions if prior Alerts are not handled.
- ipMonitor can Alert you if the Recovery Actions fail.
- ipMonitor's flexible Alert scheduling allows you to be notified by email or phone during certain hours of the day or days of the week. At other times, Recovery Alerts could be scheduled to automatically take recovery actions.
- ipMonitor's Alerts can be configured to process any number of notification, integration and recovery actions concurrently.

If you are using the Windows Recovery options for Services, you can:

- Use Alert Recovery Messages to be informed when Windows has taken a recovery action based on the Windows Recovery timing parameters you specify.
- Use the Event Log Monitor to be notified when Windows takes recovery actions on behalf of a Service.

SMTP

The Simple Mail Transfer Protocol (SMTP) Monitor uses the following process to test a SMTP mail server's ability to accept incoming sessions, as well as its level of responsiveness:

1. The SMTP Monitor opens a connection to the specified SMTP mail server and waits for the server to respond with a standard "Service Ready" Code 220 opening message.
2. Upon receipt of the opening message, the SMTP Monitor safely disconnects from the server by sending a QUIT command to terminate the SMTP connection.
3. If the mail server fails to respond or responds with an error code indicating that the Service is not available, ipMonitor considers the test to have failed.

Use the SMTP Monitor to test that:

- A mail client can open a connection with a SMTP mail server.
- The server adheres to the SMTP protocol by responding with the correct codes.
- The server responds within a required number of seconds.

Minimizing SMTP Server Load

SMTP servers are often configured to perform a reverse lookup on all incoming connections. This is done to attempt to verify that the IP address of the SMTP client matches the host/domain submitted when the connection is established.

Because the IP address of the SMTP Monitor may be verified each time the server is tested:

- Delays can occur when connecting to the server.
- The load on your SMTP server can increase if aggressive Timing Parameters are used.

To avoid this, you can:

- Add a reverse DNS entry for ipMonitor's host machine.
- Adjust the SMTP Monitor's Timing Parameters by increasing the Maximum Test Duration value and the Delays Between Tests parameters.

SNMP

The lightweight SNMP Monitor tests an SNMP agent's ability to respond to an information request, as well as its level of responsiveness.

ipMonitor measures round trip time by sending a request for a fixed piece of information, `sysUpTime` oid 1.3.6.1.2.1.1.3.0, to the specified SNMP agent and then waiting for a valid response.

The Monitor test will pass if the Monitor receives a valid response within the required timeout period.

The SNMP Monitor tests that:

- The target SNMP agent is running and able to respond.
- The response makes the complete round trip within a specific number of seconds.

To monitor the end-to-end performance of your SNMP-enabled devices or applications from the end-user perspective, use the SNMP - User Experience Monitor to perform synthetic transitions and analyze results:

1. Retrieves a Numeric or Textual value from a SNMP agent.
2. Tests the value against the rules you define.
3. Performs delta comparisons.

SNMP Agent Security

A commonly-used SNMP security feature requires you to specify exactly which IP addresses the SNMP agent is permitted to communicate with. If this is security feature is enabled on the SNMP agent you wish to monitor, you may have to configure it to include the IP address of the ipMonitor host machine. Another commonly-used SNMP security feature requires you to specify exactly which IP addresses the SNMP agent is permitted to communicate with. If this is security feature is enabled on the SNMP agent you wish to monitor, you may have to configure it to include the IP address of the ipMonitor host machine.

SNMP – User Experience

The SNMP - User Experience Monitor is used to retrieve and analyze data from SNMP enabled network devices, services and applications. The SNMP - User Experience Monitor retrieves a Numeric or Textual value from an SNMP agent and then tests the value against the rules you define.

- Common uses of the SNMP - User Experience Monitor include:
- Identifying ICMP flood attacks
- Trapping spikes in network traffic
- Identifying packet failures
- Ensuring a minimum level of network availability
- Monitoring environmental conditions in server rooms and cabinets
- Identifying hardware problems in advance of costly failures

To locate OIDs for your applications and equipment:

- Use the ipMonitor SNMP - User Experience Monitor Wizard to query the SNMP-enabled device and retrieve SNMP data.
- Use ipMonitor's database of precompiled MIBs that can be browsed or queried. MIB Information is provided for common Windows and hardware applications. You can access the MIB database from the Configuration tab.
- To expand the default MIB database, use the Custom Database Builder available on the ipMonitor Support Portal to select MIBs from ipMonitor's MIB Repository and perform automated MIB compilations. You can then add the newly-created Custom MIB Database to your ipMonitor installation.
  Note: The Custom Database Builder is only available to licensed ipMonitor customers. For detailed instructions on compiling and importing a MIB database, refer to the tutorial entitled Add a Custom MIB Database to your ipMonitor Installation, located on the Support Portal.
- Use ipMonitor's SNMP Assistant, available from the ipMonitor Support Portal, to scan and collect information from your SNMP-enabled network devices and applications. This "scan" process allows you to discover whether a specific device supports an object defined by a particular MIB, as well as the type of information it will return.
- Contact your vendor directly to acquire MIBs for your various applications and equipment.

SNMP Data Types

The SNMP - User Experience Monitor is able to evaluate the following SNMP data-type values:

- INTEGER (up to 64-bit)
- OCTET STRING
- OBJECT IDENTIFIER
- IPADDRESS
- GAUGE
- TIMETICKS
- NULL

Test Results

- **value**. The numeric and textual value returned by the Monitor's Data OID.

SNMP – User Experience Wizard

The SNMP - User Experience Monitor Wizard is designed to help you configure an SNMP - User Experience Monitor with the least amount of initial input. There are a number of benefits to this approach:

- The SNMP - User Experience Monitor Wizard allows you to walk an SNMP-enabled device and retrieve a set of SNMP data without requiring an exact OID.
- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The SNMP - User Experience Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

The wizard has four pages:

- Step 1: Select SNMP Device and Scan Parameters
- Step 2: Select an SNMP Object to Monitor
- Step 3: Provide SNMP Object comparison Rules
- Step 4: Name and configure your SNMP User Experience Monitor

Step 1: Select SNMP Device and Scan Parameters

The following example illustrates the configuration process for creating an SNMP - User Experience Monitor to monitor the temperature reported by an APC environment probe:

To create a new SNMP - User Experience Monitor:

1. Log in to the ipMonitor Administration interface.
2. Click the Monitors menu option, then select Add a Monitor.
3. Select the **SNMP - User Experience (Wizard**) from the SNMP category.

Alternatively, you can also select the SNMP Wizard from the Configuration tab.

Step 2: Select an SNMP Object to Monitor

Browse through the returned set of Objects and their corresponding Values, and then click the Select button adjacent to the Object you want to monitor.

Step 3: Provide SNMP Object comparison Rules

Examine the details of the selected Object. This information is ideal for determining the type analysis that can be performed in the Analysis of Test Results section.

Comparison Rules

The type of data supported by the selected OID will determine the possible methods of analysis. Use the Object information outlined above to appropriately set the Comparison Rules in order to ensure the Monitor will pass upon being enabled.

Step 4: Name and configure your SNMP User Experience Monitor

Monitor Name

Enter a concise, descriptive name for the new Monitor. The Monitor Name will be displayed in the Monitors List, Monitor Status, Reports and Logs pages. Names may not be greater than 64 characters. Since ipMonitor does not use the name field to identify the Monitor internally, Monitor Names can be changed at any time without data loss.

Parent Group - Create in Existing Group

If this option is enabled, select one of the existing Groups from the Selected Group drop-down list. The new Monitor will automatically be added to this Group upon creation.

Parent Group - Create New Group

If this option is enabled, type the name of the new Group within the **Group Name** field. The new Monitor will automatically be added to this Group upon creation.

Create Monitor Enabled

After the Monitor is created, ipMonitor will immediately start testing the specified server or device using the configured settings. This option is enabled by default.

Store Monitor Statistics for Recent Activity and Historical Reports

ipMonitor will immediately begin to record test results, which are then used to generate Recent Activity and Historical Reports. This option is disabled by default.

Finish

Click the Finish button to exit the wizard and access the new Monitor in edit mode. You can make any final modifications to the Monitor in this mode, including setting Timing and Notification parameters.

After you are satisfied with the configuration settings, click the OK button at the bottom of the page. The new Monitor will be displayed within the Monitors List, and can be accessed for further configuration adjustments at any time.

SNMP Trap – User Experience

The SNMP Trap User Experience Monitor operates differently than all other Monitors in ipMonitor. It does not poll resources on timed intervals. Instead, it listens for incoming SNMP Traps and performs tests on the data it receives.

ipMonitor assumes the role of an SNMP manager by following this procedure:

1. It listens for any incoming Traps sent by SNMP Agents. These provide networking information for servers, applications or devices on the network.
2. ipMonitor then parses each Trap's Protocol Data Unit (PDU) message it receives using the "Trap Filtering" settings for each SNMP Trap User Experience Monitor it has configured, in order to determine whether the Trap applies to it.
3. If the incoming Trap applies to a SNMP Trap User Experience Monitor, an Alert will be triggered.
4. The SNMP Trap User Experience Monitor may optionally be configured to examine the Variable Binding information within a Trap. For example, it may search for temperature information, remaining battery power, an application error condition, and so on.
5. Any retrieved Variable Binding information can then be parsed by a Content Generator you have previously created and pushed to any Alert Type in ipMonitor that supports Information Alerts.

Integrating ipMonitor with third-party Network Management solutions:

- Many network servers, applications and devices include SNMP Agents to send out Traps. However, most do not send out Alerts. Using ipMonitor, these Agents can take advantage of ipMonitor's Alerting system to process Alerts.
- The SNMP Trap User Experience Monitor can also integrate with your other Network Management solutions that are SNMP-enabled. Incoming SNMP traps can be processed into Alerts for notification, integration and recovery

Turning on the SNMP Trap Listener

SNMP Trap listening is disabled by default. This is done to ensure that ipMonitor properly co-exists with existing Network management software.

To enable the SNMP Trap Listener:

1. Launch the ipMonitor Configuration Program from the ipMonitor program group.
2. Select the **Communications: Web Server Ports** option.

3. In the **SNMP Trap Listener** section, specify a listening **IP Address** and **Port** (UDP) for all SNMP Trap User Experience Monitors and ensure the **Enabled** check box is selected.

Any agent you configure to send Traps to ipMonitor must use this same IP Address and Port combination.

Conflicts with the Windows SNMP Trap Service:

If the Windows SNMP Trap Service is enabled on the ipMonitor host computer, it is very likely to conflict with ipMonitor's SNMP Trap Listener. Both are bound by default to port 162.

To resolve conflicts with the Windows SNMP trap service:

- Change ipMonitor's SNMP Trap Listener port to one that is unused, then also change the outbound port of all the SNMP agents that will be sending Traps to ipMonitor.
  -or-
- Disable the Windows SNMP Trap Service from the Windows Control Panel/Services interface. There are no adverse effects to disabling the Windows SNMP Trap service unless you are running another SNMP solution on the ipMonitor server that requires use of the Windows SNMP Trap service.

Using filters in the SNMP Trap Monitor:

The **Trap Filtering** dialog box is used to filter incoming Trap PDU information sent to ipMonitor. The SNMP **Community** string acts like a password for SNMP. When ipMonitor receives a Trap from an Agent, it will include the SNMP Community string. If both ipMonitor and the Agent use this same Read-Only string, ipMonitor will continue its "Trap Filtering" and progress to the IP Range test.

