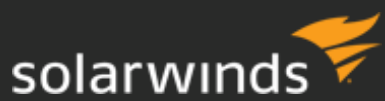




## ADMINISTRATOR GUIDE

# ipMonitor

Version 10.8.3



Last Updated: Tuesday, November 6, 2018

Retrieve the latest version from: [https://support.solarwinds.com/Success\\_Center/ipMonitor/ipMonitor\\_Documentation](https://support.solarwinds.com/Success_Center/ipMonitor/ipMonitor_Documentation)

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

# Table of Contents

<b>Introduction</b>	<b>13</b>
Monitoring	13
Alerting	13
Recovery	13
Reporting	13
<b>Upgrade ipMonitor</b>	<b>14</b>
Preflight upgrade checklist	14
Prepare your environment to upgrade	15
Upgrade ipMonitor to the latest version	15
Verify the upgrade	22
Troubleshooting	22
Want to learn more?	22
<b>Customize the Dashboard</b>	<b>23</b>
<b>Manage devices</b>	<b>24</b>
Details	24
Create groups	24
Add monitors and devices to a group	24
Create SmartGroups	24
Create a sample SmartGroup	25
Create subnets	25
Map	25
View a map of a device or group	26
Resize a map	26
Add a map to the main dashboard	26
Map editor	26
Edit a map	26
Move map objects within the map	26
Add a background to the map	26

Change the icon of a map object .....	27
Resize an object .....	27
Connect lines and assign monitors .....	27
Create a connection between two objects .....	27
Assign a monitor to a connection .....	27
NOC .....	27
Mass edit monitor properties .....	28
Mass edit tags .....	28
<b>View Reports .....</b>	<b>29</b>
Create a configurable report .....	29
Edit a configurable report .....	29
Report templates .....	29
Quick device and group reports .....	30
System status report .....	30
Report for business hours .....	31
<b>Configuration .....</b>	<b>32</b>
Sessions .....	32
Notes .....	32
Scheduled Reporting Tasks .....	32
Configure Email Report Publisher or Disk Report Publisher .....	33
<b>THWACK .....</b>	<b>34</b>
<b>Relations .....</b>	<b>35</b>
Relationship types .....	35
Monitors .....	35
Groups .....	35
Alerts .....	36
Actions .....	36
Configurable reports .....	36
Report publishers .....	36
Maintenance schedules .....	36
Credentials .....	36

<b>Monitors</b>	<b>38</b>
DNS names require lookup time	38
How monitors work	38
Monitor states	39
Scan the network	39
General monitor settings	40
Monitor submenu	40
Monitor status	40
Identification	41
Timing	41
Notification Control	42
Recovery Parameters	43
Downtime simulator	43
What the Downtime Simulator reports	44
How the Downtime Simulator works	44
Configure the Downtime Simulator	46
Downtime Simulator example of an IIS restart	46
<b>Group dependencies</b>	<b>48</b>
Groups	50
All Managed Devices group	50
Orphaned Objects group	50
<b>Monitor types</b>	<b>51</b>
Active Directory	52
Bandwidth Usage	53
Battery	54
Test results	54
CPU Usage	54
Test results	54
DNS User Experience	55
DNS TCP	55
DNS UDP	56

Directory .....	56
Drive Space .....	57
Test results .....	57
Event Log .....	57
Tests on Event Log monitors differ from other monitors .....	58
Recommended default timing interval .....	59
Exchange Round-Trip Email wizard .....	59
Exchange Server 2000 and 2003 .....	59
Exchange Server 2007 and 2010 .....	59
WMI requirements .....	60
Troubleshoot WMI .....	60
External Process .....	63
Analysis of test results .....	63
Process Return Value .....	64
Environment Variable .....	64
Test results .....	66
Fan .....	67
File Property .....	67
Test results .....	68
File Watching .....	68
Example .....	68
Sample line in Syslog: Cisco PIX firewall .....	68
Monitor configuration settings .....	69
Content generator .....	69
Name: Cisco PIX Interface .....	69
Information alert results .....	70
Finger .....	70
FTP .....	70
FTP User Experience .....	71
Generic WMI .....	71
Gopher .....	72

HTML/ASP .....	72
HTTP .....	73
HTTP User Experience .....	74
HTTPS .....	74
Humidity .....	75
Test results .....	75
IMAP4 .....	75
IMAP4 User Experience .....	76
ipMonitor .....	76
Group testing .....	77
IRC .....	78
Kerberos 5 .....	78
LDAP .....	78
Link - User Experience .....	79
Test results .....	80
Lotus Notes .....	80
MAPI - User Experience .....	80
Microsoft Outlook account requirements .....	81
Use the Microsoft CDO .....	81
Set up a Windows Mail Profile .....	82
Test email message .....	82
Memory Usage .....	82
Network Speed .....	83
NNTP .....	84
NTP .....	84
Ping .....	85
POP3 .....	85
POP3 - User Experience .....	86
Implementation .....	86
Printer monitor .....	87
RADIUS .....	87

Test limitations .....	87
RWHOIS .....	87
Service .....	88
Windows recovery options for services .....	88
SMTP .....	89
Minimize the SMTP server load .....	89
SNMP .....	90
SNMP agent security .....	90
SNMP - User Experience .....	90
SNMP - User Experience wizard .....	91
Step 1: Select SNMP device and scan parameters .....	91
Step 2: Select an SNMP object to monitor .....	91
Step 3: Provide SNMP object comparison rules .....	91
Step 4: Name and configure your SNMP User Experience monitor .....	92
SNMP Trap - User Experience .....	92
Integrate ipMonitor with third-party network management solutions .....	93
Turn on the SNMP Trap Listener .....	93
Conflicts with the Windows SNMP trap service .....	93
Use filters in the SNMP Trap monitor .....	94
IP address range .....	94
Generic Type .....	94
Enterprise OID .....	95
Get Info .....	95
To OID .....	95
Enterprise Specific Kind .....	95
SNPP .....	96
SQL - ADO .....	96
OLE DB provider requirements .....	96
Verify your OLE DB provider .....	97
SQL - ADO User Experience .....	97
Test results .....	98



SQL ADO wizard .....	98
Step 1: Select database type .....	98
Step 2: Data source location .....	98
Step 3: Assign login credential .....	99
Step 4: Select database .....	99
Step 5: Select database table .....	99
Step 6: Generate SQL Query .....	99
Step 7: Analysis of results .....	99
Step 8: Name Monitor .....	101
Manually configure the ADO User Experience monitor .....	101
Database Type .....	101
Credential for Monitoring .....	101
Run this test from an external process .....	101
SQL Authentication .....	102
Integrated Windows Authentication .....	102
Named Instance .....	102
TCP/IP Connection to SQL Server 2000 .....	103
Retrieve a Maximum of "x" Rows .....	104
Examine the Row Count .....	104
Number of Rows Retrieved Must Be .....	104
Examine the Row Content .....	104
Examine Column Number .....	104
Column Will .....	104
SQL Server .....	105
Windows Management Instrumentation (WMI) requirements .....	105
TELNET .....	105
Temperature .....	106
Test results .....	106
Temperature wizard .....	106
Step 1: Specify the location of the device .....	107
Step 2: Select interface and monitoring thresholds .....	107

Step 3: Create the new temperature monitor .....	108
Windows .....	108
WHOIS .....	109
Test Results .....	110
<b>Alerts and notifications .....</b>	<b>111</b>
How alerts work when a monitor detects a problem .....	111
Escalating Alerts .....	111
Scheduling Alerts .....	111
Credentials .....	112
Alert escalation .....	112
How to notify a supervisor after the sixth alert .....	112
Timing considerations .....	112
Failure and alerting process .....	113
Timing Settings : Delays Between Tests While .....	113
Notification Control .....	113
Preview the process with the Downtime Simulator .....	114
Schedule alerts .....	114
Seven-day availability calendar .....	114
Customize notifications with tokens .....	114
Date, time, and formatting tokens .....	114
Monitor information tokens .....	115
Alert and action tokens .....	117
System tokens .....	118
Content Generator token restrictions .....	118
<b>Action types .....</b>	<b>119</b>
Automatic Report .....	119
Custom Email .....	120
Event Log .....	120
External Process .....	120
Net Send Broadcast .....	121
Reboot Server .....	121

Restart Service .....	122
Simple Beeper .....	122
Beeper hardware requirements .....	122
Simple Email .....	122
SMS Numeric Pager .....	123
Supported paging protocols .....	123
Hardware requirements .....	124
About SMS .....	124
SMS Text Pager .....	124
SMS Text Pager - GSM .....	124
Hardware requirements .....	125
SMS Text Pager - TAP and UCP .....	125
Hardware requirements .....	125
SNMP Trap .....	125
Set up the alert .....	127
HP OpenView .....	127
Text Log .....	127
<b>Information alerts .....</b>	<b>128</b>
Content Generator .....	128
Information action messages .....	129
Additional content generator tokens .....	130
Numeric Tokens .....	130
Property Tokens .....	130
Event Log Tokens .....	131
SNMP Trap Tokens .....	131
File Watching Tokens .....	132
<b>Log files .....</b>	<b>133</b>
Generated Log Files .....	133
ipm.log .....	133
runtime.log .....	134
runtime_bkg_reports.log .....	134

snmptrap.log .....	134
<b>Maintenance schedules .....</b>	<b>135</b>
Suspend monitors while ipMonitor reboots services and computers .....	135
Suspend monitors during network maintenance .....	136
Internal Maintenance .....	136
Standalone backup .....	136
<b>Security model .....</b>	<b>137</b>
Authentication methods .....	137
IP access filters .....	138
User accounts .....	138
Administrator accounts .....	139
User accounts .....	139
Guest accounts .....	139
Account Permissions .....	139
Strong passwords .....	140
SSL .....	140
Certificate requirements .....	140
Obtain an SSL certificate .....	140
Self-signed certificates .....	141
Trusted Certificate Authority .....	141
Microsoft Certificate Authority .....	141
<b>Credentials .....</b>	<b>142</b>
Credentials wizard .....	143
Required permissions .....	143
SNMPv3 authentication .....	143
Local security policies and credentials .....	144
Credentials Manager .....	146
Adding a credential .....	147
Orphaned credentials .....	147
Reinitialize an orphaned credential .....	147
Change monitoring credentials in bulk .....	147

# Introduction

SolarWinds® ipMonitor uses data collection tools to proactively monitor your small to medium business network. The application includes alert types to notify you in the event of trouble and automatically recover critical applications, servers and infrastructure devices whenever possible.

## Monitoring

SolarWinds ipMonitor proactively discovers your critical network resources and tracks their availability, responsiveness and performance quality by monitoring the health of:

- Businesses and web applications, such as SQL databases, web servers, commerce, and mail servers
- Infrastructure equipment, such as server computers, switches, routers, and power backup systems
- Services including IP-based services and Microsoft Windows services

## Alerting

Alert actions in ipMonitor provide methods to alert you by phone using email or SMS, numeric or alphanumeric pager, or wireless devices using email or net broadcast.

## Recovery

Each monitor allows you to set operating environment variables. Alerts use these variables when a problem is detected. When a failure occurs, SolarWinds ipMonitor implements the following recovery actions:

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


## Reporting

SolarWinds ipMonitor provides in-depth visual analysis of your monitor statistics with detailed reports. These reports include:

- Dashboard and Network Operation Center (NOC) views that provide reports for all personnel who manage the network
- Configurable data analysis reports in graphical and tabular formats
- Reports with instance access to statistics recorded by any monitor or group
- Reports that explore the database of test results to identify the error messages that triggered the alerts
- Email reports that can be distributed to single or multiple recipients

# Upgrade ipMonitor

This section walks you through the process of upgrading your SolarWinds ipMonitor software.

 SolarWinds Technical Support no longer provides support for ipMonitor 10.6 and earlier versions. All information and procedures for these versions are provided for guidance only. See [Currently supported software versions](#) for details.

## Preflight upgrade checklist


This preflight checklist details a number of important steps to help you plan and prepare for the upgrade.

When you are ready to upgrade, complete these steps. They include the common actions you need to complete before you upgrade your ipMonitor software.

<input type="checkbox"/>	Review the release notes	Review the <a href="#">product release notes</a> and available documentation in our <a href="#">Success Center</a> .
<input type="checkbox"/>	Review the system requirements	Make sure your environment has all of the required hardware and software requirements for your installations.  See the ipMonitor Installation Guide located in the <a href="#">Success Center</a> for details.
<input type="checkbox"/>	Review your licenses	Review your current product license and determine if you need to make any changes. You can download any updated license keys for your upgrade through your <a href="#">Customer Portal</a> . Verify any license upgrades and needs with your SolarWinds account manager or <a href="#">contact SolarWinds</a> .
<input type="checkbox"/>	Gather credentials	Make sure you have the following: <ul style="list-style-type: none"><li>• User account credentials for all users you want to add as ipMonitor administrators</li><li>• IP address and listening port number for the SNMP Trap Listener (port 443 for HTTPS or port 8080 for HTTP)</li><li>• (Optional) Local System account credentials to run the ipMonitor service on a local user account</li></ul>
<input type="checkbox"/>	Run all Windows updates	Before you upgrade, check for and run all Microsoft Windows updates on your ipMonitor server. As you upgrade, if a Windows update runs, your system may reboot as needed by Windows.
<input type="checkbox"/>	Schedule the upgrade	Set up the maintenance window, preferably during off-peak hours. Depending on the size of environment, you may need additional time to complete the upgrade.
<input type="checkbox"/>	Notify your company	Send a message to your company of the upgrade schedule and maintenance window. If you need additional help, contact and allocate specific staff to be available.

## Prepare your environment to upgrade


When you are ready to upgrade, complete these steps. They include the common actions you need to complete before upgrading products.

 If you have a test or staging environment, we highly recommend testing the upgrade first. You cannot roll back an installation when it is completed.

<input type="checkbox"/>	Back up your ipMonitor server	Create a backup of the server hosting ipMonitor.
<input type="checkbox"/>	Check your hard drive space	Verify that you have enough hard drive space for the zipped and unzipped installer.

## Upgrade ipMonitor to the latest version

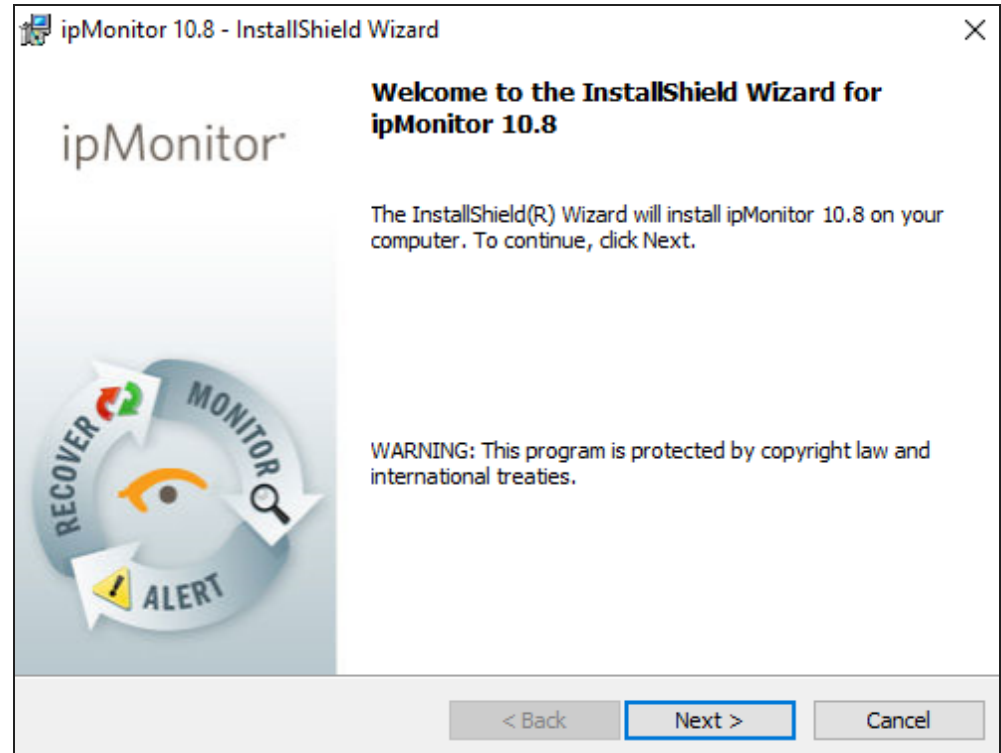
This checklist details the steps for upgrading ipMonitor in your environment.

 If you have a test or staging environment, we highly recommend testing the upgrade first. You cannot roll back an upgrade once it's completed.

<input type="checkbox"/>	Download the installation files from the Customer Portal	<ol style="list-style-type: none"> <li>1. Go to <a href="https://customerportal.solarwinds.com">customerportal.solarwinds.com</a>.</li> <li>2. In the Log In tab, enter your organization's SWID and your email address, and then click Log In.</li> <li>3. Click Downloads &gt; Download Product.</li> <li>4. Click the Products drop-down menu and select ipMonitor.</li> <li>5. Locate the targeted download.</li> <li>6. Click the Download Type drop-down menu, select a version, and then click Download.</li> </ol>
<input type="checkbox"/>	Run the installation file	<ol style="list-style-type: none"> <li>1. Log in as an administrator to the server where you will install ipMonitor.</li> <li>2. Extract the contents of the downloaded installation ZIP file to the server.</li> <li>3. Run the EXE file.</li> </ol>

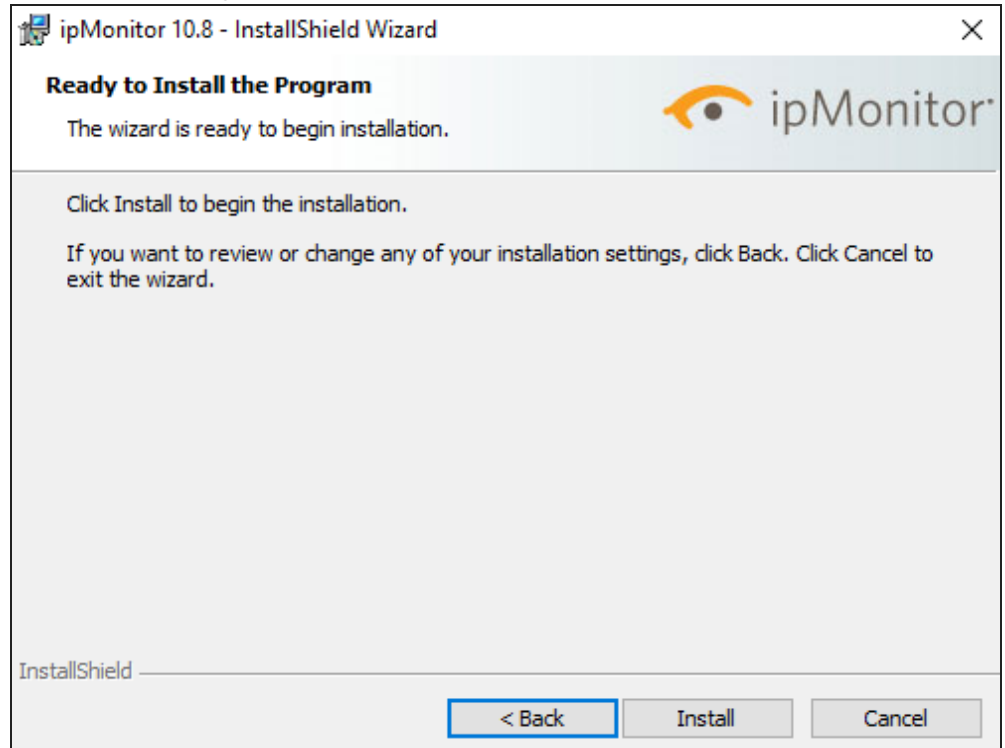
- ☐ Complete the installation wizard

1. Click Next on the Welcome window.

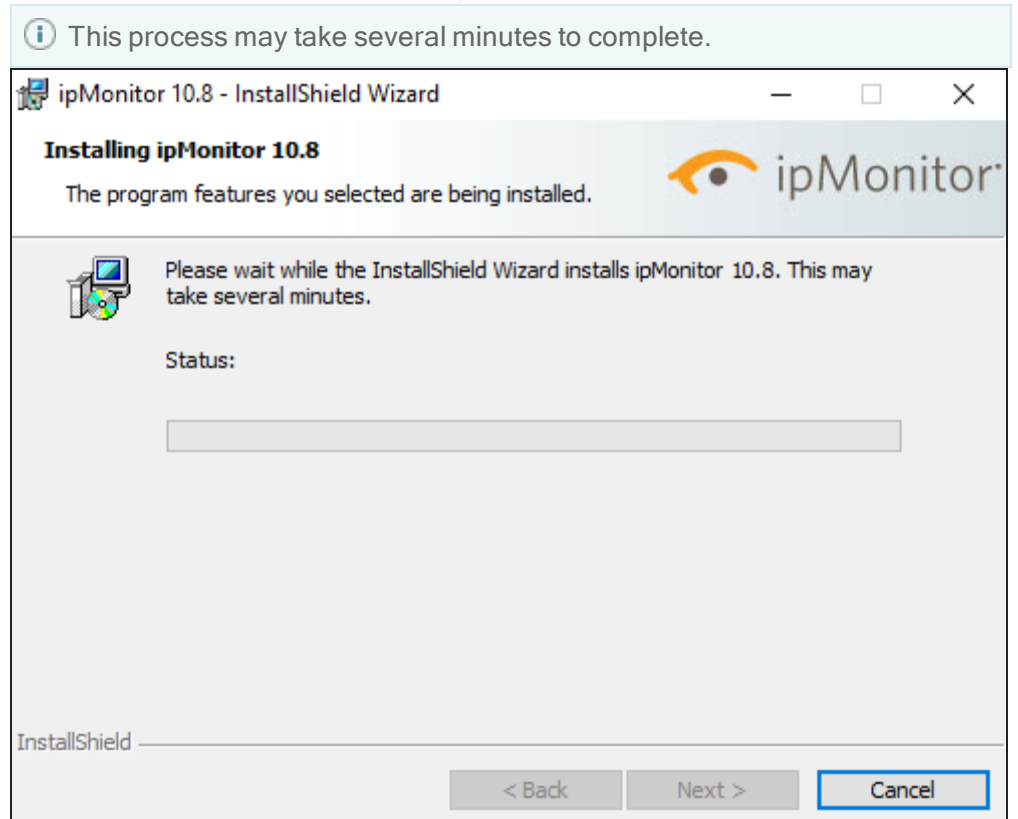




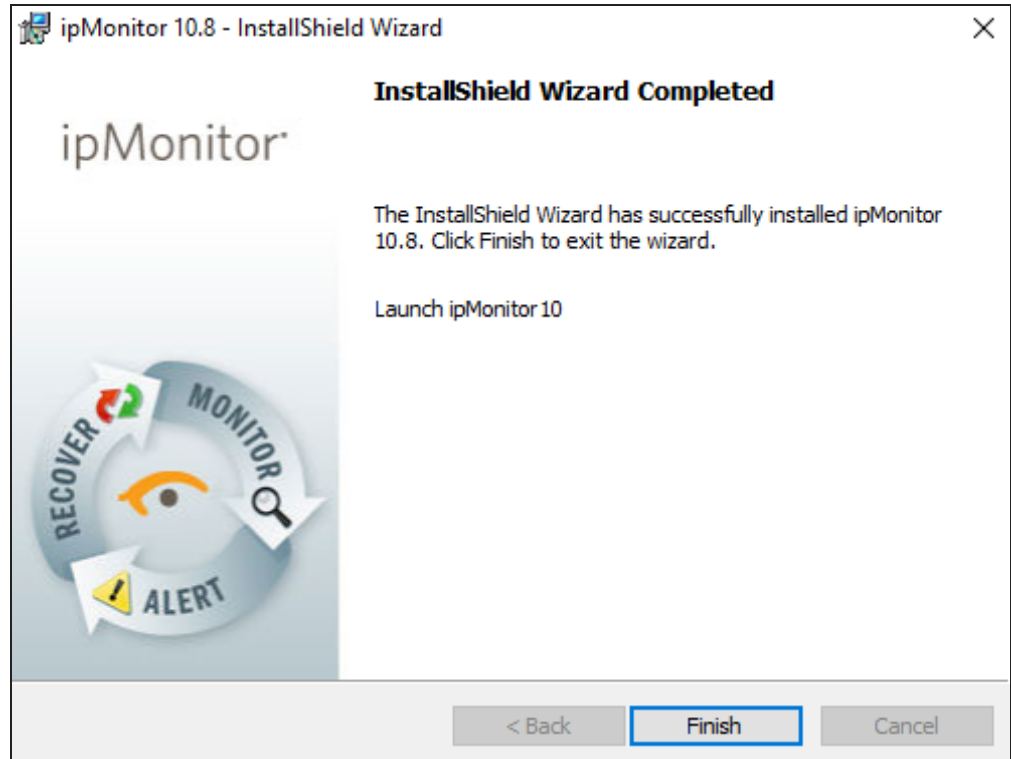
2. Click Install to begin the installation.



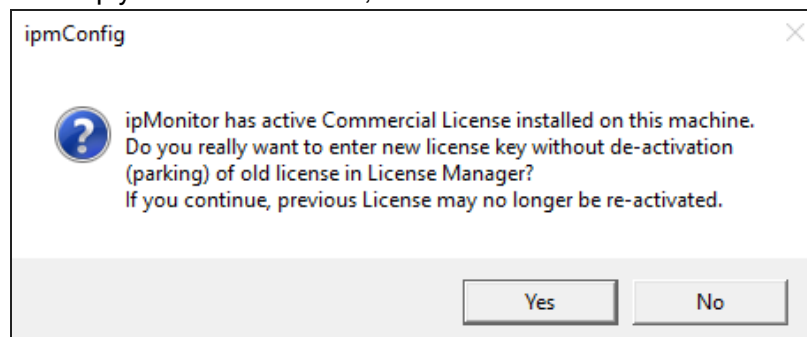
The installation files are installed on your server.



3. When prompted, click Finish.




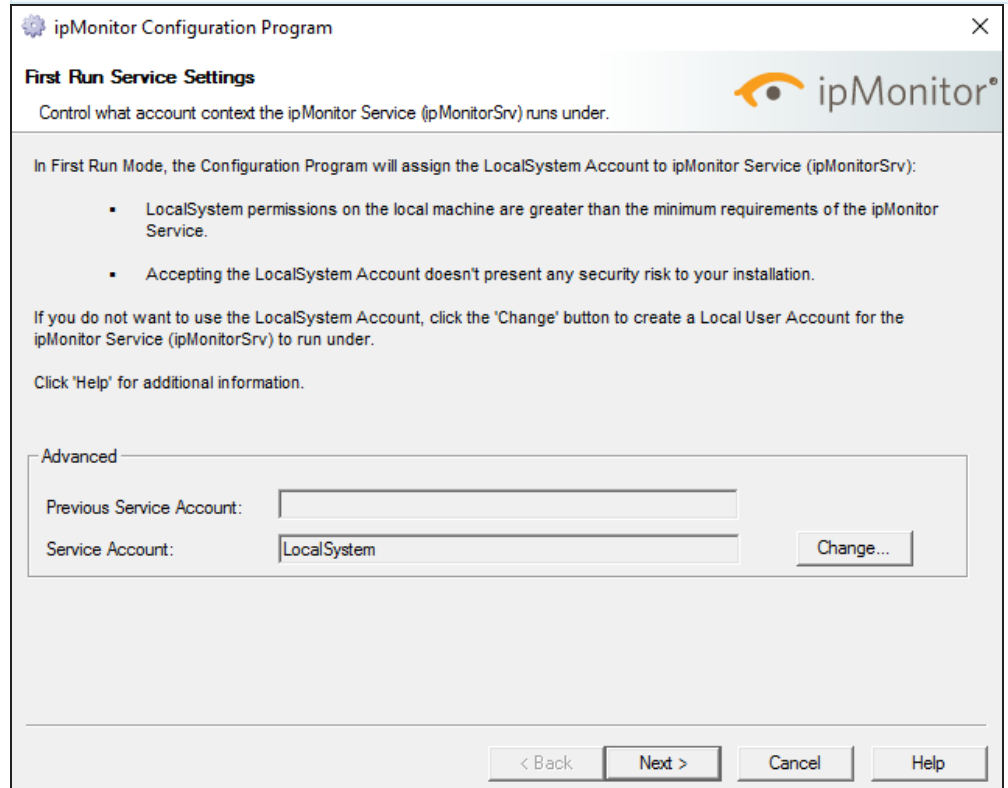
4. To keep your current license, click No.