The SNMP default communities are:

Private (Read-Write)

Public (Read-Only)

Some SNMP Agents allow you to use non-default Community strings. This is typically done to improve the SNMP security model, often in conjunction with a non-standard SNMP port.

Allowed IP Address Range (start) & (end)
For security purposes, Traps can be accepted based on a range of IP addresses:

For a range, enter the start and end of the range of IP addresses from which SNMP Traps will be accepted.

For a single IP address, enter the same start and end IP address.

Filter using the source address from within the SNMP TRAP packet, not the IP Header
To increase the flexibility of the SNMP Trap QA Monitor IP address filtering, two variations are supported:

If this option is checked, the SNMP Trap QA Monitor will use the IP address specified by the Agent in the incoming Trap packet to perform its **Allowed IP Address Range** validation.

If this option is not checked, the SNMP Trap QA Monitor will use the IP address specified in the IP Header.

Generic Type
The incoming **Generic Trap** field must be one of the predefined SNMPv1 Trap types:

Any indicates that any of the Trap types listed below will be accepted.

coldStart(0) signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

warmStart(1) signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

linkDown(2) signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.

linkUp(3) signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.

authentication-Failure(4) signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.

egpNeighborLoss(5) signifies that an EGP neighbor for whom the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.

enterprise-Specific(6) signifies that the sending protocol entity recognizes that some enterprise-specific event has occurred. The specific-trap field identifies the particular trap which occurred.

Refer to RFC 1157 for more information.

Enterprise OID
Enter the **Object Identifier** that identifies the network management subsystem that generated the SNMP Trap. The OID identifies the object's position in a global object registration tree.

To locate OIDs for your applications and equipment:

Use ipMonitor's database of precompiled MIBs that can be browsed or queried (located in the **Tools** drop-down menu). MIB Information is provided for common Windows and hardware applications.

To expand the default MIB database, use the Custom Database Builder available on the ipMonitor Support Portal to select MIBs from ipMonitor's MIB Repository and perform automated MIB compilations. You can then add the newly-created Custom MIB Database to your ipMonitor installation.

Note: The Custom Database Builder is only available to Licensed ipMonitor customers. For detailed instructions on compiling and importing a MIB database, refer to the Add a Custom MIB Database to your ipMonitor Installation, located in the Customer Portal.

Contact your vendor directly to acquire MIBs for your various applications and equipment.

Get Info

Click the **Get Info** button to query ipMonitor's built-in SNMP database for details about the OID you enter. **Type Information** is ideal for determining what type analysis can be performed in the **Analysis of Test Results** section.

To OID

Click the **To OID** button to convert the readable label of the OID path into its standard numerical notation. For example, clicking the **To OID** button will convert **sysUpTime.0** to **1.3.6.1.2.1.1.3.0**

An Enterprise OID prefix can be specified by using an asterisk as a wildcard character. For example: 1.3.6.1.4.1.*

Anything below the asterisk is accepted. This allows you to configure a single SNMP Trap QA Monitor to accept Traps from multiple SNMP-enabled devices or applications.

Enterprise Specific Kind

The **Enterprise Specific Kind** field is used to isolate vendor specific problems.

If enterpriseSpecific is selected for the Generic Type field, ipMonitor allows you to optionally add one or more Specific Trap Kinds unique to the network management subsystem generating the Trap.

To add more Specific Kinds, click the Add... button, and then click the Or... button for any subsequent entries. This makes it possible to Alert based on more than one Specific Kind of Trap.

SNPP

The Simple Network Paging Protocol Monitor is used to test a SNPP server for availability, as well as its level of responsiveness.

SNPP is used to deliver "pages" to individual paging terminals without the need for modems and phone lines to deliver alphanumeric pages.

The SNPP Monitor:

1. Connects to the Service and waits for the Service to respond.
2. Considers the test successful if the SNPP server responds indicating that it is available within the specified Maximum Test Duration.
3. Safely disconnects from the server upon receipt of the opening response.
4. Considers the test to have failed if the SNPP server fails to respond or responds with an error code indicating that the Service is not available.

Use the SNPP Monitor to test that:

- A SNPP client can open a connection with a SNPP server.
- The server adheres to the SNPP protocol by responding with the correct codes.
- The server responds within a required number of seconds.

SQL: ADO

The ADO Monitor tests the ability to log in to a SQL Server or other supported data source. It effectively ensures that:

- Enough "connection handles" are available.
- The specified account can log in to the database.

Microsoft ActiveX Data Objects (ADO) provides a set of advanced database abstraction classes used by applications to access and interact with data from a variety of sources through an installed OLE Database provider.

The ADO Monitor Wizard is designed to help you configure an ADO Monitor with the least amount of initial input.

Benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The ADO Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

OLE DB Provider Requirements

The ADO Monitor requires that you have the correct OLE DB Provider installed to provide access to the Database Type you wish to use. The following Database Types are supported:

- Microsoft SQL Server
- Sybase SQL Server
- IBM DB2
- IBM Informix
- PostgreSQL
- Oracle
- MySQL
- Other

Note: The "Other" database type allows you to manually configure the ADO Monitor to test many other data sources, such as: SAP DB, FrontBase, FoxPro and LDAP.

Providers have different implementation requirements and guidelines. We recommend consulting the documentation provided by the appropriate third-party vendors before proceeding to install OLE DB Providers.

For basic instructions regarding configuring the supported data base types outlined above, refer to the provider configuration articles available on the ipMonitor Support Portal.

How to Verify Your OLE DB Provider

ipMonitor includes a Universal Data Link file that will launch the Windows Data Link Properties dialog box in order to test connections between the ipMonitor host computer and OLE DB data sources.

For example, the following procedure illustrates how to verify that the SQL Server OLE DB provider is properly installed on the ipMonitor host machine, and that connectivity to the SQL Server can be established:

1. Double-click the **ipm7adotest.udl** file located in the **\ipMonitor** root directory.
2. From the **Provider** tab, select the correct OLE DB Provider from the list. If the required Provider does not appear in the list, it will need to be installed before ipMonitor will be able to connect.
3. From the **Connection** tab, select the SQL Server instance and enter the necessary login and database information.
4. Click the **Test Connection** button. If the test is successful, a **Test Connection succeeded** message box will appear.
5. Click the **OK** button to save the settings.

In the example shown above, Use Windows NT Integrated Security is selected to log on to a Microsoft SQL Server. In other words:

- The SQL Server is configured to use Windows NT authentication to allow access to its data.
- The Account used to log in to the ipMonitor host machine and launch the ipm7adotest.udl file must have the necessary privileges to run the remote procedure call and authenticate to the SQL server.

SQL: ADO – User Experience

The ActiveX Data Object User Experience monitor monitors a SQL Server or other supported data source from the end-user perspective by using synthetic transactions to:

- Test login ability.
- Perform a query.
- Retrieve data.
- Analyze results for correctness.

The Wizard is designed to help you configure a monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- ipMonitor automatically creates the SQL Statement using the information you provide.
- The Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Note1: The ADO - User Experience Monitor requires that you have MDAC 2.6 or greater installed on the ipMonitor host computer. MDAC 2.5 and earlier do not support Named Instances, which are used when more than one instance of SQL Server is running on a machine.

Note2: The ADO Monitor Wizard allows you to configure ADO Monitors quickly and easily. However, if you prefer greater control over the process, you can Clone an existing ADO Monitor and make any required configuration changes manually.

Test Results

- **rows dl**. The total number of rows returned to the monitor for analysis.

SQL ADO Wizard

Step 1: Select Database Type

The following example illustrates the configuration process for creating an ADO – User Experience monitor to monitor the Microsoft SQL Server Database type.

1. Log in to the ipMonitor Administration interface.
2. Click the Monitors menu option, then select Add a Monitor.
3. Select the ADO-User Experience (SQL Query) monitor from the Windows NT/2000 based category and then click the Continue button.
4. Select a Database Type from the list provided.

Only correctly installed OLE DB Providers will be selectable for Monitor configuration. OLE DB Providers that have not been installed on the ipMonitor host machine will appear under the **Unavailable Database Types** heading. If necessary, contact your vendor to acquire the correct OLE DB Provider for your Database Type and install it before continuing.

Selecting the **Other** database type allows you to manually configure the ADO - User Experience Monitor to test many other data sources such as SAP DB, FrontBase, FoxPro and LDAP.

Step 2: Data Source Location

Specify the Server Address of the SQL Server Database you want to monitor.

Use TCP/IP versus Named Pipes

Select this check box to force ipMonitor to use TCP/IP instead of a named pipe to connect to a Microsoft SQL Server database. Type the IP address and port of the server database in the **Server Address** text box. For example, xxx.xxx.xxx.xxx,1433. 1433 is the default port number for SQL servers.

Use Data Encryption

Select this check box to force ipMonitor to encrypt the data transmitted between the ipMonitor host machine and the database being queried.

Specify a Microsoft SQL Server Instance

Select this check box to connect to a named instance of Microsoft SQL Server. Type the instance name in the Server Address text box.

Step 3: Assign Login Credential

Select a credential to use while monitoring. Depending on the data source configured for the ADO Monitor, it is likely that a form of authentication to the data source will be required to connect and/or log in.

Step 4: Select Database

Select the database to be used in the monitor. Depending on the database type, this step may not be displayed.

Step 5: Select Database Table

Select the database table to be used in the monitor.

Show only User Tables

Select this option to display only user-created tables in the Tables list.

Show both User and System Tables

Select this option to display both user-created tables and system tables in the Tables list.

Step 6: Generate SQL Query

ipMonitor uses a SQL statement to query the database. You can supply your own SQL statement, or have ipMonitor generate one automatically based on the table columns that you select.

Automatically generate an SQL Statement from selected Columns

Select this option to list the columns in the database table. The list displays the Data Type and length of each column, and whether the column is allowed to contain a null value.

Select the check boxes next to the columns you want to include in the automatically- generated SQL statement.

Manually supply an SQL Statement

Select this option to enter your own SQL statement in a text box.

Step 7: Analysis of Results

ipMonitor matches the results of the SQL query to the test parameters that you set up here to determine whether the monitor should pass or fail.

Maximum Rows to Retrieve

This value represents the maximum number of rows that the query will be permitted to return to the ADO - User Experience Monitor for analysis. The default value is set to 300.

Examine the number of Retrieved Rows based on a numeric equation

If this option is selected, you must choose an operator and number that will be used to test the number of rows returned by the query. Supported numeric tests are as follows:

Pass if the number of rows is:

- < Less than "X"
- > Greater than "X"
- <= Less than or equal to "X"
- >= Greater than or equal to "X"
- == Equal to "X"
- != Not equal to "X"

Examine Row Content to perform textual or numeric analysis

This option can be used to perform textual or numeric analysis on the data contained in the Column you specified.

If the query result set returns more than 1 Row:

- Each Row in the result set is examined sequentially from first to last
- All configured tests are performed on the Column you specify
- If any condition you specify is met the test passes

Examine Column

When specifying the column to examine, note that column 1 is the first column. Counting is 1-based, not 0-based.

The data in the specified column can be either a string, or a number.