5. To continue running the ipMonitor Service on the Local System account, click Next.

To run the ipMonitor Service on a Local User account, click Change, complete the fields, and then click Next to continue.

 See [Credentials Wizard](#) for details about local security policies that must be enabled for a Local User account.

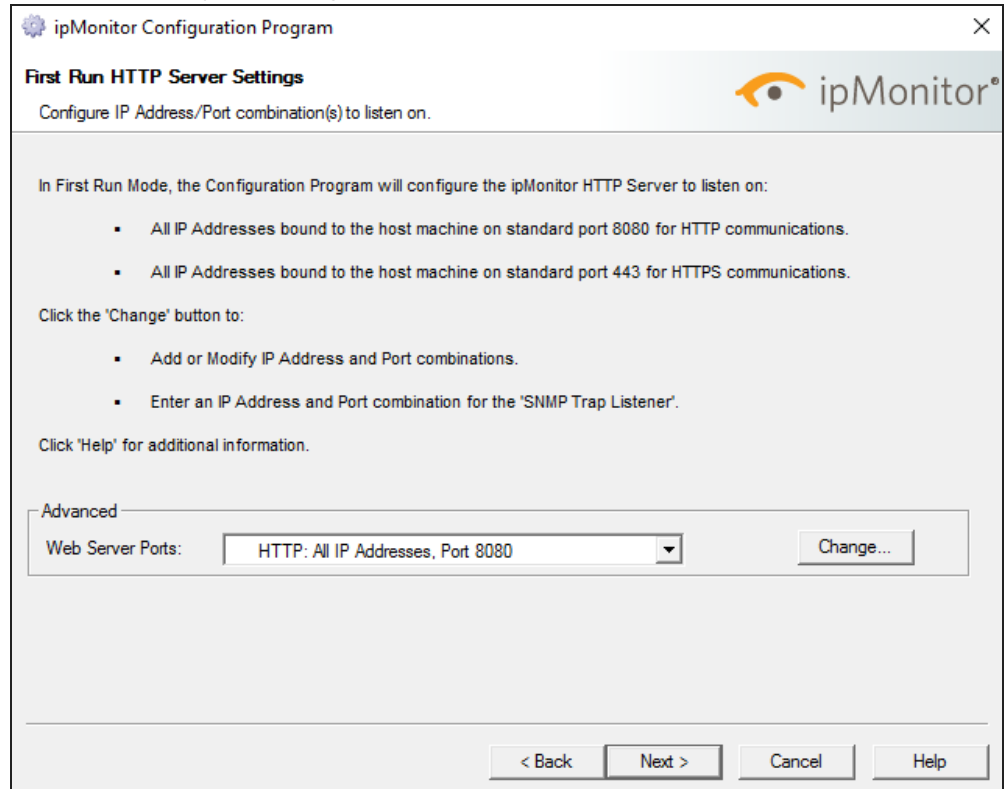


The dialog box is titled "ipMonitor Configuration Program" and "First Run Service Settings". It contains the following text and controls:

- Control what account context the ipMonitor Service (ipMonitorSrv) runs under.
- In First Run Mode, the Configuration Program will assign the LocalSystem Account to ipMonitor Service (ipMonitorSrv):
  - LocalSystem permissions on the local machine are greater than the minimum requirements of the ipMonitor Service.
  - Accepting the LocalSystem Account doesn't present any security risk to your installation.
- If you do not want to use the LocalSystem Account, click the 'Change' button to create a Local User Account for the ipMonitor Service (ipMonitorSrv) to run under.
- Click 'Help' for additional information.
- Advanced section with two text boxes:
  - Previous Service Account: (empty)
  - Service Account: LocalSystem
- A "Change..." button next to the Service Account field.
- Navigation buttons at the bottom: "< Back", "Next >", "Cancel", and "Help".

6. To use the existing IP address and port combinations for the SNMP Trap Listener, click Next.

To add or modify the IP address and listening port, click Change, complete the fields and save your changes, and then click Next .



The image shows a screenshot of the 'ipMonitor Configuration Program' window, specifically the 'First Run HTTP Server Settings' dialog. The window title is 'ipMonitor Configuration Program' with a close button (X) in the top right corner. The main heading is 'First Run HTTP Server Settings' with the subtext 'Configure IP Address/Port combination(s) to listen on.' and the 'ipMonitor' logo in the top right. The text inside the dialog states: 'In First Run Mode, the Configuration Program will configure the ipMonitor HTTP Server to listen on:' followed by two bullet points: 'All IP Addresses bound to the host machine on standard port 8080 for HTTP communications.' and 'All IP Addresses bound to the host machine on standard port 443 for HTTPS communications.' Below this, it says 'Click the \'Change\' button to:' followed by two bullet points: 'Add or Modify IP Address and Port combinations.' and 'Enter an IP Address and Port combination for the \'SNMP Trap Listener\'.' It also mentions 'Click \'Help\' for additional information.' At the bottom, there is an 'Advanced' section with a 'Web Server Ports:' label, a dropdown menu showing 'HTTP: All IP Addresses, Port 8080', and a 'Change...' button. At the very bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

ipMonitor Configuration Program

**First Run HTTP Server Settings**

Configure IP Address/Port combination(s) to listen on.

In First Run Mode, the Configuration Program will configure the ipMonitor HTTP Server to listen on:

- All IP Addresses bound to the host machine on standard port 8080 for HTTP communications.
- All IP Addresses bound to the host machine on standard port 443 for HTTPS communications.

Click the 'Change' button to:

- Add or Modify IP Address and Port combinations.
- Enter an IP Address and Port combination for the 'SNMP Trap Listener'.


Click 'Help' for additional information.


Advanced

Web Server Ports: HTTP: All IP Addresses, Port 8080 Change...

< Back Next > Cancel Help


7. (Optional) Complete the tasks in the New ipMonitor Administrator Account box to configure additional users as ipMonitor administrators. Otherwise, click Next to continue.

 All existing users can still log in to ipMonitor.

 ipMonitor Configuration Program

**First Run Administrator Account**

Add Administrator Accounts to ipMonitor.




In order to log in to ipMonitor, you must create an Administrator Account.

ipMonitor Administrator accounts have access to all features and can create and manage other Administrator, User or Guest Accounts and credentials.

Note: Standard and Guest ipMonitor Accounts are strictly internal to the ipMonitor software. Windows ipMonitor Accounts are associated with Windows Local Machine or Domain Accounts.

Click 'Help' for additional information.

New ipMonitor Administrator Account

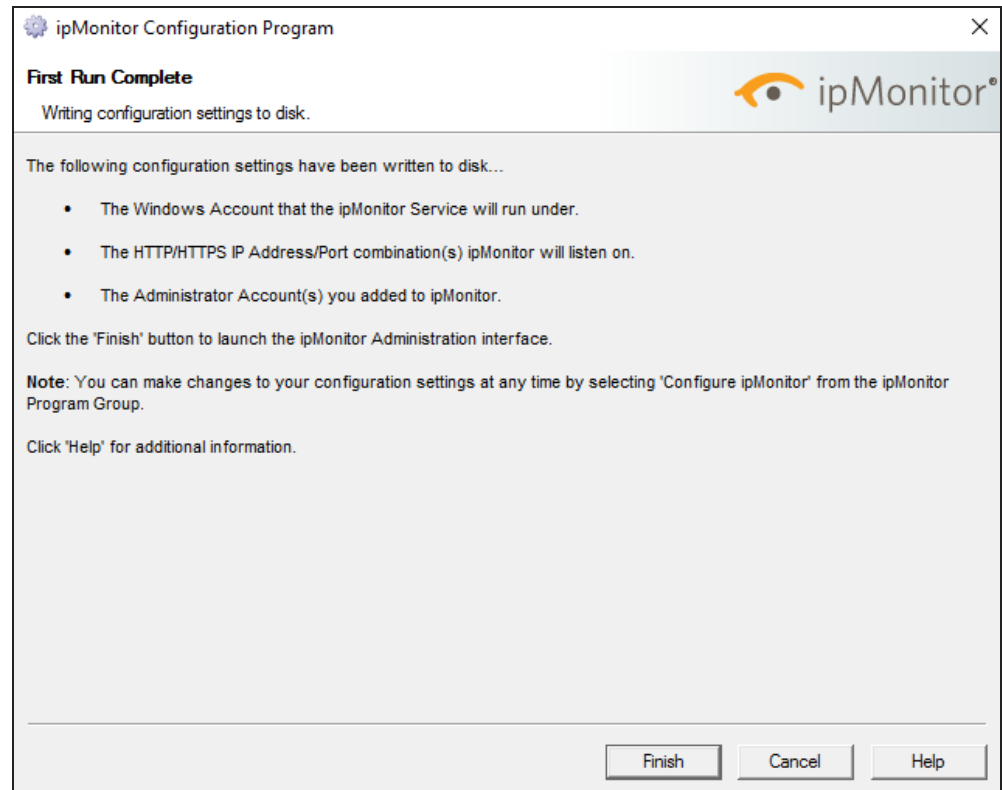
 Admin account with the name "ian" already exists.  
You can add a second admin account now or skip this step and click 'Next'

Account Type: ☒ Windows Account  
☐ Standard ipMonitor Account

Username and Domain:

For example: MY\_DOMAIN\_NAME\John.Smith

8. Click Finish to complete the ipMonitor upgrade and launch the ipMonitor administrator interface.



Your ipMonitor software is upgraded to the current release.

## Verify the upgrade

Open the application and verify the version displayed in the footer of the web console. Try current and new features with your system to check performance and expected functionality. If you run into issues, check the troubleshooting tips.

## Troubleshooting

If you run into issues after the upgrade, check our [Success Center](#) for troubleshooting. Search for ipMonitor, the version number, any error codes or messages displayed, and the general issue you found.

If an issue occurs that you cannot resolve, [contact Support](#). Create a screen shot of the issue and any error codes you receive. Attach and add this information to your ticket.

## Want to learn more?

- Check the ipMonitor Getting Started Guide, Administrator Guide, and additional ipMonitor documentation on the [ipMonitor Documentation website](#).
- Review the latest [ipMonitor release notes](#).

# Customize the Dashboard

The Dashboard consolidates a variety of small reports called web resources into a summary page that displays status information for any device, group, or monitor. Each monitor, device, and group includes a Dashboard view that you can customize with different resources to show the information you want.

From here, you can change the layout of the web resources and display top devices by bandwidth use, ping time, CPU utilization, and other criteria.

Click **Change Columns** to change the layout of Dashboard views.

If you want to change the width of a column, enter a new value in the **Width** field.

# Manage devices

The Devices tab contains [Details](#), [Map](#), and [Network Operations Center \(NOC\)](#) views that allow you to classify, organize, and view the status of the devices and monitors in your network.

## Details

The Details view provides a tree view representation of your network. In this view, you can create [groups](#), [SmartGroups](#), and [subnets](#).

## Create groups

SolarWinds ipMonitor allows you to organize individual monitors and devices together under a group. A group does not contain the actual monitors and devices, but references them as members. As a result, monitors and devices can belong to several different groups.

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

1. In the Devices tab, select a group in the tree where you want to create the new group.
2. In the Add menu, click Add New Group.
3. Enter a group name, and click OK.

You can choose group names based on their level of importance, purpose, location, responsibility, and department.

## Add monitors and devices to a group

1. Select the group.
2. In the Add menu, click Add Existing Monitors or Add Existing Devices.
3. Select the monitors or devices that you want to add. You can add both monitors and devices to the same group.
4. Click Continue.

## Create SmartGroups

SmartGroups are dynamic groups that include content determined by a filter you create. Unlike regular groups that include static content, SmartGroup content automatically keeps track of changes in your network.

For example, you can create a SmartGroup for a group of all network devices located in Texas, or a group of all offline monitors in your network.

1. In the Devices tab, select Add New SmartGroup in the Add menu.
2. Create filter rules that define the SmartGroup, and click OK.




## Create a sample SmartGroup

In this example, you will create a SmartGroup that contains all devices manufactured by Cisco Systems.

1. Select the My Network group in the devices tree.
2. In the Add menu, select Add New SmartGroup.
3. Enter:  
`All Cisco Devices`
4. In the SmartGroup Contains field, select Devices.
5. In the Start With field, select No Devices.
6. Add a rule that compares the Device Vendor property of each device.
  - a. In the devices Where menu, select property.
  - b. Click Click here to Select a Property to open the property menu.
  - c. Click the drop-down menu and select Device Properties.
  - d. Click Device Vendor, and close the menu.
7. Use the Regex Wizard to create a regular expression for the Matches regular expression field that matches the case-sensitive string `Cisco`.
  - a. Click Regex Wizard.
  - b. In the Match begins with field, enter:  
`Cisco`.
  - c. At the bottom, copy the text created in the Regular Expression you have built field, and close the wizard.
  - d. Paste the text into the Matches regular expression field.
8. Click OK to create the SmartGroup.

## Create subnets

A subnet is an IP address range within your network. When you add a new subnet, ipMonitor, creates a group that contains references to devices within the subnet. These references are automatically created when you create the subnet.

 Do not manually add devices to a subnet.

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

## Map

A map is a graphical representation of your network devices and monitors. You can visualize the effects of a failing device or monitor with the help of maps.

Default maps are created in ipMonitor for each group and device in your network.

## View a map of a device or group

1. In the Devices tab, select the group or device from the tree.
2. Click Map.

## Resize a map

To resize the map, you can:

- Move the scale slider to zoom in or out.
- Click Fit To Screen to automatically size the map to the full extent of the area.

## Add a map to the main dashboard

1. Click the Dashboard tab.
2. In the Add Web Resource menu, select Map.
3. In the Edit menu of the new map resource, click Select Map.
4. In the Select map to display list, click the specific device or group map that you want to display.
5. Click Save, and then confirm the change.

The new map replaces the default map in the Dashboard.