Column Will

Several numeric and text comparison methods are available including Regular Expression and string matches. Pass if the content of the column adheres to any of the following:

- RegEx match - Enter a Regular Expression to match
- RegEx non-match - Enter a Regular Expression not to match
- Substring search - Search for a case sensitive substring
- == Exact match
- != Non-match

Preview

The **Preview** button display the data contained within the columns selected. For easy identification, rows highlighted in red indicate a "fail" scenario. Within the preview window, clicking the Stretch Table button will expand the table to fit all content selected. If you have chosen to view a large number of columns, some of the content may be truncated unless you expand the resulting preview table.

Step 8: Name Monitor

Enter a concise, descriptive name for the new Monitor.

Create Monitor Enabled

After the Monitor is created, it immediately starts querying the Database with the configuration options selected. This option is enabled by default.

Store Monitor Statistics for Recent Activity and Historical Reports

ipMonitor will immediately begin to record test results, which are then used to generate Recent Activity and Historical Reports. This option is disabled by default.

Create

Click **Create** to exit the wizard and access the new Monitor in edit mode. You can make any final modifications to the Monitor in this mode, including setting Timing and Notification parameters.

Manually Configuring the ADO User Experience Monitor

The Test Parameters dialog box is used to specify the parameters the ADO user experience monitor uses to open a connection to the data source.

The example discussed here relates to configuring the ADO User Experience monitor to test connectivity to a Microsoft SQL Server 2000 Database Server. Notes are provided for other OLE DB Providers as appropriate.

Database Type

Select a Database Type from the ADO - User Experience Monitor's list of supported OLE DB providers.

Credential for Monitoring

Depending on the data source configured for the ADO - User Experience Monitor, it is likely that a form of authentication will be required to connect and/or login.

Typically, a Credential will be created and assigned to the ADO - User Experience Monitor in order to impersonate the account information required to access and query the data source.

If a Credential for Monitoring is not assigned, ipMonitor will use the privileges of the current Windows Account assigned to the ipMonitor Service.

To select a Credential:

- Click the Select... button to pop up the Credentials for Monitoring dialog
- Select an existing Credential from the Windows category
- To create a new Credential, click the New Credential button to start the Wizard

Run this test from an external process

Enabling this option allows ipMonitor to continue monitoring the database even if a temporary OLE DB connection problem occurs.

In the example shown below, we are configuring the ADO User Experience Monitor to a test Microsoft SQL Server 2000 Database Server. The following authentication methods are possible:

SQL Authentication
Using SQL Authentication also known "Mixed Mode":

- Provider = sqloledb
- Data Source = ServerName
- Initial Catalog = DatabaseName

A Credential for Monitoring will need to be created and assigned to provide the User Name and Password required to authenticate. Only select the following option within the Usage Restrictions section of the Credential's settings:

- May be used with ActiveX Data Objects (ADO)

Integrated Windows Authentication

Using Integrated Windows Authentication also known as a "Trusted Connection":

- Provider = sqloledb
- Data Source = ServerName
- Initial Catalog = DatabaseName
- Integrated Security = SSPI

Use the AND... button to specify the additional Integrated Security = SSPI parameter.

A Credential for Monitoring is required if the ipMonitor Service account does not have sufficient rights to connect to the database server. Only select the following option within Usage Restrictions section of Credential's settings:

- May be used with Windows Impersonation for use with RPC

Note: For specific configuration details regarding configuration of a Credential to be used with the ADO - User Experience Monitor, see “Credentials Manager” on page 221.

Additional Connection Types

The ADO - User Experience Monitor supports both Named Instance and TCP/IP connection options.

Named Instance

To connect to a Named Instance:

- Provider = sqloledb
- Data Source = ServerName\InstanceName
- Initial Catalog = DatabaseName

If the Named Instance uses SQL Authentication, a Credential for Monitoring will need to be created. If the Named Instance uses Integrated Windows Authentication, a Credential may be required as noted above.

Use the AND... button to specify the Integrated Security = SSPI parameter.

Note: In order to connect to a SQL Server 2000 Named Instance, the ipMonitor host machine must have MDAC 2.6 or greater installed.

TCP/IP Connection to SQL Server 2000

To connect to SQL Server 2000 via an IP Address:

- Provider = sqloledb
- Data Source = xxx.xxx.xxx.xxx,1433
- Initial Catalog = DatabaseName
- Network Library = DBMSSOCN

Parameters to Specify:

- xxx.xxx.xxx.xxx is IP address of the database server.
- 1433 is the default port number for SQL Server. The IP address and port are separated by a comma.
- Use the AND... button to enter Network Library = DBMSSOCN indicating TCP/IP should be used instead of Named Pipes.
- Use the AND... button to enter Encrypt = yes indicating encryption will be used.

SQL Statement

Enter the query statement that will be issued to the Database Server or Data Source.

Note: Do not end the SQL statement with a ";" semicolon. ipMonitor automatically adds the semicolon for you.

Locking Method

Use the Locking Method drop-down selector to specify the locking mechanism that will be placed on the query statement issued to the Database Server or Data Source. By default, the Locking Method is set to "Optimistic".

The following options are available:

- Optimistic - Allows simultaneous editing of a record; locking it only when an update is attempted.
- Batch Optimistic - This option is required only when updating records in batches rather than individually.
- Pessimistic - Immediately locks a record when the retrieval process is initiated.
- Read Only - Prevents data from ever being modified.

Analysis of Test Results

The Analysis of Test Results section is used to validate query results. It controls the number of Rows that will be retrieved and the type of analysis the Monitor will perform on the result set.

Success can be determined strictly by:

- Retrieving up to a Maximum of "x" number of Rows

Further analysis is possible by:

- Examining Row Count
- Examining Row Content

Retrieve a Maximum of "x" Rows

The Retrieve Maximum Rows parameter is used to control the maximum number of rows that the query will be permitted to return to the ADO - User Experience Monitor for analysis. This helps to:

- Control impact on the SQL server or data source being monitored
- Reduce network bandwidth consumed
- Reduce the amount of processing ipMonitor is required to do

Examine the Row Count

The Examine Row Count option can be used to validate results based on the numeric equation you configure.

Number of Rows Retrieved Must Be

Select an operator and enter a number that will be used to test the number of rows returned by the query.

Examine the Row Content

The Examine Row Content option can be used to perform textual or numeric analysis on the data contained in the Column you specify.

When the query result set returns more than 1 Row:

- Each Row in the result set is examined sequentially from first to last
- All configured tests are performed on the Column you specify
- If any condition you specify is met the test passes

Examine Column Number

When specifying the Column Number to examine, note that column 1 is the first column. Counting is 1-based, not 0-based.

Column Will

This equation determines success if the test passes.

Several text comparison methods are available including Regular Expression and string matches:

Note: ipMonitor includes a RegEx Wizard to help create Regular Expressions.

The AND button and the OR button can be used to increase the flexibility of the test.

SQL Server

The SQL Server Monitor opens a connection to the specified SQL server and tests the performance of its subsystems to determine the server's general health. The overall performance of the server is typically dictated by its weakest performing subsystem.

The Monitor's ability to retrieve and analyze data allows an Administrator to:

- Use preconfigured performance counters made available by the Windows Management Instrumentation service to test multiple SQL sever subsystems at once.
- Quickly identify any performance degradation in critical SQL Server components.
- Determine the exact point of failure.
- Take corrective action before outages occur.

Windows Management Instrumentation (WMI) Requirements

For the SQL Server Monitor to properly monitor a SQL Server, Windows Management Instrumentation (WMI) must be enabled and functioning properly. In addition, the remote server must be accessible through an RPC connection in order to run the WMI queries.

Allowing cross domain WMI without local accounts credentials may be used with Windows Impersonation for use with RPC. Credentials using NTLM Authentication Schemes (Windows LT Lan Manager) will function across domains without local accounts.

With the exception of the Minimum SQL Memory (kb) and the Cache Hit Ratio Percentage counters, the default value represents a threshold rate that is not to be exceeded.

Counters are tested in the order that they appear. In the event of multiple counter failures, only the first counter error encountered will be reported.

The SQL Server Monitor's built-in internal sampling helps combat counter spikes. The Monitor will issue the WMI query 5 times, once every second, and then calculate an average based on the query results.

TELNET

The TELNET Monitor tests the ability of a TCP/IP-based Service to accept incoming sessions, as well as its level of responsiveness.

The TELNET Monitor provides a method to monitor the availability of connection-based TCP/IP applications and devices that are not directly supported within ipMonitor by a specific Monitor type.

The TELNET Monitor establishes a TCP/IP connection to the remote resource. After availability has been confirmed, the Monitor safely disconnects.

Use the TELNET Monitor to test that:

- A TCP/IP connection to an application or device can be established.
- The application or device responds within a required number of seconds.

Any connection-based application can be monitored using the TELNET protocol even if the application is they are not directly supported by a monitor type. To test if the service or device is accepting sessions, specify the correct TCP/IP port.

Temperature

The Temperature Monitor uses SNMP communication to assess temperature levels in a specific area. The Monitor's ability to retrieve and analyze the response received from a temperature sensor allows an Administrator to:

- Be notified when abnormal temperature levels are detected.
- Ensure that temperature levels in a specific area remain within acceptable limits.
- Obtain an accurate picture of current temperature levels.

If your server room cooling system fails, temperature levels can climb rapidly in a short amount of time. Being made aware of a temperature problem and dealing with it as quickly as possible is vital to ensuring your critical servers and other network components remain undamaged.

Note: The Humidity, Temperature, Battery and Fan Monitors' default Delays Between Tests While: Up, Warn, Down and Lost settings are slightly different from those of other Monitor types. Due to the high potential for disaster when abnormal conditions are detected, these default settings have been lowered from 300 seconds to 60 seconds between tests.

The Temperature Monitor Wizard is designed to help you configure a Temperature Monitor with the least amount of initial input. There are a number of benefits to this approach:

- Configuration is fast and easy, allowing you to get the Monitor up and running quickly.
- The Temperature Monitor Wizard allows you to test all the parameters you enter along the way to make sure that the Monitor will work as expected immediately upon being enabled to go live in a production environment.

Note: The Temperature Monitor Wizard allows you to configure Temperature Monitors quickly and easily. However, if you prefer greater control over the process, you can Clone an existing Temperature Monitor and make any required configuration changes manually.

Test Results

- **temperature**. The temperature response received from the sensor, displayed in either Fahrenheit (F) or Celsius (C) format.

Temperature Wizard

The following example illustrates the configuration process for creating a Temperature Monitor to communicate with an APC SmartSlot environment sensor.

Step 1: Specify the Location of the Device

1. Log in to the ipMonitor Administration web interface.
2. Click the Monitors menu option, and then click Add Monitor.
3. Select the Temperature Monitor Monitor from the Resource Based category.