## Map editor

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

### Edit a map

1. In the Details view, click the device or group with the map you want to edit.
2. Click Map > Edit Map.

### Move map objects within the map

Perform any of the following options:

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

### Add a background to the map

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

## Change the icon of a map object

1. Click the object.
2. Click the Icons list, and select an icon category.
3. Click an icon.

## Resize an object

Click the object and drag the bounding box to resize.

## Connect lines and assign monitors


You can create logical connections that represent the status of a monitor between any two objects. For example, you can draw a line between two devices and assign a bandwidth monitor to that connection. If the monitor moves into a down state, the state is reflected in the map.

### Create a connection between two objects

1. In the Drawing Tools palette, click the line drawing tool.
2. Drag a line from one object to another.

### Assign a monitor to a connection

1. In 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 click OK.

 The monitor status indicators in the Map Editor are not active. Exit the Map Editor to view the true status of the monitor.

## NOC

The Network Operations Center (NOC) view provides a glance at status reports for IT personnel and network operations groups who manage the network 24 hours a day.

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. The resource color can also change to red, and then to dark red as ipMonitor detects successive failures.

As the failure detection process occurs, the interface is re-flowed to move the failing monitors 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. When you enable sound in your web browser, ipMonitor emits a sound when an alert is received.

# Mass edit monitor properties

Use the Mass Edit feature to apply large-scale changes to configuration fields across any number of monitors using a rule-based system.

Using this 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

Access the Mass Edit feature for Monitor Properties

1. In the Devices tab, click Edit > Mass Edit.
2. Select Monitor Properties.

# Mass edit tags

You can use the Mass Edit feature to quickly apply large-scale changes to custom tags across any number of monitors using a rule-based system.

1. Log in to the ipMonitor web interface.
2. Click the Devices tab.
3. Click Edit > Mass Edit.
4. Select Monitor Tags.

# View Reports

The Reports tab displays a list of configurable reports that provide detailed monitoring data in both graphical and tabular formats.

These reports monitoring data for response time, uptime, and downtime for specified time periods. You can also leverage the historical data to view long-term and short-term performance trends, identify problems, and report operational efficiency for individual monitors and monitor groups.

Using the customizable options, you can:

- Use the available data sources to display data averages for CPU, memory, battery, temperature, humidity, hard drive and bandwidth usage monitors in graphical or tabular format
- Display monitor data in line graphs, vertical bar graphs, horizontal bar graphs, area graphs, and tables
- Display data spanning multiple time periods in one report
- Display statistics 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, such as business hours for work weeks

## Create a configurable report

The Add Report Wizard tests the selected customization options by previewing the appearance of the report before saving it. This allows you to create a report with the least amount of input.

1. Go to the Reports tab.
2. In the My Reports column, click Add New Report.

## Edit a configurable report

1. Go to the Reports tab.
2. In the My Reports column, click the drop-down menu next to the report that you want to configure.
3. Select a command from the menu.

## Report templates

Report templates can help you create customized Service Level Agreement (SLA) reports based on recurring time selections. You can create reports that display response time, uptime, and downtime for specified time periods. Additionally, 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.


Using report templates you can:

- Use the available data sources to display data averages and view these averages for CPU, memory, battery, temperature, humidity, drive space, and bandwidth usage monitors in graphs or tabular format
- Arrange monitor data for display in graphs or tables
- Display data spanning multiple periods in one report
- Display statistics 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 through design and layout control
- Add custom logos or other graphics, and use CSS and HTML code to customize the appearance of each report
- Add custom headers and footers to each report
- Assign permission levels to determine which administrator or user account can view a particular report

## Quick device and group reports

Although you cannot edit the report parameters of a device or a group report, you can save an editable copy to My Reports where you can edit the report like any other customizable report.

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

 If you select a report type that does not exist for your selection, you will see a blank report.

To save an editable version of a Quick Report, click Save to My Reports.

## System status report

The system status report provides details about ipMonitor and the server hosting the application.

Print out this report before you contact SolarWinds Technical Support. This report includes information for troubleshooting the application, including:

- Product version and build number
- Free hard disk space
- Available memory
- Physical memory
- Additional information used for troubleshooting purposes.

# Report for business hours

You can create a report that is scheduled to reflect business hours.

1. Create a report using the Add New Report Wizard.
2. In the Edit Report page, click Add Time Selection.
3. Under Time Navigation Rules, select the following settings:
  - Start At: "This" Week
  - then go Forward: 1 Day
  - then go Forward: 9 Hours
4. Under Time Selection, enter 8 Hours, and click OK.

This creates a time selection for 9 AM to 5 PM, beginning on Monday.
5. Repeat Steps 2 through 4 for the remaining days of the business week using the following settings:
  - a. Tuesday:
    - Start At: "This" Week
    - then go Forward: 2 Days
    - then go Forward: 9 Hours
    - Include: 8 Hours
  - b. Wednesday:
    - Start At: "This" Week
    - then go Forward: 3 Days
    - then go Forward: 9 Hours
    - Include: 8 Hours
  - c. Thursday:
    - Start At: "This" Week
    - then go Forward: 4 Days
    - then go Forward: 9 Hours
    - Include: 8 Hours
  - d. Friday:
    - a. Start At: "This" Week
    - b. then go Forward: 5 Days
    - c. then go Forward: 9 Hours
    - d. Include: 8 Hours
6. Add the report elements for each time selection.

# Configuration

The Configuration page provides access to all configurable ipMonitor items and settings. These settings include [sessions](#), [notes](#), [scheduled reports](#), alerts, user accounts, credentials, and tools to help you administer your network.


## Sessions

Use this page to view administrators and users currently logged in to ipMonitor.

## Notes

Notes allows you to post messages for all ipMonitor administrators and users regarding configuration settings, policy information, problem resolution, and so on. This feature is ideal for IT departments with teams of people accessing the administrator interface at various times during the week.

1. On the Configuration page, click My Settings.
2. In the Start Page list, select Notes.  
The Notes page will be the first page that administrators and users see after logging in. New messages will display at the top of the page

 Administrators can delete any posted message. Users can only delete messages posted by non-administrators.

## Scheduled Reporting Tasks

You can use Scheduled Reporting Tasks to email your configurable reports and quick reports to a list of users at scheduled intervals, or save them to a directory using Report Publisher.

You can configure the reports to display the response time, uptime, and downtime for specified time periods. Additionally, 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.

Using the Report Publisher, you can:

- Email reports to users on a daily or weekly basis
- Email reports to multiple recipients
- Manage the images included in the report
- Change the report file name
- Save the report to a specific directory



## Configure Email Report Publisher or Disk Report Publisher

Email Report Publishers email your reports to a list of users based on a predetermined schedule. Disk Report Publishers saves your reports to a specific location.

1. In the Configuration tab, click Scheduled Reporting Tasks.
2. Click Add Email Report Publisher or Add Disk Report Publisher.

# THWACK

The THWACK tab provides quick access to the most recent [THWACK community forum posts](#) and file uploads for ipMonitor. You can search for ipMonitor-related content from the web interface.

# Relations

The Relations page shows how the essential elements of your network (such as monitors, alerts, and actions) relate with each other. These relationships ensure that the assigned personnel are notified when a problem occurs.

You can access the Relations window from the Edit page of any configuration element.

## Relationship types

You can associate ipMonitor features with other configuration elements. The types of relations displayed in the Relations window depend on the feature you are editing.

### Monitors

A monitor is a background process that continuously tests a target resource on timed intervals.

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 associated with the monitor
- Any action that is part of a monitoring alert
- Any maintenance schedule that regulates scheduled monitor downtime
- 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

SolarWinds ipMonitor allows you to group multiple individual monitors together and assign dependencies to them. 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

Alert relations can include any monitor or group assigned to the alert and any action belonging to the alert.

## Actions

Action relations can include:

- Any monitor or 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 report relations can include:

- Any monitor or group included in the configurable report
- Any report publisher that contains the configurable report

## Report publishers

Report publishers allow you to save configurable reports 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

Administrators can use maintenance schedules to temporarily disable monitoring on certain resources—for example, performing data back ups or service restart actions.

Maintenance schedule relations can include:

- Any monitor or group affected by the maintenance schedule
- Any credential assigned to the maintenance schedule

## Credentials

To fully enable ipMonitor, various monitors, alerts, and management features must be able to access Windows file system objects or services through 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
- Manual backup action assigned to this credential
- Recurring internal maintenance backup action assigned to the credetial

# Monitors

SolarWinds ipMonitor includes a comprehensive suite of monitors to monitor system resources, applications, infrastructure equipment, servers, and essential services 24 hours a day.

MONITOR	DESCRIPTION
Quality assurance	Performs result analysis testing for critical applications, such as SQL database servers, commerce solutions, and dynamic web applications.
SNMP polling and trap	Provides industry standard methods for monitoring devices, such as routers, switches, and load balancers.
Windows	Tests key aspects of Microsoft® Windows® operating systems.
Resource	Tests finite system resources and alerts before consumption becomes critical.
Uptime	Tests the availability of popular TCP/IP protocol-based application-layer protocols, such as HTTP, HTTPS, SNMP, and so on.

## DNS names require lookup time

SolarWinds recommends minimizing the use of DNS names for TCP/IP-based monitors. You can time service-level response more accurately by removing DNS lookup from the equation. Some exceptions apply to monitors that require access to the Windows files system, and HTTP-based monitors.

If your network uses a Dynamic Host Configuration Protocol (DHCP) server to automatically assign IP addresses, enter an IP address only if it is reserved. Otherwise, enter a domain name. If a monitor is configured to use an IP address and that IP address was dynamically assigned to another resource, the monitor would stop monitoring the target resource.

## How monitors work

Testing methods vary depending on the monitor capabilities and the test parameters you specify during the monitor configuration.







Incorporating flexible timing parameters allow you to intensify or lessen testing during each [monitor state](#). Each time a monitor test fails, the sequential failure count is incremented and checked against the configured number of failures allowed before generating an alert. A successful test 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 yes, action parameters and action schedules are checked for actions within the alert.
3. Any active actions are carried out.

## Monitor states

The following table lists the monitor states.

ICON	MONITOR STATE	DESCRIPTION
 Green	Up and Listening	The device is responding as expected or ipMonitor is listening for inbound SNMP traps.
 Amber	Warn	There is an unexpected result. Testing is in progress, but no alerts were 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 were sent.
 Light Gray	Suspended or in Maintenance	The monitor is disabled or in Maintenance mode.
 Dark Gray	Uninitialized	The monitor was not initialized. No testing has occurred.

You can view the state of a monitor by

- Accessing Live Reports in the Administrator dashboard. Monitors are sorted and color-coded based on their state.
- Accessing the Edit Monitor page. The monitor status is displayed at the top of the page.

## Scan the network

The Device Discovery Wizard searches for devices on your network and recommends resources to monitor.

Potential monitors you can add are based on the types of detected resources. Although recommended monitors can be added to an installation, you can customize the interface using the Add Device Wizard in the Device Discovery feature.

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

The Device Discovery Wizard allows you to:

- Control the discovery methods ipMonitor uses to perform the network scan
- Control the range of IP addresses that will be scanned
- Add non-standard ports to the list of ports that ipMonitor will probe
- Navigate through the list of returned items using the Add Device Wizard tree structure, which provides a visual representation of the device
- Use cached scan results to add monitors and groups to your installation over a period of time
- 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

The following table lists the Device Discovery Wizard options.

OPTION	DESCRIPTION
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.

## General monitor settings

All monitor types available in ipMonitor include the following configuration options:

- [Monitor submenu](#)
- [Monitor status](#)
- [Identification](#)
- [Timing](#)
- [Notification Control](#)
- [Recovery parameters](#)

### Monitor submenu

The Monitor submenu allows you to perform maintenance actions, configure a downtime simulator, view a report, access the Relations page, and open a new window to display the monitor configuration settings in XML format.

The Monitor submenu is located at the top of each Edit Monitor page.

### Monitor status


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



SETTING	DESCRIPTION
Status	<p>The result of the last test performed by the monitor.</p> <p>Different monitor types generate specific test results and error codes based on the monitor capabilities. See the specific monitor section for a detailed explanation of the test results and reported error codes.</p>
Availability	The percentage of time the monitor has been available. This calculation is based on the coverage time.
Coverage	<p>The total length of time ipMonitor has been monitoring the resource. This value is reset when ipMonitor is restarted.</p> <p>Coverage excludes any period while the monitor is suspended, disabled, or in maintenance mode.</p>
Duration	The length of time since the monitor changed operational states. This includes time elapsed since scheduled maintenance.

## Identification

The Identification setting defines the monitor name and instructs ipMonitor to store statistics.

SETTING	DESCRIPTION
Monitor Name	<p>The name of the monitor.</p> <p>Because ipMonitor does not use the name field to identify the monitor internally, monitor names can be changed at any time without data loss.</p> <div>  Monitor names cannot be greater than 64 characters.         </div>
Store Monitor Statistics for Recent Activity and Historical Reports	When selected, ipMonitor records the test results used to generate recent activity and historical reports.

## Timing

Timing parameters allow you to intensify or lessen testing during the monitor Up, Warn, Down and Lost states. For example, you can intensify testing when a monitor enters a Warn state and reduce testing when a monitor enters a Lost state.

SETTING	DESCRIPTION
Maximum Test Duration	The method used to time out a monitor test.

SETTING	DESCRIPTION
	If a response is not returned within the defined number of seconds, the test fails.
Delays Between Tests While: Up	The number of seconds between each test while the monitor is in an Up (or OK) state.
Delays Between Tests While: Warn	The number of seconds between each test while the monitor is in a Warn state (a problem has been detected).  Alerts are not processed during the Warn state.
Delays Between Tests While: Down	The number of seconds between each test while the monitor is in a Down state (a failure has been confirmed).  Alerts are processed during the Down state.
Delays Between Tests While: Lost	The number of seconds between each test while the monitor is in a Lost state (the resource continues to be down and the maximum number of alerts have been processed).  No further alerts will be processed until the monitor recovers.

## Notification Control

Notification Control determines how many test failures must occur before an alert is sent, as well as the maximum number of alerts that will be sent.