Step 2: Select Interface and Monitoring Thresholds

Communication Type

The Simple Network Management Protocol allows the Monitor to perform a lightweight transaction in order to communicate with SNMP-enabled network devices. Select the Management Information Base (MIB) ipMonitor will use to connect to the specified environment sensor:

- **SNMP (American Power Conversion).** The PowerNet MIB is specific to American Power Conversion (APC) Corporation, and is recommended to administrators who wish to monitor temperature levels detected by an APC environment sensor.
- **SNMP (Dell)**. The Dell Environmental Monitoring MIB is specific to Dell Corporation, and is recommended to administrators who wish to monitor temperature levels detected by a Dell environment sensor.
- **SNMP (IBM)**. The IBM MIB is specific to IBM Corporation, and is recommended to administrators who wish to monitor temperature levels detected by an IBM environment sensor.
- **SNMP (Hewlett Packard)**. The Hewlett Packard MIB is specific to Hewlett Packard Corporation, and is recommended to administrators who wish to monitor temperature levels detected by a Hewlett Packard environment sensor.
- **SNMP (Netbotz)**. The NetBotz BotzWare MIB is specific to NetBotz Corporation, and is recommended to administrators who wish to monitor temperature levels detected by a NetBotz environment sensor.
- **SNMP (Powerware)**. The XUPS MIB is specific to PowerWare Corporation, and is recommended to administrators who wish to monitor temperature levels detected by a PowerWare environment sensor.

- **SNMP (Sensatronics)**. The Sensatronics MIB is specific to Sensatronics LLC, and is recommended to administrators who wish to monitor temperature levels detected by a Sensatronics environment sensor.
- **SNMP (Tripp Lite)**. The Tripp Lite MIB is specific to Tripp Lite Corporation, and is recommended to administrators who wish to monitor temperature levels detected by a Tripp Lite environment sensor.
- **SNMP (RFC 1628)**. The RFC 1628 MIB, also known as the UPS MIB, defines objects for managing various uninterruptible power supply (UPS) systems and the environment sensors they support.

Temperature Sensor

Select the desired temperature sensor to monitor from the list provided.

Temperature Unit

Select whether to view the temperature retrieved by the Monitor in either Fahrenheit or Celsius format.

Note: Although it can be changed on a per-Monitor basis, this field displays the Temperature Unit selected within Server Settings. By default, temperature data is displayed using the Fahrenheit scale. Changing the format from Fahrenheit to Celsius, and the other way around, automatically converts the existing Minimum and Maximum Temperature values to the correct number.

Minimum Temperature

Enter the low temperature threshold value that will cause the Temperature Monitor test to fail. By default, the Minimum Temperature threshold is set to 32 degrees Fahrenheit.

Maximum Temperature

Enter the high temperature threshold value that will cause the Temperature Monitor test to fail. By default, the Maximum Temperature threshold is set to 113 degrees Fahrenheit.

Note: You will need to adjust the default value based on the type of temperature sensor and the type of environment being monitored.

Step 3: Create the New Temperature Monitor

Enter a concise, descriptive name for the new Monitor.

WHOIS

The WHOIS Monitor is used to test a Remote WHOIS server for availability, as well as its level of responsiveness.

The WHOIS protocol is used to query WHOIS servers in order to look up registration information for Top Level Domains that are registered with Domain Name Registrars.

The WHOIS Monitor:

1. connects to the Service, performs a fixed request (127.0.0.1) and waits for the Service to respond.
2. considers the test successful if the WHOIS server responds that it is available within the specified Maximum Test Duration.
3. safely disconnects from the server upon receipt of the opening response.
4. considers the test to have failed if the WHOIS server fails to respond or responds with an error code indicating that the Service is not available.

Use the WHOIS Monitor to test that:

- A WHOIS client can open a connection with a WHOIS server.
- The server adheres to the WHOIS protocol by responding with the correct codes.
- The server responds within a required number of seconds.

Chapter 11

Alerts and Notifications

An alert is a collection of actions that act on behalf of a set of Monitors. Alerts allow specific Administrators and departments to watch specific monitors, and determine when and how they are alerted of monitor failures.

ipMonitor's alerts and suite of actions provide the flexibility required to accommodate many different types of notification methods and Recovery actions.

Alert features allow you to:

- Configure each Alert to be responsible for a single Monitor, many Monitors or Groups of Monitors.
- Create any number of actions within each alert.
- Schedule each action independently.
- Specify escalated actions as problems remain uncorrected.

Examples of escalated actions include scenarios such as:

- During work hours, notify Administrators first, and then attempt to fix the problem using a Recovery Action (Reboot Server or Restart Service).
- During non-work hours, attempt to fix the problem using a recovery action, and then contact Administrators if the recovery fails.

How it Works: When a Monitor Detects a Problem

If a monitor detects that the quality of service has degraded, a predefined threshold has been surpassed, a specific content pattern has been detected, or a connection failure has taken place, the following events occur in sequence:

1. Each alert is scanned to find which have been assigned to the failed monitor and to the groups that the monitor belongs to.
2. The **Alert Range** is checked for each action within the alert to determine if the alert should be triggered.
3. The **Alert Schedule** is checked to determine if the action is active for the current time period.
4. The selected notifications for the alert are sent. If there are no notifications selected, the action is not carried out.

Escalating Alerts

ipMonitor supports escalated alerting. By controlling the number of monitor failures that are allowed to accumulate before triggering each action, you can share alerts amongst Administrators with different areas of responsibility, amongst various Recovery Actions, or both.

Scheduling Alerts

Each action supports an independent schedule, based on a week-long calendar. Time periods can be configured in 15-minute intervals.

Credentials

You can set different credentials for each action. This allows you to use specific credentials when executing certain actions that require authentication. Actions can also use the Windows account assigned to the ipMonitor Service as their credential.

Alert Escalation

Often called Ordered Alerting, the ability to escalate alerts makes it easy to share responsibilities among Administrators who have varying levels of responsibility.

The Alert Range parameter located within the Availability section of each configured action determines exactly which Failure Notifications an action will handle.

Example: Notifying a Supervisor After the 6th Failure

You can configure an Alert to only send notifications when very specific failure instances occur.

For example, a supervisor may want to know a resource has not recovered after the 6th failure, but may not want to know about any prior failures. It may be that the supervisor has IT staff to handle such problems. Should the supervisor be alerted, it would mean that either the problem is serious, or the IT staff has failed to respond to the Alerts in a timely manner.

To carry out this scenario:

- The Monitor must be configured to trigger at least six Alerts. This ability is controlled by the **Maximum Alerts to Send** setting.
- The IT staff's Alert Range setting should be set to **1-5**, meaning that the IT staff would receive the first five alerts. Or possibly, the five Alerts could be divided amongst two or three IT staff.
- The supervisor's **Alert Range** setting would be set to **6**. He or she would only receive the sixth Alert.

By default, the Alert Range parameter is set to 1-, meaning:

- Send all Alerts
  -or-
- Send 1 through to "n" as determined by the Monitor's Maximum Alerts to Send parameter.

Timing Considerations

If time delays are likely to occur before a resource responds or is processed, test durations must take this into consideration.

For example, setting the **Maximum Test Duration** setting for a POP3 User Experience Monitor to 60 seconds will produce intermittently incorrect results. The mail server could take up to 15 minutes to move an incoming message from the inbound queue to the mailbox during peak times.

Although extreme, this example illustrates how important timing considerations can be to alert escalations.

Another situation to consider:

When creating a **Reboot Server Alert** to follow a **Restart Service Alert**, you would want to take into consideration the length of time required to actually restart the Service and for ipMonitor to confirm Recovery. If the specified time period is not long enough, the computer might be unnecessarily rebooted.

In this example, the potential delay in restarting the service must be accounted for as part of the testing interval for the **Delays Between Tests While: Down** setting in the Monitor's configuration.

Failure and Alerting Process

ipMonitor processes each alert based on the settings specified during the monitor configuration.

The parameters entered in a Monitor's Timing section allow you to intensify or lessen testing during each of a Monitor's four testing states: Up, Warn, Down and Lost.

Notification Control settings determine how many test failures must occur before an Alert is sent, as well as the maximum number of Alerts that will be sent.

This example illustrates how the **Timing** and **Notification Control** settings affect the failure and alerting process.

Timing Settings :: Delays Between Tests While

Up	30 seconds
Warn	30 seconds
Down	60 seconds
Lost	30 seconds

Notification Control

Accumulated Failures per Alert	3
Maximum Alerts to Send	3

The table below outlines changes in Failure Count and Monitor State as the Monitor progresses from a Warn to a Lost state. A monitor will advance from a Fail to a Lost state when the maximum number of Alerts has been processed.

Failure Count	State	Action	Time Elapsed
1	Warn	None	0:00
2	Warn	None	0:30
3	Fail	Alert	1:00
4	Fail	None	2:00
5	Fail	None	3:00
6	Fail	Alert	4:00
7	Fail	None	5:00
8	Fail	None	6:00
9	Fail	Alert	7:00
10	Lost	None	7:30

Using the Downtime Simulator to Preview the Process

Each Monitor has a **Downtime Simulator** menu option that will demonstrate the entire alerting process from a configured **Start Time** and **Duration**. The primary purpose of the Downtime Simulator is to test alert coverage for a Monitor at a specific time of day during any day of the week. It does this by processing every action that can be triggered by the Monitor across all Alerts.

Scheduling Alerts

Independent scheduling is supported on a per-Action basis:

- Schedules are based on a weeklong calendar.
- Time periods can be configured in 15-minute blocks.
- Any possible combination of time intervals can be scheduled.

This independent scheduling system provides IT departments a high degree of flexibility. Within the same alert, during work hours you can configure actions to be sent directly to your email or pager, so you can take action yourself. After hours, you might choose to run additional diagnostic scripts, or automatically launch a recovery action and log the event.

Weeklong Availability Calendar

The graphical availability display shows configured time intervals. The green, darker blocks represent active time periods. The gray, ligheter blocks show inactive time periods.

Click a day of the week or a time block to display the weeklong calendar.

You can toggle individual 15-minute intervals or entire horizontal rows. The **Morning** and **Afternoon** buttons allow you select part of the day or the entire day.

Click the **Select Day to Overwrite** list to choose another day of the week, and then click the **Copy** button to duplicate your settings and fill in the time blocks for other days of the week.

Customizing Notifications Using Tokens

Alert actions are fully customizable using tokens:

- When an Action is carried out, Tokens are replaced with dynamic content.
- The detailed Token List and convenient Token Selector make it easy to quickly build dynamic Alert strings when configuring your Alert.

Date, Time, and Formatting Tokens

Insert the following Tokens into your action notifications to obtain detailed date and time information.

Token Name	Description	Sample Return Value
%date%	Date (yy-mm-dd)	04-03-02
%dday%	Day (dd)	17
%mmon%	Month (mm)	07
%monthtext%	Month (full text)	January
%monthtext3%	Month (three letters)	Jan
%week%	Week in current month (one digit)	1
%weekday%	Weekday (one digit, Sunday = 0)	4
%weekdaytext%	Weekday (full text)	Friday
%weekdaytext3%	Weekday (three letters)	Fri
%year%	Year (yyyy)	2004
%yyear%	Year (yy)	04
%time%	Time (hh:mm::ss) based on 24-hour clock	20:25:28
%rfc822date%	Date/time in email format	Tue, 02 Mar 2004 20:25:28 -0500
%%	Percent	%

Monitor Information Tokens

Insert the following Tokens into your Alerts to obtain Monitor-specific information, such as Monitor Name, Type, Duration of Monitor failure, and so on.

Token Name	Description	Sample Return Value
%monitorid%	Monitor ID	589478484027
%monitorname%	Monitor Name	HTTP - Website
%monitortype%	Monitor Type	ado
%monitoravail%	Monitor available time (%)	99.95
%monitorcoverage%	Monitor coverage time (seconds)	174697
%monitorfailures%	Monitor Failures	0
%monitorcriticals%	Monitor Failures - Critical	0
%monitorcritstoalert%	Critical Alert	3
%monitorstatus%	Last Monitor Status	could not obtain an IP address for the device;
%monitorlastrun%	Date / Time Monitor Last Run	Sun, 21 Dec 2003 17:29:10 -500
%monitordowndate%	Date / Time Monitor Reported Failure	Sun, 21 Dec 2003 17:29:10 -500
%monitormaxtest%	Maximum Test Duration (seconds)	300
%monitoralertmax%	Maximum Alerts to Send	3
%monitoralertno%	Alert Number	2
%monitoralertssent%	Number of Alerts Sent	1
%monitordownlength%	Duration of Monitor Failure	0.80 minutes
%monitoruplength%	Total Monitor Up Time	2 days, 2 hours, 2.70 min
%monitorstate%	Current Monitor State (text)	down
%monitorstatenum%	Current Monitor State (number)	1
%monitortestup%	Delay Between Tests While Up (seconds)	300
%monitortestwarn%	Delay Between Tests While Warn (seconds)	300
%monitortestdown%	Delay Between Tests While Down (seconds)	300
%monitortestlost%	Delay Between Tests While Lost (seconds)	300
%monitor[addr]% %monitor[port]% %monitor[target]% %monitor[info/logfile]%	Monitor Configuration Data from the Branch found in Popup XML	10.25.0.10 53 INTRANETSRV Security

Token Name	Description	Sample Return Value
%monitortag[...]%	Value of Tag Name Specified	Brian Smith, cell: 555-9876

%monitor[...]% may contain other values in the branch displayed using the Popup XML feature. These fields are specific to the Monitor.

%monitortag[...]% will display the value of a custom Tag for the specific Monitor. The Name of the Tag is entered within the square brackets [ ].

Alert and Action Tokens

Insert the following tokens into your alerts to obtain alert-specific information:

Token Name	Description	Sample Return Value
%parentalertname%	Returns the name of the alert this action belongs to.	Night Crew
%actionname%	Returns the name of the action	Internal Helpdesk - Simple Email
%action[sendmail/emailto]% %action[emailfrom]%	Returns the specified configuration data for the action	admin@xyzcompany.com ipm7@xyzcompany.com
%actiontag[...]%	Returns the value of the specified action tag	http://intranet. xyzcompany.com/ recovery.aspx

%action[...]% may contain other values in the branch displayed using the Popup XML feature. These fields are specific to the action. In cases where the xml branch below contains a list of values, only the first value is retrieved. For example: `%alert[sendmail/emailto]%`.

%actiontag[...]% will display the value of a custom Tag for the specific action. The Name of the Tag is entered within the square brackets [ ].

System Tokens

Insert the following Tokens into your Alerts to obtain system-specific information, such as the ipMonitor Server Name, CPU utilization by the ipMonitor process, available drive space, and so on.

Token Name	Description	Sample Return Value
%instancename%	ipMonitor Server Name	ipMonitor Server [PRIMARY]
%processcpu%	ipMonitor CPU Utilization	56.78 seconds
%processuptime%	ipMonitor Uptime	3.81 hours
%processavg%	ipMonitor CPU Load	0.40%
%sysmemavail%	Physical Memory Available	359.83 MB
%sysswapavail%	Commit Memory Available	535.78 MB
%ipmdriveavail%	ipMonitor Drive-Space Available	26.15 GB

Content Generator Token Restrictions

The Content Generator has access to `%monitor[...]%` and `%monitortag[...]%`, but does not have access to `%alert[...]%` or `%alerttag[...]%`.

Chapter 12

Action Types

Actions can be scheduled based on a weeklong calendar. For more information, see Scheduling Alerts” on page 177.

You can create the following types of actions:

- Automatic Report
- Custom Email
- Event Log
- External Process
- Net Send Broadcast
- Reboot Server
- Restart Service
- Simple Beeper
- Simple Email
- SMS Numeric Pager
- SMS Text Pager
- SNMP Trap
- Text Log

Automatic Report

The Automatic Report Alert emails a Recent Activity Report to a specified recipient or group of recipients. The Recent Activity Report consists of uptime and downtime information as well as any failure events for the last 24 hours.

The Automatic Report Alert:

- Shows the network's behavior leading up to the Alert being triggered and before responding to the problem.
- Can be sent to multiple recipients.
- Supports ipMonitor Alert Tokens.
- Supports setting an Optional SMTP Relay Server within Server Settings to ensure that email Alerts are accurately delivered.
- Supports different types of email-enabled devices.

Use the Automatic Report Alert to:

- Examine a Recent Activity Report in order to analyze a problem immediately after it has occurred.
- Send custom Failure and Recovery Alerts using text and ipMonitor Tokens.

Email Alert messages are not stored by ipMonitor. If a mail server is unavailable to receive the email Alert, it will be discarded. The Optional SMTP relay server field within Server Settings can be used to ensure that email Alerts are successfully delivered to the intended recipients. ipMonitor will attempt to relay messages through this server first.

Should the SMTP relay server connection fail, or not be specified, then ipMonitor will use MX records through DNS queries to find a list of potential mail servers. If a DNS Server has been specified in the "Optional DNS override server (for MX records)" section under "Server Settings", then ipMonitor will connect to this DNS server to retrieve MX record information for the recipient domain. If a server is not specified, ipMonitor will use the DNS Server(s) configured for the ipMonitor server's network connection. Once the MX records are retrieved, ipMonitor will attempt to connect to each server listed, in order of MX preference. The relay procedure will complete with a successful transmission to one of the potential relay servers or will exhaust the MX records and fail to relay the message.

Custom Email

The Custom Email Alert sends a fully configured email message to a list of recipients.

The message body, subject line and email headers can all be completely customized in accordance with the RFC 822 specification, which defines a standard format for electronic messages consisting of a set of header fields and an optional body.

Messages can be made complex and rich with formally-structured components of information or be kept small and simple, with a minimum of such information.

The Custom Email Alert:

- Can be sent to multiple recipients.
- Uses the RFC 822 Standard for the Format of ARPA Internet Text Messages.
- Supports ipMonitor Alert Tokens.
- Supports setting an Optional SMTP Relay Server within Server Settings to ensure that email Alerts are accurately delivered.

Use the Custom Email Alert to:

- Integrate email Alerts into the Internal Help / Ticket systems within a corporate network infrastructure.
- Send custom Failure Notifications, Recovery Notifications and Information Messages using text and ipMonitor Alert Tokens.

Event Log

The Event Log Alert writes an entry to the Windows NT/2K/XP/2003 Application Event Log of the ipMonitor host machine.

The Event Log Alert:

- Stores events on the ipMonitor host machine for security reasons.
- Does not require further Alert Parameters configuration.
- Supports designating Error, Success, Warning and Information Event Types.
- Supports passing ipMonitor Alert Tokens to define the Event Description string.

Use the Event Log Alert to:

- Log fully customized Failure Notifications, Recovery Notifications and Information Messages using text and ipMonitor Alert Tokens.

External Process

The External Process Alert runs a third-party executable program or script with any required parameters. If an Alerting Credential is not defined, the Alert will use the current Windows account assigned to the ipMonitor Service.

The External Process Alert:

- Supports setting Environment Variable names and values that may be read by the executable file when it is started.
- Supports using a Credential to transmit account and password information.
- Supports passing Alert Tokens on the command line to control execution of the executable/batch file/script.
- Requires Administrator privileges to configure.

Use the External Process Alert to:

- Restart failed applications.
- Perform diagnostics.
- Back-up files.
- Run scripts.
- Pass Failure and Recovery messages on the command line to the executable file, batch file or script.

Net Send Broadcast

The "Net Send" Broadcast Alert causes a "pop up" message to display on the desktop of a specified network machine.

The "Net Send" Broadcast Alert:

- Supports passing ipMonitor Alert Tokens to define the message string.
- Supports NetBIOS name or IP address for the destination 'Net Send' message.
- Supports using a Credential to transmit account and password information.
- Can send custom Failure, Recovery and Information Messages using text and ipMonitor Alert Tokens.
- Requires Administrator privileges on the target machine.

Reboot Server

The Reboot Server Alert Recovery Action attempts to reboot a Windows workstation or server computer when a Monitor encounters a problem.

The Reboot Server Alert:

- Uses the Recovery Parameters defined during Monitor Configuration.
- Supports using a Credential defined during Monitor Configuration.
- Can service many individual Monitors because Recovery Parameters are passed to the Recovery Alert by the failing Monitor.

Use the Reboot Server Alert to:

- Remotely reboot a Windows workstation or server computer.
- Configure escalated alerting and attempt to reboot a workstation or server after a recovery application has been run to restore service, or the Restart Service Action has been carried out.

The machine to be rebooted is defined in the failing Monitor's configuration settings, under the **Recovery Parameters** section. If a specific User Account and Password is required for this action to be performed, the **Credential for Recovery** selected during Monitor configuration will be used.

Restart Service

The Restart Service Alert Recovery Action attempts to restart a Service or list of Services on the specified Windows workstation or server computer when a Monitor encounters a problem.

The Restart Service Alert:

- Attempts to restart the Services defined during Monitor Configuration within the Recovery Parameters section.
- Supports restarting Services with Dependencies.
- Supports using a Credential defined during Monitor Configuration.
- Can service many individual Monitors because Recovery Parameters are passed to the Recovery Alert by the failing Monitor.

Use the Restart Service Alert to:

- Remotely restart a Windows NT/2000/XP/2003 Service or list of Services.

Both the hostname of the server / workstation, and the Windows Services to be restarted are defined in the failing Monitor's configuration settings, under the Recovery Parameters section. If a specific User Account and Password is required for this action to be performed, the Credential for Recovery selected during Monitor configuration will be used.

Note: If a Service has any Dependencies assigned, they must be included in the list of Services. Otherwise, the Recovery Action will not be able to complete successfully.

Simple Beeper

The Simple Beeper Alert sends a numeric message to a simple numeric pager by simulating touch-tone key presses.

The Simple Beeper Alert:

- Can only send messages made up of numbers and spaces.
- Uses TAPI or Direct Port Access to communicate with a modem.
- Can set a delay period after the modem has connected with the provider, before "keying" in the message.
- Supports selectable COM Ports.
- Supports ipMonitor Alert Tokens.

Use the Simple Beeper Alert to:

- Send Failure and Recovery Notifications to a simple beeper using numerical values and ipMonitor Alert Tokens that contain numeric-only data.

Beeper Hardware Requirements

The Simple Beeper Alert requires the following hardware to be installed on the ipMonitor host computer:

- A COM Port for your modem.
- A Hayes-compatible Modem 2400 baud or faster.
- A telephone line that will not be used by any other device when ipMonitor needs to page administrators.

The telephone line you use for ipMonitor cannot be shared with a Remote Access Server (RAS). Even when idle, the RAS owns the communication port in order to watch for and connect to incoming callers.

Simple Email

The Simple Email Alert sends a dynamically formatted email that displays the Date, Time, Monitor Name, Monitor Type, Monitor Address, Alert Name, Reason for Alert, and any custom data such as that trapped by Information Alerts.