SETTING	DESCRIPTION
Accumulated Failures per Alert	Each time a monitor test fails during a Warn state, the sequential failure count is incremented and checked against the accumulated failures per alert that must occur before alerting can take place. A successful test at any point resets the accumulated failure count to zero.
Maximum Alerts to Send	The number of alerts to process during a Down state before changing the monitor state to Lost.  A successful test by the monitor at any point while in the Down or Lost state will cause the alert sequence to be reset. SolarWinds recommends enabling Send Recovery notifications within alerts to notify you when the monitor recovers.

## Recovery Parameters

Use recovery parameters to take corrective action to automatically restore a failed resource using:

- External Process Recovery alert
- Reboot Server Recovery alert
- Restart Service Recovery alert


Although recovery alerts are responsible for executing the corrective procedure, you must define the recovery parameters in the monitor that triggers the alert. Maximum recovery coverage is possible because a one-to-one relationship exists between each monitor and the resource it is testing. Additionally, a single recovery alert can service many individual monitors because recovery parameters are passed to the recovery alert by the monitor.

In the FQDN/NetBIOS/IP Address field, enter the fully qualified domain name, NetBIOS name, or IP address of the computer that will be rebooted by the Reboot Server alert, or the computer hosting the Windows service that will be restarted.


 The Reboot Server and Restart Service alerts require this field.

Use the Credential for Recovery parameter to enable a specific credential to be used when executing Recovery alerts that require access to restricted resources such as Windows Services.

Click New Credential to start the New Credential wizard.

 The Reboot Server alert, Restart Service alert, and External Process alert require you to select a credential. If a credential is not assigned, ipMonitor uses the Microsoft Windows account assigned to the ipMonitor service. In this scenario, your results depend on the level of access the ipMonitor service account has to resources through the network.

Use the Windows NT Services parameter to define the list of Windows Services to restart.

 If a service has dependencies, you must select ALL dependent services. The Restart Service alert requires this parameter.

## Downtime simulator

Use the Downtime Simulator to test your monitor before you roll it out. This process allows you to test the alerting process and confirm the alert coverage for a specific time of day.

The Downtime Simulator runs a synthetic failure by:

- Applying the configuration parameters of the monitor
- Scanning each alert to find any associations with the monitor
- Checking range parameters and schedules for actions within the alert
- Carrying out any active actions

## What the Downtime Simulator reports



Use the following columns to help you pinpoint a problem.

COLUMN	DESCRIPTION
Queued	Indicates whether an action will be attempted or triggered.
Enabled	Indicates whether an action has the appropriate Send Failure Notifications or Enable Recovery Action message selected.
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	<p>indicates whether the Alert Range setting corresponds to or includes the alert count number sent by the failing monitor.</p> <p>You can use configurable alert ranges to receive all or some alerts when a problem occurs.</p>

## How the Downtime Simulator works

The Downtime Simulator uses Timing and Notification Control parameters to control the failure and alerting process for each monitor.

The following example uses the Monitor Timing and Notification Control parameters.

**Timing**  

Maximum Test Duration

seconds

Delays Between Tests While:

Up

seconds

Warn (failures but not alerting)



seconds

Down (alerts in progress)

seconds

Lost (no alerts permitted)

seconds

**Notification Control**  

Accumulated Failures per Alert

Maximum Alerts to Send

The following table provides an example of the alerting process. Three failed tests must accumulate before each alert is sent. The Maximum Alerts to Send value is set to 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?
	<b>Restart IIS</b> 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?
	<b>Restart IIS</b> 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?
	<b>Restart IIS</b> NO NO YES YES
	XYZ Admin Email Alert YES YES YES YES
Sat, 09:51:50	Waiting 5 mins, 0.00 secs ...

In the Time values column, 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, the value is 10 seconds.

In the Downtime Simulator Time column, look at the Timing parameters for the monitor. In this example, we used the default setting of 300 seconds for each Monitor State, but the time of each test increments by 310 seconds (five minutes ten seconds). This is explained using the following formula:

10-second Average Test Duration + 300-second Delay Between Tests

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

 In a real-world scenario, the numbers in the Time column would be much more variable. 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.

## Configure the Downtime Simulator

Enter Edit mode for the specific monitor you want to test, and then click Downtime Simulator on the submenu bar. If you make any changes to the simulation settings, click Update to refresh the Simulation Results.

OPTION	
Downtime Duration	Enter the number of downtime minutes to simulate. 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 allow for each test in the simulation. This is displayed in the Time column.

If you enter a Downtime Duration for the Downtime Simulator value that includes an extended amount of time, you will see several red Lost tests. If you enter a value that is too short, you will not see any Lost tests. The Warn and Down states may also be truncated.

The Up (green) state at the bottom of the downtime simulation displays alert information when the monitored resource recovers.

You can save the Downtime Simulator configuration parameters for your account when you log out. Press the Shift key and click either Logout this session or Logout all sessions.

## Downtime Simulator example of an IIS restart

You can use alert ranges to escalate an action to another administrator or automatically take corrective action when a problem is not resolved in a reasonable amount of time. For example, when you use an HTTP monitor on a Microsoft Internet Information Services (IIS) server, the following results occur:

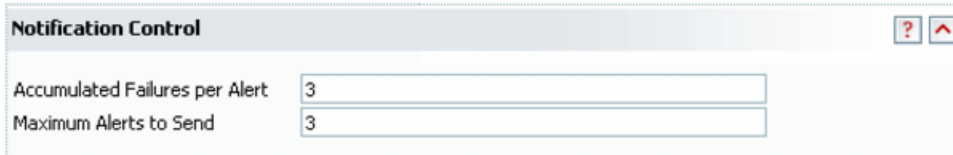
- ipMonitor sends an email to notify the web administrator of the problem.
- The IIS service is automatically restarted if the administrator does not respond in a timely manner.
- The administrator receives an email indicating if the web server has recovered. This action occurs when Send Recovery Notifications is enabled for the email action.

Below is an example of an IIS restart in the Downtime Simulator.

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?
	<b>Restart IIS</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>	<b>NO</b>
	XYZ Admin Email Alert	YES	YES	YES	YES
Sat, 09:10:30	Waiting 5 mins, 0.00 secs ...				

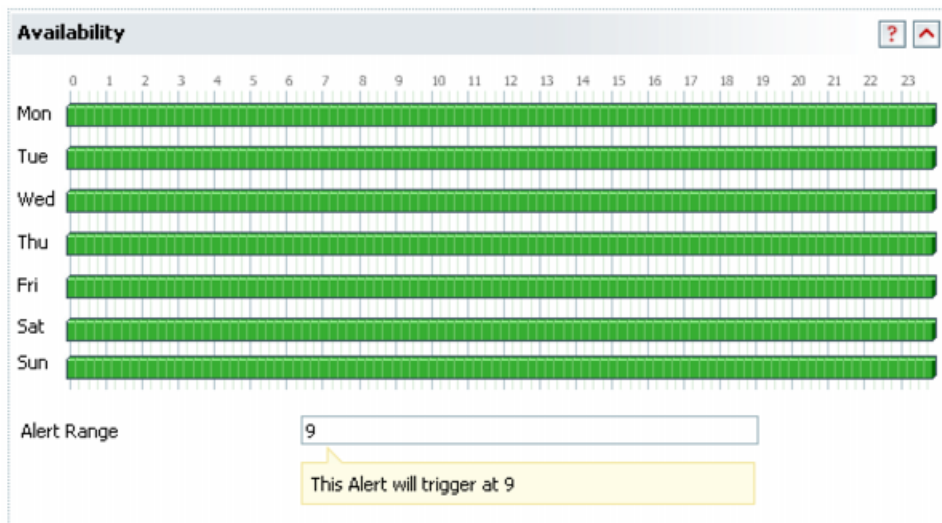
The bold text indicates a problem with the action. Viewing each of the failure notifications sent by the monitor in this simulation, notice that the Restart IIS action is displayed in bold. The Enable Recovery Action option is selected, and is scheduled for availability at this time. However, the action is not queued because its Alert Range value is out of range.

The monitor states the Maximum Alerts to Send value is 3.



The Notification Control dialog box contains two input fields. The first field, labeled 'Accumulated Failures per Alert', has the value '3'. The second field, labeled 'Maximum Alerts to Send', also has the value '3'. There are help and close buttons in the top right corner.


The problem is in the alert range for the Restart IIS alert, which is set to 9.



To ensure the proper alert escalation occurs, reset the Maximum Alerts to Send value to 9.

# Group dependencies

You can group multiple individual monitors together to assign 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.

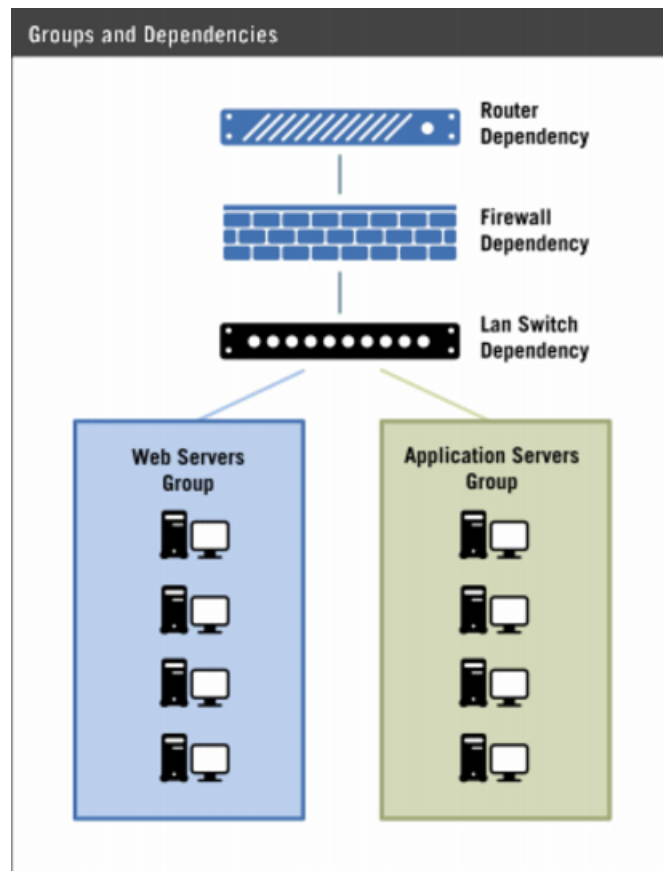
Dependencies define the relationship between critical resources and resources that depend on them for all or part of their functionality. A router, switch, server computer, or stable path to another network would all be valid dependencies.

Defining dependency relationships allows you to:

- Minimize the number of redundant alerts
- Isolate the root cause of the problem
- Prevent configured recovery alerts from attempting to restart services and applications if such an action is not required

For example, consider a web solution comprised 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 fails or becomes unavailable, all member monitors for both groups would be affected, generating several alerts.

When you define the switch monitor as a dependency, only the switch failure triggers an alert. This helps you:

- Isolate the root cause of the problem
- Minimize the number of unnecessary alerts
- Ensure 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, individual group members can still trigger alerts. 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.

**i** After a dependency monitor reaches the Down state, members that are currently in an Up or Warn state will not reach Down or Lost state. When all dependencies return to an Up state from a Down state, all alerting functionality is restored.

# Groups

You can assign monitors to multiple groups. For example, you could assign a PING monitor that traverses a network switch as a dependency to many groups that depend on the availability of the switch.

A group inherits the most critical state of any monitor assigned to it, including dependency monitors. 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 monitor state progresses to Down, the state of the entire group becomes Down.

## 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. By default, all new devices are automatically added to the All Managed Devices group. This group is required for ease of management, and acts as the parent for all network devices. This group cannot be deleted, nor can ipMonitor be configured to operate without it.

In environments with 50 or more monitors, the All Managed Devices group is never assigned to an alert. It is only used to add members to your subsequent groups, which are assigned to alerts.

In environments with less than 50 monitors, the All Devices group may be the only group you need. You can apply dependencies and an alert to this group to prevent unnecessary actions and help locate and resolve problems in a timely manner.

## Orphaned Objects group

The Orphaned Objects system group serves as a temporary container for monitors and groups that do not have valid parent objects. Monitors 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 or group:

1. Select the orphaned monitor, and click Move.
2. Select a device from the Destination Device or Group list, and then click Continue.  
The monitor is moved and assigned to the destination device or group.

# Monitor types

The following table lists the monitors included with ipMonitor.

ACTIVE DIRECTORY	IRC
<a href="#">Bandwidth Usage</a>	Kerberos 5
<a href="#">Battery</a>	LDAP
<a href="#">CPU Usage</a>	Link - User Experience
<a href="#">DNS User Experience</a>	Lotus Notes
<a href="#">DNS TCP</a>	MAPI - User Experience
<a href="#">DNS UDP</a>	Memory Usage
<a href="#">Directory</a>	Network Speed
<a href="#">Drive Space</a>	NNTP
<a href="#">Event Log</a>	NTP
<a href="#">Exchange Round Trip-Trip Email Wizard</a>	Ping
<a href="#">Exchange Server 2000</a>	POP3
<a href="#">Exchange Server 2003</a>	
<a href="#">Exchange Server 2007</a>	POP3 - User Experience
<a href="#">Exchange Server 2010</a>	Printer
<a href="#">External Process</a>	RADIUS
<a href="#">Fan</a>	RWHOIS
<a href="#">File Property</a>	Service
<a href="#">File Watching</a>	SMTP
<a href="#">Finger</a>	SNMP
<a href="#">FTP</a>	SNMP - User Experience
<a href="#">FTP User Experience</a>	SNMP Trap- User Experience
<a href="#">Generic WMI Monitor</a>	SNPP

<a href="#">Gopher</a>	SQL:ADO
<a href="#">HTML / ASP</a>	SQL:ADO - User Experience
<a href="#">HTTP</a>	SQL Server
<a href="#">HTTP User Experience</a>	TELNET
<a href="#">HTTPS</a>	Temperature
<a href="#">Humidity</a>	WHOIS
<a href="#">IMAP4</a>	Windows
<a href="#">IMAP4 - User Experience</a>	
<a href="#">ipMonitor</a>	


## Active Directory

Active Directory is the directory service included with Microsoft® Windows® and Windows Server® operating systems. Active Directory provides a centralized location to store information about networked devices, services, and users. It also provides a means to securely add, modify, delete, and locate data in the directory store.

Active Directory resolves domain object names to object records using Lightweight Directory Access Protocol (LDAP) search or modify requests.

Use the Active Directory monitor to:

- Establish a connection to the Active Directory service
- Send a bind request to make an LDAP v2 request
- Send a search request to determine which LDAP versions the Active Directory Service supports
- Send an unbind request for the Active Directory server to close the TCP connection
- Test if a server adheres to the Active Directory protocol by responding with the correct codes
- Test that the server responds within a required number of seconds

 The Active Directory monitor supports LDAP2—the most commonly supported version.

## Bandwidth Usage

The Bandwidth Usage monitor uses RPC or SNMP communications to measure the amount of inbound and outbound traffic traveling through a network interface on the local machine, a remote Windows computer, or an SNMP-enabled device.


Use the Bandwidth Usage monitor to:

- Test the bandwidth rate over time to distinguish between a steady increase in network usage and a sudden data spike
- Detect heavy bandwidth utilization
- Alert administrators if bandwidth usage exceeds a specified threshold
- Determine the amount of traffic used by a resource uses on the network
- Configure bandwidth monitors to test only the incoming or outgoing data rates
- Monitor the inbound and outbound traffic separately

The Bandwidth Usage Monitor wizard is designed to help you configure a Bandwidth Usage monitor with the least amount of initial input. Using the wizard, you can test all parameters in a production environment to ensure the monitor works as expected.

### Test results

The following table lists the test results when the Monitor is in an Up state.

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

TEST RESULT	DESCRIPTION
In	Inbound data received by the server displayed in kilobytes (KB).
Out	Outbound data sent by the server displayed in kilobytes (KB).
KB/s	Current amount of bandwidth consumption displayed in KB/s (1024 bytes per second).
KB/s-avg	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	Current amount of bandwidth consumption displayed in kb/s (1000 bits per second).
Kb/s-avg	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.
Total Bandwidth	Total inbound and outbound data.

# Battery

The Battery monitor uses SNMP communications to test the remaining charge in a UPS battery.

Administrators can use the Battery monitor to:

- Send a notification when a power outage occurs
- Determine the remaining charge in the battery
- Determine battery health and current operational conditions

Use this monitor to extend the running time of servers and components in your organization.

## Test results

When the Monitor is in an Up state, test results are reported as Capacity. This value (in percentage) indicates the current capacity of the UPS battery being monitored

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 system running Microsoft® Windows® or Linux, or an SNMP-enabled device.

Use the CPU Usage monitor to:

- Detect heavy CPU utilization before it impacts system performance
- Alert administrators wne the CPU utilization exceeds the specified threshold

## Test results

The following table lists the test results when the monitor is in an Up state.

TEST RESULT	
Usage	The CPU load currently on the system represented as a percentage (%).
Usage-avg	The average CPU load on the system represented as a percentage (%). This result 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 verifies that the primary and secondary DNS servers can respond to a record query in a timely manner.

This monitor uses the Universal Datagram Protocol (UDP)—the primary method of communication with DNS servers. The monitor alternately queries the primary and secondary DNS servers for a domain name until a DNS responds or the Maximum Test Duration time expires.

The results of the domain name resolutions are compared against a list of expected IP addresses. The result sets are verified in one of two ways:

- They must include all of the IP addresses in the expected list
- They must have at least one of the IP addresses in the expected list

The monitor considers the test to have failed if these conditions are not satisfied or if both DNS servers fail to respond within the Maximum Test Duration time.

To use the DNS User Experience monitor to test, verify that:

- At least one DNS server is Up and running
- The primary DNS server, the secondary DSN server, or both servers can respond to a domain name query, perform a lookup, and resolve a host name
- The results of the resolved domain name correctly corresponds to the expected IP address
- The complete round trip time until the response is received is within a specific number of seconds

## DNS TCP

The DNS TCP monitor verifies that the DNS server can respond to a record query within a timely manner.

This monitor uses the Transmission Control Protocol (TCP), which is the secondary method for DNS server communications. Because 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, this process is considered less efficient for 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 the round trip time by sending a query for the root server A Record at <http://a.root-servers.net> to the specified DNS server and waiting for a response. The monitor test will pass if the monitor receives a valid positive or negative response within the required timeout period.

Use the DNS TCP monitor to:

- Test if the DNS server is Up and running and able to process and respond to a query
- Test if the response makes a complete round trip within a predetermined number of seconds

# DNS UDP

The DNS UDP monitor verifies that the DNS server can respond to a record query within a timely manner.

The DNS UDP monitor uses the Universal Datagram Protocol—the primary method of communication with DNS servers. ipMonitor measures round trip time by sending a query for the root server A record located at <http://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.

Use the DNS UDP monitor to:

- Test that the DNS server is Up and running and able to process and respond to a query
- Test if the response makes a complete round trip within a predetermined number of seconds

## Directory

The Directory monitor detects modifications to a directory structure and alerts you when the structure changes beyond a predetermined limit.

The monitor tests the directory properties to determine whether:

- The directory exists
- Files were added or removed from a directory
- The directory size changed.
- Changes were applied to sub-directories

The Directory monitor tests the structure and content of a directory at periodic intervals to detect any changes outside your predetermined limits. When a change occurs, the Monitor can trigger a:

- Failure Notification alert
- Information alert
- A Failure Notification and Information alert

Configuring Information alerts is an optional process. You can configure the monitor to send an Information alert but remain in an Up state, even if a change is detected by separating Information alerts from monitoring actions and Failure Notifications. This process gives you maximum flexibility to configure each directory monitor to meet your specific needs for all tested directories.

Use the Directory monitor to:

- Monitor allotted storage space in a user directory
- Detect whether critical files were removed from a directory
- Ensure that all required backups are completed



- Monitor files that could potentially grow large enough to impact disk space
- Monitor directories containing files that are likely to grow and multiply at a rapid rate

## Drive Space


The Drive Space monitor uses a remote procedure call (RPC) or SNMP communication to test the amount of available drive space on a specified drive, share, or mount. If the available space is less than required, a failure state occurs.

Using the RPC communication method, the Drive Space monitor can monitor any host machine running a supported Microsoft® Windows® operating system. See the [ipMonitor Installation Guide](#) for operating system requirements.

Using the SNMP communication method, the Drive Space monitor can monitor any SNMP-enabled host machine running a supported Windows operating system or UNIX and UNIX-like operating systems (such as Linux, Solaris, HP-UX, and so on). See the [ipMonitor Installation Guide](#) for operating system requirements.

Use the Drive Space monitor to:

- Ensure that critical resources do not run out of drive space
- Automatically take recovery actions to free up drive space

 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 manually make any required configuration changes.

## Test results

The following table lists the test results when the monitor is in an Up state.

TEST RESULT	DESCRIPTION
Space	The monitored available space reported in gigabytes (GB) and megabytes (MB).
Avail	The monitored available space reported as a percentage (%) of the entire drive.

## Event Log

The Event Log monitor locates information within Error, Warning, Information, Success Audit and Failure Audit events that are recorded in the Microsoft Windows event logs.

The following logs can be monitored for any server or workstation version of Windows:

- Application log
- Security log
- System log

The following additional logs can be monitored for computers running as a domain controller:

- Directory service log
- File Replication service log

The DNS server log can be monitored for computers running as a Domain Name System (DNS) server.

The Event Log monitor uses header information to locate specific events. However, the description is often the most useful piece of information because it indicates problem occurrence 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 (regex) 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 displays ipMonitor events relating to the monitor status. It does not display the events captured by the Windows Event Log monitor.

If you need a history of events captured by the Windows Event Log monitor, create a Text Log action to record the information messages generated by the monitor.

1. Click the Configuration tab.
2. Click Alert List.
3. Click an alert.
4. In the Add Action menu, click Text Log.
5. In the Action Name field, enter:  
`Text Log Action`
6. Enter the file name and directory for the log file. For example:  
`eventlog.txt C:\.`
7. Select Send Information Messages.
8. Click OK.

## Tests on Event Log monitors differ from other monitors


When you create a new Event Log monitor, the monitor starts searching forward from the time of creation. It does not search historical content currently in the Event log file.

When you configure your monitors, you can suspend and then unsuspend a monitor to force an immediate test. This procedure does not work with the Event Log monitor because its pointer resets to its current time—or essentially the end of the log file. A real event needs to occur for the monitor to send an Information alert.

However, the Preview test searches the content in the Event log, which is ideal for configuration and troubleshooting purposes.

## Recommended default timing interval

SolarWinds recommends using the default 300 second timing intervals between scans. 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. The 300-second interval is a good balance between the length of time it takes to query the Event Log and the load placed on the target machine's CPU.

 Setting the timing interval below 180 seconds can generate security and authentication issues, especially in situations where multiple event log monitors target a single machine using a credential that impersonates a domain account.

## Exchange Round-Trip Email wizard

The Exchange Round-Trip Email wizard configures an IMAP4, POP3, or MAPI User Experience monitor with the least amount of initial input. Using this wizard, you can test all parameters you enter along the way to make sure that the new monitor will work as expected before going live in a production environment.

Before you create a MAPI User Experience Monitor using this wizard, ensure that:

- The monitor can access the Microsoft Outlook messaging subsystem. A full Microsoft Outlook version that supports the MAPI protocol must be installed on the ipMonitor server. Microsoft Outlook does not need to be running for the monitor to function correctly.
- You have a Microsoft Outlook email account under the default mail profile of the Windows user account impersonated by the monitor.

## Exchange Server 2000 and 2003

The Exchange Server 2000 or 2003 monitor opens a connection to a database server running a Microsoft Exchange Server and tests its subsystem performance to determine the server's general health. The overall server performance is typically dictated by its weakest performing subsystem.

Administrators can use this monitor to:

- Use pre-configured performance counters provided by the Windows Management Instrumentation service to test multiple Exchange Server subsystems at once
- Identify any performance degradation in critical Exchange Server components
- Determine the exact point of failure
- Take corrective action before email outages occur

## Exchange Server 2007 and 2010

The Exchange Server 2007/2010 monitor opens a connection to a database server hosting Microsoft Exchange Server 2007 or Exchange Server 2010 and tests the performance of its subsystems to determine the server's overall health.

Administrators can use this monitor to:

- Implement pre-configured performance counters provided by the Windows Management Instrumentation service to test multiple Exchange Server subsystems at once
- Identify any performance degradation in critical Exchange Server components
- Determine the exact point of failure
- Take corrective action before email outages occur

## WMI requirements

The Exchange Server monitor requires Windows Management Instrumentation (WMI) to be enabled. Also, the remote server must be accessible through an RPC connection to run the WMI queries.


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

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

## Troubleshoot WMI

1. Verify that the RPC service is enabled and started on the remote system
  - a. Log on to the target server as an administrator.
  - b. Open Windows Services.
  - c. Verify that the Remote Procedure Call (RPC) service is enabled and started.

2. Verify that DCOM is enabled and configured correctly on the remote system.
  - a. Log on to the target server as an administrator.
  - b. Navigate to Start > Control Panel > Administrative Tools > Component Services.

 In the Control Panel, switch to Classic View to use this navigation path.
  - c. Expand Component Services > Computers.
  - d. Right-click My Computer and 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. In the Launch and Activation Permissions grouping, click Edit Limits.
  - j. Ensure the user account you want to use to monitor resources over WMI has Local Launch, Remote Launch, Local Activation, and Remote Activation enabled, and then click OK.
  - k. Click Edit Default.
  - l. Ensure the user account you want to use to monitor resources over WMI has Local Launch, Remote Launch, Local Activation, and Remote Activation enabled.
  - m. 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 targeted server as an administrator.
- b. Navigate to Start > Control Panel > Administrative Tools > Computer Management > Services and Applications.


 Switch to Classic View in the Control Panel to use this navigation path.

- c. Select WMI Control.
- d. Right-click WMI Control and select Properties.
- e. Select the Security tab, expand Root, and click CIMV2.
- f. Click Security and select the user account used to access this computer.
- g. Grant the following permissions:
  - Enable Account
  - Remote Enable
- h. Click Advanced and select the user account used to access this computer.
- i. Click Edit.
- j. In the Apply to field, select This namespace and subnamespaces and click OK.
- k. In Advanced Security Settings for CIMV2 window, click OK.
- l. In the Security for Root\CIMV2 window, click OK.
- m. In the Computer Management navigation pane, click Services.
- n. In the Services result pane, select Windows Management Instrumentation, and then click Restart.

4. If you are monitoring a target in a workgroup, disable remote User Account Control (UAC).

 This action 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.

5. Edit the registry.

 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.

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

6. If the target computer has Windows Firewall enabled, add a Remote WMI exception to allow remote WMI traffic through. See Connecting to WMI Remotely with VBScript on the Microsoft website located at <http://www.microsoft.com> for details.
  - a. Click Start > Run.
  - b. Execute the following command, and press Enter:  
`cmdclick`
  - c. At the command prompt, type the following command, and press Enter:  
`netsh firewall set service RemoteAdmin enable`
  - d. At the command prompt, type `exit` and press ENTER.

## External Process

The External Process monitor launches an external program or script. It can also launch a script using an executable program, such as a PuTTY link (`plink.exe`) or a Windows script (`cscript.exe`). Any required command line parameters can be passed to the third party executable on startup.

Administrators can use the External Process monitor 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 that its value is correct

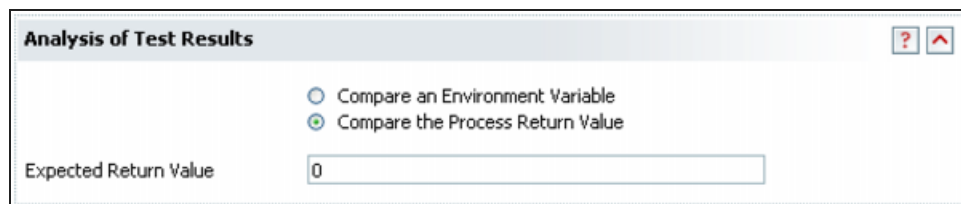
## Analysis of test results

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.



The screenshot shows a dialog box titled "Analysis of Test Results" with a question mark icon and an up arrow icon in the top right corner. Inside the dialog, there are two radio buttons: "Compare an Environment Variable" (which is unselected) and "Compare the Process Return Value" (which is selected). Below the radio buttons, there is a label "Expected Return Value" followed by a text input field containing the number "0".