The Simple Email Alert:

- Can be sent to multiple recipients.
- Allows message formatting from a selectable list of options: To, From, Date, Subject, and Message Body.
- Allows individual Message Body content configuration for Failure Messages, Recovery Messages and Information Messages.
- Supports ipMonitor Alert Tokens.
- Supports setting an Optional SMTP Relay Server within Server Settings to ensure that email Alerts are accurately delivered.

Use the Simple Email Alert to:

- Format and deliver a text email message using data generated by ipMonitor when the Alert is triggered on behalf of a Monitor or Group of Monitors.
- Send custom Failure Notifications, Recovery Notifications and Information Messages using text and ipMonitor Tokens.

Note: Email Alert messages are not stored by ipMonitor. If a mail server is unavailable to receive the email Alert, it will be discarded. The Optional SMTP relay server field located within Server Settings can be used to ensure that email Alerts are successfully delivered to the intended recipients. Server Settings can be accessed from the Configuration tab..

SMS Numeric Pager

The SMS Numeric Pager sends a numeric message via a mobile service provider to a pager device capable of receiving a SMS message. Messages can only be made up of numbers, spaces, and depending on your pager model and wireless provider, a limited number of punctuation characters. Most pagers will only accept simple punctuation such as dashes, commas, and periods. Accented characters and other special symbols will not display properly.

The SMS Numeric Pager:

- Uses TAPI or Direct Port Access to communicate with a modem.
- Supports entering a password for pager services that require a password.
- Supports pausing the dial sequence, for example while your phone system selects an outgoing phone line.
- Allows full control over modem settings: COM Port, Baud rate, Data Bits, Parity, Init String and Dial String, as well as forcing the modem to behave as low-speed modem.
- Supports ipMonitor Alert Tokens.

Use the SMS Numeric Pager to send custom Failure and Recovery Notifications to a pager or cell phone that supports the given paging protocol, using numerical values and ipMonitor Tokens containing numeric-only data.

Supported Paging Protocols

ipMonitor supports two paging protocols:

- TAP. Telocator Alphanumeric input Protocol (TAP) is a paging protocol used to transmit up to a thousand 7-bit characters to an alphanumeric pager or cell phone. It is used primarily in North America to take advantage of TAP/SMS numerical paging.
- UCP. Universal Computer Protocol (UCP) is the primary paging protocol used by European network providers. This protocol is implemented to run over TCP/IP and X.25 networks.

SMS Pager Hardware Requirements

The SMS Numeric Pager Alert requires the following hardware to be installed on the ipMonitor host computer:

- A COM Port for your modem.
- Hayes-compatible Modem that is 2400 baud or faster.
- A telephone line that will not be used by any other device when ipMonitor needs to page administrators.

Should the telephone line be in use when ipMonitor attempts to send an Alert, the number of times ipMonitor will retry the connection is determined by the value specified in the Dial Attempts field.

The telephone line used for ipMonitor cannot be shared with a Remote Access Server (RAS). Even when idle, the RAS owns the communication port in order to watch for and connect to incoming callers.

Before configuring the SMS Numeric Pager, you may want to contact your paging service provider to obtain necessary configuration details. Paging services most often accept pages through the use of operator dispatch: the operator types in a message, transmits it to their server, and then to your pager. Most paging services also have the ability to receive messages by modem, which are in turn broadcast by their wireless telecommunications equipment. You will want to ensure that pages generated by ipMonitor are sent to a modem and not a human operator.

SMS Background

SMS is a text message service that enables short messages of no more than 160 characters in length to be sent and transmitted to and from a pager, cell phone or IP address. Unlike paging, but similar to e-mail, short messages are stored and forwarded at SMS centers, allowing you to retrieve them at a later time. SMS messages are sent to the pager or cell phone over the system's control channel, which is separate from the voice channel.

SMS Text Pager

The SMS Text Pager Alert sends a text message to an alphanumeric pager or digital phone with Short Message Service (SMS) support.

Use the Simple SMS Text Pager to send custom Failure Notifications, Recovery Notifications and Information Messages to an alphanumeric pager or cell phone using text and ipMonitor Alert Tokens.

ipMonitor supports three different SMS text pager protocols:

- SMS Text Pager (GSM)
- SMS Text Pager (TAP and UCP)

SMS Text Pager (GSM)

The SMS Text Pager: GSM Alert:

- Is widely used to take advantage of GSM/SMS mobile communication.
- Works with a majority of GSM modems.
- Can send a maximum of 5,049 characters per message.
- Uses Direct Port Access to communicate with a modem.
- Supports pausing the dial sequence, for example while your phone system selects an outgoing phone line.
- Allows full control over modem settings: COM Port, Baud rate, Data Bits, Parity, Init String and Dial String, as well as forcing the modem to behave as low-speed modem.
- Supports ipMonitor Alert Tokens.

GSM Hardware Requirements

SMS Text Pager:GSM Alerts requires you to have the following installed on the ipMonitor host computer:

- A GSM Mobile network subscription.
- A COM Port for your modem.
- A Hayes-compatible GSM/GPRS Modem capable of supporting AT commands.

GSM was originally developed as the European communication standard for digital mobile and cellular service. However, it is now present in more than 160 countries and is widely considered one of the world's main digital wireless standards. GSM uses narrowband Time Division Multiple Access (TDMA), which allows eight simultaneous calls on the same radio frequency. It is used on the 900 MHz and 1800 MHz frequencies in Europe, Asia and Australia, and the MHz 1900 frequency in North America and Latin America.

SMS Text Pager (TAP and UCP)

The SMS Text Pager: TAP and UCP alerts send a text message via a mobile service provider to an alphanumeric pager or digital phone with Short Message Service (SMS) support.

The SMS Text Pager: UCP Alert:

- Uses TAPI or Direct Port Access to communicate with a modem.
- Supports entering a password for pager services that require a password.
- Supports pausing the dial sequence, for example while your phone system selects an outgoing phone line.
- Allows full control over modem settings: COM Port, Baud rate, Data Bits, Parity, Init String and Dial String, as well as forcing the modem to behave as low-speed modem.
- Supports ipMonitor Alert Tokens.

TAP and UCP Hardware Requirements

The SMS Text Pager Alert requires the following hardware to be installed on the ipMonitor host computer:

- A COM Port for your modem.
- A Hayes-compatible Modem that is 2400 baud or faster.
- A telephone line that will not be used by any other device when ipMonitor needs to page administrators.

SMS is a text message service that enables short messages of no more than 160 characters in length to be sent and transmitted to and from a pager, cell phone or IP address. Unlike paging, but similar to e-mail, short messages are stored and forwarded at SMS centers, allowing you to retrieve them at a later time. SMS messages are sent to the pager or cell phone over the system's control channel, which is separate from the voice channel.

SNMP Trap

The SNMP Trap Alert sends an SNMP Trap to the SNMP manager specified. Its function is to send the Alert text to an SNMP manager where it is analyzed by string pattern matching rules, then reported and recorded by your existing network management software.

The SNMP Trap Alert:

- Sends an SNMP Trap to the SNMP management application of your choice.
- Supports both enterprise-specific and generic Trap types such as Cold Start, Warm Start, Link Down, and so on.
- Supports ipMonitor Alert Tokens.

Use the SNMP Trap Alert to:

- Integrate ipMonitor into any existing network management software you already run.
- Send custom Failure Notifications, Recovery Notifications and Information Messages using text and ipMonitor Alert Tokens.

Quick Set up

To quickly configure the SNMP Trap Alert in a simple manner, enable it to send a "link down" message for failures, and a "link up" message for recoveries.

The default SNMP OID is the is the "system" object from MIB-II (RFC 1213):

1.3.6.1.2.1.1

Using this Alert with HP OpenView

Note: If you are using this Alert with HP Openview, enter the following SNMP OID into the "Message Content OID" field: 1.3.1.4.1.11.2.17.1

If you are not receiving traps, you may have to input the SNMP OID preferred by the management software.

Text Log

The Text Log Alert records a pre-defined entry to a text log at a specified location.

The Text Log Alert:

- Supports using Local or UNC paths to the directory where the log file is created / located.
- Supports passing ipMonitor Alert Tokens to define the Event string.

Use the Text Log Alert to:

- Create a log file showing activity pertaining to a single Monitor or a Group of Monitors.
- Create a log file that can be analyzed by other software applications of your own design.
- Log fully customized Failure Notifications, Recovery Notifications and Information Messages using text and ipMonitor Alert Tokens.

Chapter 13

Information Alerts

Information Alerts are a special ipMonitor Notification type. Their purpose is to locate and retrieve information within structured data sources that contain variable data.

Information Alerts are only triggered by the File Watching, Event Log and SNMP Trap Monitors. For these Monitor types that produce variable results, Information Alerts are able to report exactly why a Monitor fails, as opposed to only revealing that a failure occurred.

Information Alerts are able to:

- Search data sources with variable content.
- Capture results based on one or more specified criteria.
- Arrange data into a specific format.
- Push reformatted data into Alert messages.

Configuring Information Alerts starts in the Monitor configuration interface by adding one or more Search Scenarios.

A Search Scenario:

- Is a search pattern articulated through a Regular Expression.
- Is used when parsing the data source to locate patterns of information.

Regular Expressions can be constructed using ipMonitor's RegEx Wizard. For more information, refer to RegEx Wizard.

After a Search Scenario captures information from the data source, it is passed to a Content Generator.

A Content Generator:

- Is assigned in the Monitor settings.
- Is used to format captured data for readability or layout.
- Sends formatted data to Information Alerts.

Content Generator

The Content Generator is used to format data into messages for Information Actions.

The Event Log, SNMP Trap and File Watching Monitors support the use of Regular Expressions to capture variable data such as:

- An Event Log description.
- Variable-binding data from an SNMP Trap.
- A line from a log file.

Captured data is then passed to a Content Generator for parsing into a message. Additional information relating to the Monitor such as the Event timestamp or the source IP address of a received SNMP Trap can also be included in the message.

After the message is structured correctly, it may be passed to any number of actions that are configured to act on the specific Monitor that triggered the Alert.

A Content Generator contains three elements:

- **Name**. Identifies the Content Generator
- **Value**. Defines the layout of the "captured" data. This will be the format of the Alert message.
- **Coalesce Separator**. specifies the string used to terminate each captured data "element". By default, this is \r\n (CRLF)

The default Content Generator in ipMonitor generates a message that contains the number of matches captured by the monitor in the data source.

You will need to create a user-defined Content Generator to return an Information Alert message in a customized format. Customized messages can be structured for different purposes, for example, for use with email actions, text logs or SNMP Traps.

Information Action Messages

Within the configuration interface for actions, the **Notification Content - Information Messages** section is used to control output of Information Action messages. The **Send Information Notifications** option must be selected for the Alert to act on Information Actions.

To insert Messages formatted by Content Generators into actions, add the following Alert Token in the **Information Message Body** section:

```
%generatedcontent%
```

The following action types fully support Information Action messages:

- Simple Email
- Customized Email
- Net Broadcast
- Event Log
- Text Log
- SNMP Trap

Text Messaging actions are limited by the display capabilities of the target device. This should be taken into consideration when creating Content Generators for use with text messaging devices through the following actions:

- SMS Text Message: TAP
- SMS Text Message: UCP

The following actions do not act on Information Action messages:

- SMS Numeric Message: TAP
- SMS Numeric Message: UCP
- External Process
- Reboot Server
- Restart Service

Additional Content Generator Tokens

The SNMP Trap, Event Log and File Watching Monitors support supplemental Tokens that can be referenced in a Content Generator to provide additional information in the action message. These Tokens can be divided into two categories: Numeric Tokens and Property Tokens.

Numeric Tokens

Numeric Tokens allow you to retrieve specific text matches, or 'captures', located by a Regular Expression search. The syntax for Numeric Tokens is: `%capture[#]%`.

For example, consider a file watched by the File Watching Monitor, which contains the following entry:

```
1/30/2006 7:45:08 AM ERROR: The application failed to start.
REASON: Required resource myapp.dll could not be located.
```

Within the File Watching Monitor, the following Regular Expression has been entered:

```
ERROR\: (.*?) REASON\: (.*?)
```

In this example:

- The %capture[1]% Token would resolve to: "The application failed to start."
- The %capture[2]% Token would resolve to: "Required resource myapp.dll could not be located.".

Assuming an Information Action was correctly configured, this information would be included in the body of the message.

Note: Variables are enumerated in the same order they are defined in the RegEx. When more than one RegEx Search Scenario is configured for a Monitor, variables are enumerated starting in the first Regular Expression and counting through the last Regular Expression. For example:

First Regular Expression: %capture[1]%, %capture[2]%, %capture[3]%

Second Regular Expression: %capture[4]%, %capture[5]%, and so on.

Property Tokens

Property tokens allow you to access additional parameters describing an Event Log entry, a file entry, or an SNMP Trap. The syntax for Property Tokens is `%capture[property_name]%`.

For example:

%capture[timewritten]% (Event Log Monitor specific)

%capture[bindings]% (SNMP Trap Monitor specific)

%capture[offset]% (File Watching Monitor specific)

Additional Content Generator Property Tokens are available to the Event Log, File Watching and SNMP Trap Monitors.

Event Log Tokens

The following table contains the Content Generator Property tokens available to Event Log monitors.

Token Name	Sample Return Value
%capture[category]%	2
%capture[computername]%	MISWKSTN
%capture[logfile]%	System
%capture[sourcename]%	W3SVC
%capture[timewritten]%	20040209102741.000000-300

SNMP Trap Tokens

The following table contains the Content Generator Property Tokens available to SNMP Trap monitors.

Token Name	Sample Return Value
%capture[agent-addr]%	10.1.2.3
%capture[community]%	public
%capture[enterprise]%	1.3.6.1.4.1.674.10892.1
%capture[generic-trap]%	enterpriseSpecific (6)
%capture[specific-trap]%	1053
%capture[time-stamp]%	9212200
%capture[1.3.6.1.2.1.1.0]%	Dell OpenManage Temperature Status [snmp: trap] is down
%capture[bindings]%	mib-2.system.0: SNMP Trap Monitor :: Dell OpenManage Temperature Status[snmp: trap] is down
%capture[bindings-raw]%	1.3.6.1.2.1.1.0: SNMP Trap Monitor :: Dell OpenManage Temperature Status[snmp: trap] is down

File Watching Tokens

The following table contains the Content Generator Property Tokens available to File Watching monitors.

Token Name	Sample Return Value
%capture[offset]%	23698

Note: `%capture[1.3.6.1.2.1.1.0]%` will display the value of the specified OID entered within the square brackets [ ]. A wildcard character (*) cannot be used to specify an OID prefix.

Chapter 14

Log Files

About Log Files

ipMonitor records a number of separate log files to provide Administrators with the necessary information required for diagnostic and troubleshooting purposes. Use the log files generated by ipMonitor to:

- Obtain information about internal ipMonitor events, such as denied access requests, Alert usage, Monitor state change, and so on.
- Retrieve diagnostic information.
- Access information relating to SNMP Traps received by ipMonitor.
- Track all generated Reports.

Generated Log Files

Depending on your ipMonitor configuration, some or all of the following log files may be viewable from the Logs page:

- `ipm.log`
- `runtime.log`
- `runtime_bkg_reports.log`
- `snmptrap.log`

`ipm.log`

The `ipm.log` file provides a record of events that have occurred internally within ipMonitor. The following optional events may be recorded into the ipm.log file:

- Record ipMonitor Startup and Shut Down.
- Record Access Attempts by Locked Out IP Addresses.
- Record Invalid HTTP Requests.
- Record Denied Access Requests (User Rights, Failed Login, Improper Credential).
- Record Attempts to Use Expired User Sessions.
- Record User Session Creation.
- Record User Session Termination.

- Record User Session Expiration (Due to Inactivity).
- Record Tests Failures.
- Record Test Recovery from Failure State.
- Record Monitor State Change.
- Record Alert Use.
- Record Alert Being Skipped.
- Record Missing Action Availability.
- Record Action Usage.
- Record Action Being Skipped.

runtime.log

As a diagnostic procedure, earlier versions of ipMonitor prior to 7.x could be run at the command-line in what was referred to as Desktop Mode. When running ipMonitor in this mode, certain diagnostic information was written to the console. Recent versions of ipMonitor now include the `runtime.log` file to provide the same diagnostic information.

runtime_bkg_reports.log

The `runtime_bkg_reports.log` file is created by the Background Report Generator to track all the Reports generated. The log file is overwritten each night with updated information.

snmptrap.log

The `snmptrap.log` file is used to record information relating to SNMP Traps that have been received by ipMonitor 8. It will only be displayed if there are entries in the log file. The following optional events may be recorded in the snmptrap.log file:

- Record Received SNMP Traps Not Expected by Any Configured Monitors.
- Record Received SNMP Traps Expected by Configured Monitors.
- Record the Contents of Any Received SNMP Trap in snmptrap.log.

Chapter 15

Maintenance Schedules

Maintenance Schedules allow Administrators to temporarily disable monitoring of certain resources, for example to perform data back-ups or Service restart actions.

Maintenance Schedules include the ability to identify all Groups and Monitors that would be affected by the scheduled downtime. Just prior to maintenance, ipMonitor suspends the affected Monitors, ensuring that planned maintenance does not trigger Alerts or display negatively in Historical Reports. After maintenance, ipMonitor reactivates the affected Monitors.

Features include:

- Maintenance can be scheduled based on rules similar to those used by Microsoft Outlook.
- Maintenance can be scheduled while ipMonitor performs routine actions. The ability is provided to define a list of actions using the Reboot server, Restart Service or Pause commands. Credentials can be configured as required on a per-action basis.
- Maintenance can be scheduled to disable Monitors while actions outside of ipMonitor occur. For example, you might need to disable
- Detailed scheduling options allow you full control over the start, end, monitoring of a SQL database while a scheduled backup is performed.frequency and duration times of the Maintenance Schedule.

Internal Maintenance

ipMonitor's Internal Maintenance allows you to perform recurring maintenance actions such as rolling log files and backing up configuration settings.

Features include:

- Internal Maintenance Actions can be scheduled to occur on specified days of the week.
- A Credential can be created and used to encrypt the Credentials Database for backup purposes.
- Supports using ipMonitor Tokens to designate file names.
- Log files are compressed using Zip format.
- Log files can be automatically rolled on a daily basis.

Standalone Backup

To archive your ipMonitor configuration settings without scheduling recurring internal maintenance, click the **Backup Now** button located on the Internal Maintenance submenu bar.

Chapter 16

Security Model

ipMonitor's Security Model encompasses authentication, authorization, encryption and protection against intrusion.

Many setup and configuration choices you make while using ipMonitor also affect the security of your ipMonitor installation. The purpose of this page is to provide a top down view of ipMonitor's various security features so you can determine which ones need to be implemented for your organization.

The need for secure network monitoring is clear:

- ipMonitor tests key resources such as operating systems, SQL databases, file servers, mail systems, commerce solutions and infrastructure equipment around-the-clock.
- The tests ipMonitor performs can include logging in to resources and generating synthetic transactions to measure quality of service.
- If unauthorized persons from within or outside of your organization were to gain access to your network monitoring solution many negative scenarios could unfold.
- Without the ability to send Alerts, it might take some time before the security breach would be discovered.

ipMonitor's Security Model is designed to:

- Provide security to the ipMonitor application itself and the critical data its stores internally.
- Provide a safe network monitoring environment through secure network monitoring techniques and standard practices.

Authentication Methods

Authentication is the act of validating a person's or client's identity. Typically, clients must present a username and password pair as a credential to identify themselves for authentication.

The Credentials Manager allows you to define authentication methods as individual credentials. Each credential, in turn, can be applied to any monitor, alert, or feature that requires special permission to access restricted network resources:

- **May be used over SSL**. ipMonitor will perform authentication if the Secure Sockets Layer (SSL) encryption method is being used.
- **May be used with Digest Authentication Schemes**. Digest authentication is a challenge/response mechanism that is based on the principle of a shared secret known to both the client and server. When challenged, ipMonitor acts as the client and creates a hash digest containing its secret key and password, which it sends to the server. If the server's independently created digest matches, the server authenticates the client.
  Note: Although Digest Authentication does not send passwords in clear text, unless SSL is used Digest Authentication is only a moderate improvement over Basic Authentication, as there is nothing to prevent recording of communications between the client and server.
- **May be used with Windows Authentication Schemes**. In a Windows networking environment, authentication methods consist of two protocols: either NTLM or Kerberos v5, depending on the Windows Operating systems involved. Both NTLM and Kerberos v5 are encrypted authentication protocols. Kerberos v5 is the default authentication mechanism for the Windows 2000, XP, and Server 2003 platforms.
- **May be used with Windows Impersonation for use with RPC**. Remote Procedure Call(RPC) is a programming interface that allows one program to use the services of another program on a remote machine. This Usage Restriction option allows the ipMonitor Service to impersonate the security context of a separate Account before carrying out the RPC call.
- **May be used with Windows Impersonation to start an external process.** This Usage Restriction option allows the ipMonitor Service to impersonate the security context of a separate Account before launching an external application or script.
- **May be used with ADO (ActiveX Data Objects)**. ADO is a programming interface from Microsoft that provides a standardized interface to many different databases and data sources. OLE DB Providers written by Microsoft and other vendors are used to connect to different types of data sources through one standardized interface.
- **May be used to encrypt data**. This Usage Restriction option allows ipMonitor to encrypt and export the Credentials Database when used to archive configuration data within the Internal Maintenance feature.
- **May be transmitted in clear text**. Using Basic Authentication, the username and password information is sent over the network encoded using Base64 encoding. Unless used over SSL, Basic Authentication is inherently insecure because Base64 can be easily decoded. Basic Authentication essentially sends the username and password as plain text.

IP Access Filters

For added security, access to the ipMonitor web interface can be restricted to specific IP addresses or ranges of IP addresses.

Using IP address ranges allows you to explicitly grant or deny access to a specific organization or entity:

- If access is denied, ipMonitor will deny access to any users coming from those IP addresses.
- If access is granted, ipMonitor will communicate only with those IP addresses and ranges of IP addresses in this IP Access Filters list.

Note: IP Access restrictions cannot be configured for individual portions of the ipMonitor application.

For information regarding how to grant or deny access to IP addresses, see “Communications: Lockout” on page 26.

User Accounts

Before the ipMonitor web interfaces can be accessed, an Administrator or User must enter an Account Name and Password combination. The account credentials entered do not belong to a Windows Account. This is strictly an internal ipMonitor account.