When you create the third-party executable or script, design it so it produces an exit code when it shuts down.

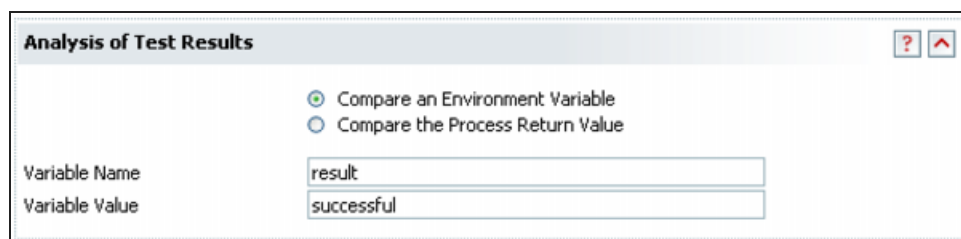
Although exit codes can be any number you choose in your program design, 0 is a standard success exit code used when an executable returns the expected value.

For example, if the target log file did not exist, the exit code 1 is returned to the ipMonitor process. This result does not match the Expected Return Value, causing the External Process monitor test to fail.

Alternatively, if exit code 0 is returned, the result matches and the External Process monitor continues 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.



The screenshot shows a dialog box titled "Analysis of Test Results" with a question mark icon and an up arrow icon in the top right corner. Inside the dialog, there are two radio buttons: "Compare an Environment Variable" (which is selected) and "Compare the Process Return Value" (which is unselected). Below the radio buttons, there are two labels: "Variable Name" followed by a text input field containing the word "result", and "Variable Value" followed by a text input field containing the word "successful".

Use Environment Variables when the content must contain file paths or special characters, such as less than ( < ) or greater than ( > ) symbols.

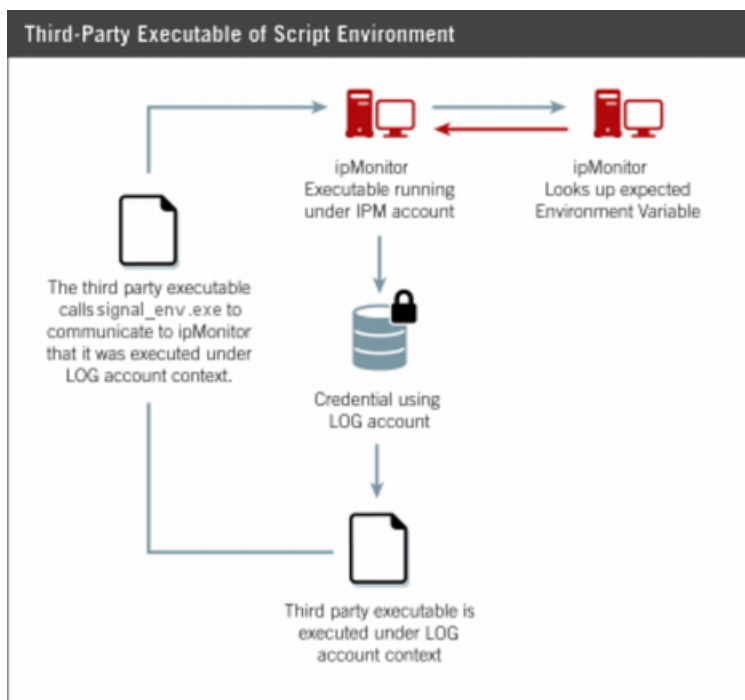
After setting the Environment Variable value, the third-party executable or script calls `signal_env.exe` for the variable to be available to the ipMonitor process.

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 monitored application or script runs.
2. During execution, the application sets the necessary Environment Variable and calls `signal_env.exe`.
3. The External Process monitor reads the Environment Variable and performs a comparison based on the monitor configuration.

In the following example, ipMonitor expects the result to equal to successful for the test to pass. Any other text string will cause the test to fail. This example illustrates the third-party executable or script environment.





The example 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 was run under the LOG account context.
- ipMonitor retrieves the LOG environment variables for comparison.

In the supported Windows operating systems, environment Variables are grouped internally into four variable categories:

- System
- Process
- User
- Volatile

System variables define the behavior of the global operating system environment. These variables apply to all machine users 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 processes. These are not stored in the registry.

User variables are only available when the user is logged in 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 login script execution. These apply to the current login session and are recorded in the registry at `HKCU\VolatileEnvironment`.

**i** ipMonitor can only set the PROCESS Environment variables to launch a script or executable through 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.

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

**i** SolarWinds recommends 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

The test results include return, which is the numeric exit code reported by the third-party executable.

# Fan


The Fan monitor uses SNMP communication to test the current fan status.

Administrators can use the Fan monitor to:

- Notify you when the fan is not functioning as expected
- Ensure that the server temperature remains within safe operating limits
- Determine the current fan health

Administrators can use this information to detect and resolve a fan issue in a timely manner before it can impact critical servers or other network components.

You can use the Fan Monitor wizard to test all parameters you enter along the way to make sure that the monitor will work as expected before moving to a production environment. If you prefer greater control over the process, you can clone an existing Fan Monitor and manually make any required configuration changes.

 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.

## File Property

The File Property monitor detects modifications made to a file and alerts you when these changes exceed a predetermined value.

You can use the File Property monitor to:

- Verify the existence of a file
- Determine whether a file has been modified
- Determine whether the size of a file has changed
- Detect 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, or both.

Configuring Information alerts is an optional process. You can configure the monitor to send an Information alert but remain in an Up state even if a change is detected by separating alerting actions from monitoring actions. 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

Test results include the current available space on the monitored share. 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. The pointer will be reset if the log file is reset.

 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 Force Test resets the testing cycle for the monitor, and you can 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. You can use ipMonitor 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 or 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 is created and saved, assign the new content generator to the File Watching monitor in the Information alert content menu, 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 user information program (RUIP) host for availability and its level of responsiveness.

The Finger protocol provides an interface to an RUIP by taking an email address as input and returning information—for example, the user is currently logged on.

The Finger monitor performs the following steps:

- Connects to the service, performs a blind query (CRLF) and waits for a response
- Considers the test successful if a valid response is returned within the specified Maximum Test Duration
- Safely disconnects from the server upon receipt of the opening message
- 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 the following:

- 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 the following:

- An FTP client can open a connection with an 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 an FTP server's ability to accept incoming sessions, process user logins, and then transmit the requested file.

Use the FTP User Experience monitor to ensure that the FTP server can perform the following:

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

FTP User Experience monitor features:

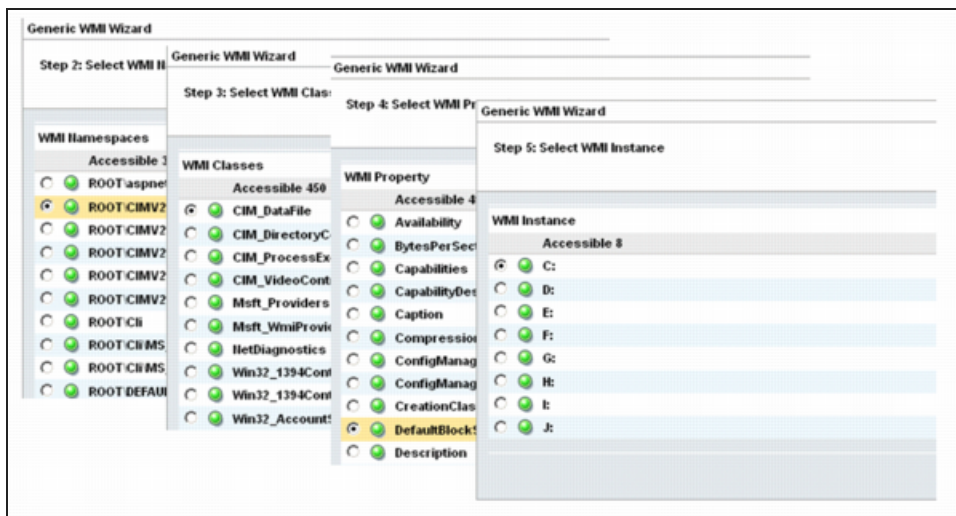
- Automatically log in to an anonymous FTP server
- Use a credential to log in to a private FTP server
- Supports either Active FTP or Passive FTP
- Perform a CRC comparison on the downloaded file to verify its contents

## Generic WMI

The Generic WMI monitor allows administrators to identify Windows operating system issues, application issues, and other potential issues.

Perform the following steps to define your WMI query:

1. Identify the host.
2. Select the following:
  - WMI Namespace
  - WMI Class
  - WMI Property
  - WMI Instance
3. Analyze the results.



## Gopher

The Gopher monitor tests a Gopher server for availability and responsiveness.

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

The Gopher monitor performs the following steps:

- Connects to the service, performs a blind query (CRLF), and waits for a response
- Considers the test successful if a valid response is returned within the specified Maximum Test Duration
- Safely disconnects from the server upon receipt of the opening message
- 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

Using the Gopher monitor, a Gopher client can open a connection with a Gopher server. The server adheres to the Gopher protocol by responding with the correct codes, and the server responds within a required number of seconds.

## HTML/ASP

The HTML/ASP monitor tests a web server to verify it can accept incoming sessions, generate a web page on the server side, and 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.

You can use the HTML / ASP monitor to:

- Monitor web-based applications for sales and customer service
- Access corporate databases and back-end applications

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



- Communicate with ipMonitor using the HTTP protocol
- Respond within a required number of seconds
- Run server side scripts, ActiveX components, access data sources, and so on to 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 the HEAD requests to save on bandwidth.
- Transmitting account and password information if required by the web server.

Test results

TEST RESULT	DESCRIPTION
Kps (kilobytes per second)	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 verifies that the web server can 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.

 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 the analysis.

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

Test results


The test results display HTTP status codes. Codes between 200 and 399 indicate success. Codes between 400 and 599 indicate an error.

# HTTP User Experience

The HTTP User Experience monitor verifies that a web server can 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 using the HTTP protocol
- Respond within a required number of seconds
- Access the source files and 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 that ipMonitor has on file

 This monitor can generate considerable bandwidth if aggressive timing parameters are applied. SolarWinds recommends keeping the default timing intervals of 300 seconds intact.

If you use log analysis or web analytics software, this monitor may generate hits. See your log analysis software for information on how to exclude ipMonitor from the analysis.

Test results

TEST RESULT	DESCRIPTION
Kps (kilobytes per second)	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 verifies that a web server can accept incoming sessions over a secure channel, generate a web page server side, and 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.

Using the HTTPS monitor, you can:

- Monitor secure web-based applications for sales and customer service
- Access corporate databases and back-end applications
- Search the delivered page for a specific text string
- Provide a warning before a server certificate expires
- Use HEAD requests to save on bandwidth
- Follow redirections until a valid file is transmitted or until an error occurs.
- Transmit account and password information when required by the web server.

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

## Humidity


The Humidity monitor uses SNMP communication to assess humidity levels in a specific area.

Administrators can use the monitor's ability to retrieve and analyze the response received from a humidity sensor to:

- Be notified when abnormal humidity conditions are detected
- Ensure that humidity levels in a specific area remain within safe operating limits
- Determine current humidity levels

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

The Humidity Monitor wizard can help you test the parameters you enter along the way to make sure that the monitor works as expected when enabled to go live in a production environment. If you prefer greater control over the process, you can clone an existing Humidity monitor and make any required configuration changes manually.

 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.

## Test results

The test results display the humidity level response (in percentage) received from the humidity sensor.

## 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.

When the monitor receives the message, it 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 whether 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 verifies that the SMTP server can receive and distribute email, and ensure that your end-users can log in from an IMAP4-enabled email client and manage their email.


The monitor uses the following process to simulate an email round trip and measure the time required for a series of transactions to occur:

1. Connects to port 25 on 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 verify 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

 ipMonitor uses a message with a special subject line to test the IMAP4 mail server send and receive functionality, similar to: 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:

- Perform internal diagnostics of the ipMonitor installation you specify.
- 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:

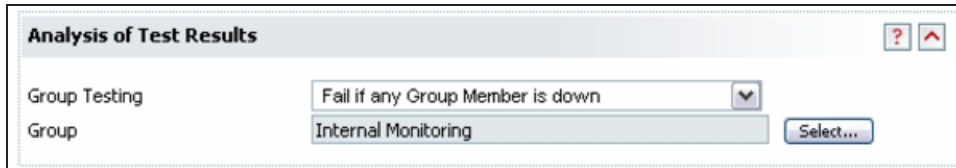
- Accept incoming sessions
- Conduct transactions via the HTTP or HTTPS protocol
- Respond within a required number of seconds

You can also use ipMonitor monitor 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.

#### Create redundant alerting

The ipMonitor monitor can 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

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

Force an immediate connection to the remote ipMonitor installation to obtain a list of groups that can be monitored by selecting a group from the list of groups displayed.

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

- IP address or domain name: ping and perform a traceroute to the remote ipMonitor installation to verify the connection.
- Port: ipMonitor can be installed on may 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.

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 verifies that the IRC server can accept incoming sessions, as well as its level of responsiveness.

IRC is a multi-person conversation system that allows you 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 performs the following steps:

1. Constructs both a user name and a nickname 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 the following:

- 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 verifies that an authentication server can 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. Authentication occurs before permission to access network resources is granted.

The Kerberos 5 monitor verifies that the Kerberos server can 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 time stamp, and other information such as flags.
- Measuring the round trip time to 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 is used to access stand-alone LDAP directory services or directory services that have an X.500 back end.

LDAP runs directly over TCP and stores information in a database structure about users, including the network privileges assigned to each user. You can revoke or change privileges using 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 LDAP version 2 client requests.

The LDAP monitor performs the following steps:

- Establishes an LDAP connection.
- Sends a bind request indicating that it is making an LDAP v2 request.
- Sends a search request asking which LDAP versions the LDAP server supports.
- Sends an unbind request for the LDAP server to close the TCP connection.

Use the LDAP Monitor to test the following:

- An LDAP client can open a connection with an 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 that the links can be successfully accessed by your website's visitors.

The requested page can be comprised of static HTML or dynamic pages, such as Microsoft Active Server pages, Cold Fusion pages, or PHP Hypertext Preprocessor pages.

To simulate a customer session, the monitor performs the following steps:

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.