- Permission levels can be assigned individually for each User Account.
- Administrator Accounts have access to all features.
- Strong passwords can be enforced installation-wide.
- RSA 512/1024 bit encryption is used internally to store all account information.

Three classes of accounts exist within ipMonitor: Administrator, User and Guest accounts.

Administrator Accounts

Administrator accounts:

- Have full access to all ipMonitor features.
- Can create, edit and delete User accounts.
- Are the only account type that has permission to access and administrate Credentials.
- Cannot be deleted until they are demoted to a general User Account.

Guest Accounts

Guest Accounts are designed to provide a common User Name and Password used to access the Reporting Interface. This allows an Administrator to post the Account Credentials on an intranet site, or to distribute the User Name and Password to those who require access.

Guest accounts only have the ability to Read or View data. Guests do not have access to the Administration Interface, nor do they have the ability to change or save their own settings beyond the current session.

The process of creating a Guest Account is much the same as creating an Administrator Account. Simply create a User Account, enter edit mode and then click the **Demote to Guest** option.

Guest Accounts can also be promoted to User status by clicking the **Promote to Normal User** option from the Edit Account page.

Account Permissions

Each User Account has its own List, Read, Write, Create, Delete and Attributes settings, which Administrators can apply to:

- Real-time Statistics
- Recent Activity
- Historic Reports
- Monitors
- Monitor Filters
- Groups
- Notifications
- Logs
- Tools
- Maintenance
- Report Generators
- Server Settings

Strong Passwords

Strong passwords can be enabled system-wide to help ensure system security. When Strong Passwords are enforced, the following rules apply:

- One or more lowercase characters
- One or more uppercase characters
- One or more numeric characters
- One or more non-alphanumeric characters
- 6 or more characters in total

Note: ipMonitor Accounts are proprietary; they are not Windows accounts.

Note: ipMonitor maintains an internal data hive which it uses to store all sensitive data. RSA 512/1024 bit encryption is applied to the hive.

SSL

To avoid sending passwords and configuration information over the network in clear text, you will need to install an SSL certificate.

SSL permits you to securely log in to the ipMonitor web interface from anywhere on the network or Internet and safely exchange account credentials, network paths, machine names and other sensitive information.

Although it is possible to use ipMonitor without an SSL certificate installed, some features such as the Credentials Manager will not be fully enabled unless you are connecting from ipMonitor's host machine. For this reason we suggest that you at least use ipMonitor's Self-Signed Certificate option.

Certificate Requirements

- Certificate types must be Server certificates.
- Certificates must be installed to the Local Machine Store.

Acquiring an SSL Certificate

Certificates are installed in the Local Machine Store of the ipMonitor host machine and can be selected using the ipMonitor. After the certificate has been installed, it will be necessary to configure at least one secure IP address and Port combination for HTTPS communications.

To configure a secure HTTPS interface for ipMonitor

1. Open the ipMonitor Configuration Program.
2. Select the Communications: Web Server Ports option from the main menu.

3. Click the Add button to enter a new IP address and port combination.
4. Specify the IP address to be used, or enter 0.0.0.0 to have ipMonitor listen on all available IP addresses.
5. Enter a Port number. The default value for HTTPS communication is 443. Also, ensure to check the SSL check box.
6. Click the OK button to have ipMonitor begin listening on the new SSL IP address and port combination.

ipMonitor supports several different ways of acquiring an SSL certificate:

- Self-Signed Certificates
- Trusted Certificate Authority
- Microsoft Certificate Authority

Self-Signed Certificates

During the initial installation, if a certificate has not been selected, ipMonitor will prompt to automatically generate a "self-signed" certificate. Should you choose this option, you can change this selection at any time using the ipMonitor Configuration program.

The main advantage of self-signed certificates is that there is no cost involved. However, because a self-signed certificate is generated and installed by ipMonitor, there is no Trusted Authority involved in issuing and verifying the certificate. As a result, you will have to instruct your web browser to trust the self-signed certificate that ipMonitor installs.

Trusted Certificate Authority

ipMonitor provides the tools required to generate a Certificate Signing Request (CSR) and install a certificate after it has been acquired from a trusted Certificate Authority.

Although this is not a complete list, certificates issued by VeriSign, FreeSSL™ or InstantSSL™ have been tested and all work equally as well. Prices vary from under a hundred dollars to a few hundred dollars depending on the organization.

Microsoft Certificate Authority

A Certificate can be requested from a Stand-Alone Certificate Authority using the Microsoft Windows 2000 or Windows 2003 Certificate Services web interface.

On networks that use a Stand-Alone Certificate Authority server, certificate requests must be made using the web interface provided by the Certificate Authority server. Certificate requests may have to be approved prior to being issued. Policy information may be obtained from the Network Administrator of your organization.

A Certificate can be requested from an enterprise certification authority using the Microsoft Management Console "Certificates" snap-in. This depends on the Active Directory.

Certificate requests may be generated from the ipMonitor machine using the MMC if a Certificate Authority server is found in Active Directory. Certificate requests may have to be approved prior to being issued. Policy information may be obtained from the Network Administrator of your organization.

Chapter 17

Credentials

Credentials are at the heart of ipMonitor's security model. Credentials were implemented to solve a security weakness present in many network monitoring and management solutions.

Typically, network monitoring solutions run all code, perform all monitoring, alerting and recovery actions, and perform any management capabilities using the account context the process or Service is installed under. In other words, network monitoring solutions support one account, which must be a network Administrator-level account in order to access resources throughout the network. This model is contrary to good security practices as it potentially exposes all the resources the Administrator account has access to.

ipMonitor solves this problem using its Credentials Manager. The Credentials Manager permits the ipMonitor Service to run under the context of an account with least privileges, and then to impersonate accounts with elevated permissions when required by Monitors, Alerts and features accessing Windows file system objects or Services via the network.

The Credentials Manager also provides the following additional benefits:

- Credentials can be tailored to the exact authentication requirements of the target resource.
- A Credential can be reused to access any number of target resources. The ipMonitor Credentials Wizard automatically categorizes Credentials for reusability.
- Use of a Credential can be limited to the Administrator who created the Credential or other Administrators can be permitted to use it.

Usage Restrictions can be applied to individual Credentials. A Credential can be:

- Used over SSL
- Used with Digest Authentication Schemes
- Used with Windows NT LAN Manager (NTLM) authentication schemes
- Used with Windows Impersonation for use with RPC
- Used with Windows Impersonation to start an external process
- Used with ADO (ActiveX Data Objects)

- Used to encrypt data
- Transmitted in clear text

If SSL is not used to log in to ipMonitor, the Credentials Manager:

- Will permit only limited viewing of Credentials.
- Will not allow configuration or management to take place.
- Will not make account based information visible or accessible.

Note: ipMonitor maintains an internal data hive which it uses to store all sensitive data. RSA 512/1024 bit encryption is applied to the hive. Usage restrictions and display categories can be changed over HTTP, however, the **Account**, **Password** and **Secret (for Radius)** fields cannot be modified.

Credentials Wizard

The Credentials wizard guides you through the creation of a Credential for use with monitors, alerts, and maintenance actions. You can apply restrictions on how the credentials can be used during this configuration process.

To run the Credentials wizard:

1. While configuring a monitor, alert, or other feature that requires access to Windows file system objects or services via the network, click **Select** when prompted to choose a credential.
2. If the credential you want to use has not yet been created, click **New Credential** located at the bottom of the pop-up window.

Note: Your credential is saved in the Credentials Manager. To edit or delete credentials, go to the **Configuration** tab and click **Credentials Manager**.

Credentials Must Possess Required Permissions

The credentials you supply must have the required permissions to access the monitored resources. For example, if you intend to monitor an Administrative share such as C$, the credential you supply must be a member of the Windows Administrators group.

Local Security Policies Affect Credentials

If the `ipmonitorsrv` ipMonitor service is running under a specific user account instead of the Local System account, you must ensure that the following Local Security Policies are enabled for this specific user account:

This credential type…	…requires these local policies
ADO	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Directory	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Drive Space	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Event Log	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Exchange Server	• Act as part of the operating system • Bypass traverse checking • Log on as a Service • Replace a process level token
External Process	• Bypass traverse checking • Log on as a Service • Replace a process level token
File Property	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
File Watching	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
FTP User Experience	• None
HTTP-based	• None
IMAP4 User Experience	• None
MAPI User Experience	• Act as part of the operating system • Bypass traverse checking • Log on as a Service • Replace a process level token
Net Send	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
POP3 User Experience	• None
RADIUS	• None
Reboot Server	• Act as part of the operating system • Bypass traverse checking • Log on as a Service

This credential type…	…requires these local policies
Restart Service	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Service	• Act as part of the operating system • Bypass traverse checking • Log on as a Service
Text Log	• Act as part of the operating system • Bypass traverse checking • Log on as a Service

After modifying any of these settings, you must refresh the applied Local Security Policy settings.

To refresh the applied Local Security Policy settings in Windows XP, Server 2003, and Vista

1. Open a command prompt.
2. Run the following command:
   `gpupdate /target:computer /force`
3. Verify in the Application Event log that the new settings were correctly applied. If an error was encounted, it will be recorded here.
4. Restart the `ipmonitorsrv` service.

To refresh the applied Local Security Policy Settings in Windows 2000

1. Open a command prompt.
2. Run the following command:
   `secedit /refreshpolicy user_policy /enforce`
3. Verify in the Application Event log that the new settings were correctly applied. If an error was encounted, it will be recorded here.
4. Restart the `ipmonitorsrv` service.

Credentials Manager

The Credentials Manager is used to create and manage ipMonitor Credentials.

Key features include:

- RSA 512/1024 bit encryption used internally to store all sensitive parameters and data.
- Access to the Credentials interface is restricted to Administrators only.
- Access-control options allow Administrators to specify who can use the Credentials, and determine their use.
- Credentials created through the use of the Credentials Wizard are stored within the Credentials Manager, allowing for quick and easy configuration changes.

Note: To use the Credentials Manager feature, you must log in over a SSL-secured connection or a local HTTP connection. If you log in through a non-secure, non-local channel, the Credentials Manager:

- Will permit only limited viewing of Credentials.
- Will not allow configuration changes.

Adding a Credential

Credentials may be added through the Credentials Manager or the Credentials Wizard. The Wizard allows you to create a new Credential while configuring a Monitor, Alert or Recovery Action, and apply it immediately. However, the Wizard cannot be used to edit or manage Credentials.

Orphaned Credentials

A Credential no longer associated with an Administrator Account is considered to be "Orphaned". This is a security precaution. It occurs when the Administrator Account that created the Credential has been deleted, or when the password for the Administrator Account was force-changed through the Account Configuration page.

Note: Administrators have the ability to change another account's password in the **Accounts List** page accessed from the **Configuration** view. "Force-changing" your password or another user's password in this configuration area intentionally orphans any Credentials owned by the user. This is a security precaution that prevents another ipMonitor administrator from hijacking another account's Credentials for his own use. However, if you use the **My Settings** configuration panel to change your password, this will not occur.

A warning message appears at the top of the Edit Credential page for any Orphaned Credential.

To reinitialize an Orphaned Credential:

1. Click the **Enable** button to reenter the Account Name and Password information.
2. Click **OK** to save your changes and associate this Credential with the ipMonitor Administrator Account currently being used.

Index

N

O