You can use the Link - User Experience monitor to:

- Verify 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

TEST RESULT	DESCRIPTION
Links	The total number of links checked during the last monitor test.
Blocked	The total number of links 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 field
Kps (kilobytes per second)	Indicates the web server's transfer data rate.

## Lotus Notes

The Lotus Notes monitor verifies that a Lotus Notes mail server can accept incoming sessions, as well as its level of responsiveness.

The Lotus Notes monitor performs the following steps:

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 the following:

- 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 simulates a around trip email and measures the time it takes for a series of transactions to occur.

Using CDO or MAPI, a program can connect to a MAPI store and perform operations against that store.



This monitor performs the following steps:

1. The monitor connects to the SMTP server on port 25 and sends an email message to the specified recipient address.
2. The monitor logs in to 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 flags it for deletion.
4. The MAPI User Experience monitor sends a LOGOUT command to Exchange Server.

The test is considered 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 the following:

- 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.

## Microsoft Outlook account requirements

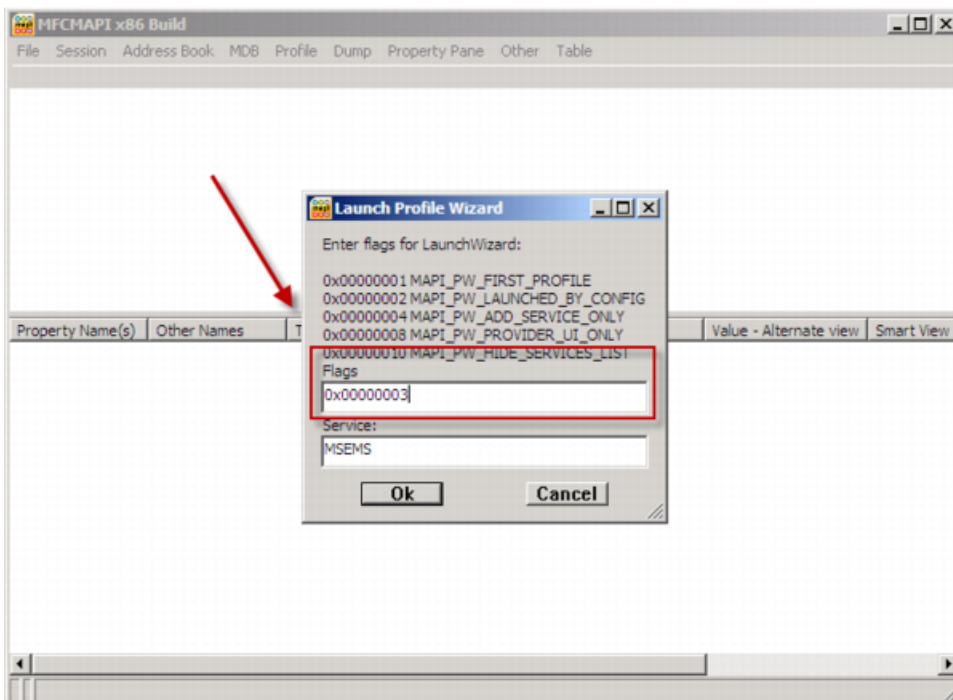
To operate correctly, this monitor requires the following Microsoft Outlook environment:

- Outlook 2007: SolarWinds recommends uninstalling Outlook from the host server and using a CDO to create a MAPI profile.
- Microsoft Outlook email account under the default Mail Profile of the Windows user account impersonated by the monitor

### Use the Microsoft CDO

The following applies to Microsoft Outlook 2007 Users. After installing the client, you can then use the MFC MAPI tool to create a MAPI profile.

When using the MAPI Profile wizard, you need to set the default flag on creation. This is done by setting the flag to 0x00000003 on the wizard parameters page.



## Set up a Windows Mail Profile

1. Log in to the ipMonitor server using the Windows Domain Account that will be used by the MAPI - User Experience monitor.
2. Install and launch Microsoft Outlook.
3. Follow the steps outlined in the Outlook Startup wizard to configure the default Mail Profile for the domain account.

When you configure the MAPI User Experience monitor, the monitoring credential should reference the Windows account used to log in to the ipMonitor server.

## 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:

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 a supported Microsoft Windows operating system
- A remote SNMP-enabled computer running a Unix-based operating system such as Linux, Solaris, HP-UX, and so on
- An SNMP-enabled device

The monitor effectively ensures that:

- Memory leaks are detected before performance is 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 help you configure a Memory Usage monitor with the least amount of initial input by testing all the parameters you enter along the way to make sure the monitor operates as expected in a production environment. If you prefer greater control over the process, clone an existing Memory Usage monitor and make any required configuration changes.


Test results

TEST RESULT	DESCRIPTION
Avail	Indicates the amount of physical memory available on the system in megabytes (MB) and percentage (%).
avail-avg	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 tests 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 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.

 SolarWinds recommends using the Network Speed in the safe zone of networks 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

TEST RESULTS	DESCRIPTION
kb/s	Indicates the network's transfer data rate, displayed in kb/s (1000 bits per second).
KB/s	Indicates the network's transfer data rate, displayed in KB/s (1024 bytes per second).

## NNTP

The Network News Transfer Protocol (NNTP) monitor verifies that a News server can 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 performs the following steps:

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 the following:

- An NNTP client can open a connection with an 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 Network Time Protocol (NTP) monitor verifies that the Network Time Protocol Service is available.

NTP is a vital resource for most networks. Clusters and other parallel processing environments depend on an accurate and synchronized Universal Time Coordinated (UTC) value. If your servers do not synchronize the current time with the NTP server, some enterprise applications may produce unexpected results.

The NTP monitor performs the following steps:

1. Opens a connection to the specified NTP server and waits for the service to respond.
2. Considers the test successful if a valid UTC time value is returned within the specified maximum test duration.
3. Safely disconnects from the server when the monitor receives the UTC time value.

4. Considers the test 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 verify that:

- An NTP client can open a connections 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 tests the availability of a specific computer or device on the Internet. The default interval is set to 60 seconds.

ipMonitor measures the 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 passes if the monitor receives a valid return packet within the required timeout period. The test fails if the monitor's specified timeout period expires.

The Ping monitor tests the following:

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

The Ping monitor is often used as a dependency for a group of monitors. For example, a web application group could include a web server, SQL server, drive space, and a Ping monitor that monitors the availability of the server computer.

In this example, you could assign the Ping monitor as a dependency for the web application group. If problems occur with the server, this configuration would prevent you from receiving alerts for all the application monitors and resource monitors configured to watch the server computer. This process would minimize the number of alerts you receive and help you identify the source of the problem.

## POP3

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

After the message is received, 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 the following:

- 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 verifies that your SMTP server can receive and distribute email and verify that your end users can log in from a POP3-enabled client and retrieve their email.

The POP3 - User Experience monitor uses the following process to simulate a round trip email, 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 the following:

- 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 Subject: ipm9:pop3:guid:141991169.

After ipMonitor logs in to the POP3 server on port 110 and retrieves the LIST of queued mail, it performs the following steps:

1. Retrieves up to a maximum of the 100 last emails.
2. Attempts to locate the email with the special subject line.
3. Makes several attempts to retrieve the email before the test expires.
4. Deletes the email after verifying the subject line to prevent email from accumulating on the POP3 server.

## Printer monitor

The Printer monitor uses the Host Resources MIB to retrieve statistics. You can use this monitor to alert on the following conditions:

- Low resources, such as low paper or toner
- Hardware malfunction, such as a paper jam or printer offline
- Maintenance service, such as service requested or overdue preventative maintenance

## RADIUS

The Remote Authentication Dial-In User Service (RADIUS) monitor verifies that an authentication server can 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 performs the following steps:

1. Test the ability of the RADIUS server to respond to an authentication request.
2. Send user credentials and connection parameters in a RADIUS message to the RADIUS server.
3. Wait for the RADIUS server to authenticate and authorize the access request.
4. Validate the RADIUS message response sent back.
5. Determine the responsiveness of the service by analyzing the round trip time.
6. Consider 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 log in to the RADIUS server using the account information provided during the initial configuration. It tests the authentication server to ensure it can perform an internal database lookup and respond to an authentication query.

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

## RWHOIS

The RWHOIS monitor tests a Remote WHOIS server for availability and 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 uses the following process:

1. Connect to the service and waits for the service to respond.
2. Consider the test successful if the RWHOIS server responds indicating that it is available within the specified Maximum Test Duration.
3. Safely disconnect 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 the following:

- An RWHOIS client can open a connection with an 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 remote procedure call (RPC) or SNMP communication to test whether a specified service is running on:

- A 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

Use the Service monitor to:

- Ensure that a critical service is not unexpectedly stopped
- Monitor the state of dependency services that must be running for a critical service to function
- Automatically take 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, 2000, XP, or 2003.

The Service Monitor wizard helps you configure a service monitor with the least amount of initial input. The wizard tests all parameters you enter along the way to make sure that the monitor runs as expected before going live in a production environment.

## Windows recovery options for services

The Windows Control Panel / Administrative Tools / Services / Recovery dialog helps you set recovery options that automatically restart the service, run a file, or reboot the computer.

The purpose of the Windows recovery options for services is similar to the ipMonitor 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 can alert you 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 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 inform you when Windows performs a recovery action based on the Windows recovery timing parameters you specify.
- Use the Event Log monitor to notify you when Windows takes recovery actions on behalf of a service.

## SMTP

The Simple Mail Transfer Protocol (SMTP) monitor verifies that the SMTP mail server can accept incoming sessions and respond in a timely manner.

To verify, the SMTP monitor uses the following process:

1. 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. When the monitor receives the opening message, the 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 verify that:

- A mail client can open a connection with an 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.

## Minimize the SMTP server load

SMTP servers are configured to perform a reverse lookup on all incoming connections. This process verifies that the IP address of the SMTP client matches the host or domain submitted when the connection is established.

Because the IP address of the SMTP monitor can be verified each time the server is tested, delays can occur when connecting to the server, or the load on your SMTP server can increase if aggressive timing parameters are used.

To avoid this issue, you can:

- Add a reverse DNS entry for the ipMonitor 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 verifies that an SNMP agent can respond to an information request in a timely manner.

ipMonitor measures the round trip time by sending a request for a fixed piece of information (such as sysUpTime OID 1.3.6.1.2.1.1.3.0) to the target SNMP agent and waits for a valid response. The monitor test will pass if the monitor receives a valid response within the required timeout period.

The SNMP monitor verifies that:

- The target SNMP agent is running and is 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 performs the following transactions:

- Retrieves a numeric or textual value from a SNMP agent.
- Tests the value against the rules you define.
- Performs delta comparisons.

## SNMP agent security

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

## SNMP - User Experience

The lightweight SNMP monitor verifies that an SNMP agent can respond to an information request in a timely manner.

ipMonitor measures round trip time by sending a request for a fixed piece of information (such as sysUpTime oid 1.3.6.1.2.1.1.3.0) to the specified SNMP agent and waits for a valid response. The Monitor test will pass if the monitor receives a valid response within the required timeout period.

The SNMP Monitor verifies 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 the following procedure:

- Retrieve a Numeric or Textual value from a SNMP agent
- Test the value against the rules you define
- Perform delta comparisons

### SNMP Agent Security

A commonly-used SNMP security feature requires you to specify which IP addresses can communicate with the SNMP agent. If this security feature is enabled on the SNMP agent you want to monitor, configure this feature to include the IP address of the ipMonitor host machine.

Another commonly-used SNMP security feature requires you to specify which IP addresses can communicate with the SNMP agent. If this security feature is enabled on the SNMP agent you want to monitor, configure this feature to include the IP address of the ipMonitor host machine.

## SNMP - User Experience wizard


The SNMP - User Experience monitor wizard help you configure an SNMP - User Experience monitor with the least amount of initial input. Using the SNMP - User Experience Monitor wizard, you can connect to an SNMP-enabled device and retrieve a set of SNMP-data without requiring an exact OID. Additionally, you can test all parameters you enter along the way to make sure that the monitor will operate as expected before you move to a production environment.

The following sections describe the screens that display in the wizard.

### 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:

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

 You can also select the SNMP wizard from the Configuration tab.

### Step 2: Select an SNMP object to monitor

Scrp;; through the returned set of objects and their corresponding values, and then click Select to select 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 you can perform in Analysis of Test Results section.

## Comparison rules

The type of data supported by the selected OID determines the possible methods of analysis. Use the object information outlined above to set the comparison rules and ensure the monitor will pass when enabled.

## Step 4: Name and configure your SNMP User Experience monitor

### Monitor Name

Enter a descriptive name for the new monitor using up to 64-characters. The monitor name will display in the Monitors List, Monitor Status, Reports and Logs pages. Because ipMonitor does not use the Name field to internally identify the monitor, you can change the monitor name at any time without losing your data.

### Parent Group - Create in Existing Group

When enabled, select an existing groups from the Selected Group list. The new monitor will automatically be added to this group.

### Parent Group - Create New Group

When enabled, type the name of the new group in the Group Name field. The new monitor will automatically be added to this group.

### Create Monitor Enabled

After you create the monitor, ipMonitor tests the target server or device using your configured settings. This option is enabled by default.

### Store Monitor Statistics for Recent Activity and Historical Reports

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

### Finish

Click Finish to exit the wizard and access the new monitor in edit mode. You can make any final modifications to the monitor (including the timing and notification parameters) in this mode.

After you complete this step, click OK. The new monitor displays within the Monitors List.

## 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 received data.

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

1. ipMonitor listens for incoming traps sent by SNMP agents. These traps provide networking information for servers, applications or devices on the network.
2. ipMonitor parses the Protocol Data Unit (PDU) message it receives from each trap using the Trap Filtering settings for each configured SNMP Trap User Experience monitor to determine whether the trap applies to it.
3. If the incoming trap applies to an SNMP Trap User Experience monitor, it triggers an alert.

Optionally, you can configure the SNMP Trap - User Experience monitor to examine the variable binding information within a trap. For example, the monitor can search for temperature information, remaining battery power, an application error condition, and so on. Any retrieved variable binding information can be parsed by a content generator you created and pushed to any alert type in ipMonitor that supports Information alerts.

## Integrate 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 integrate with your SNMP-enabled network management solutions. Incoming SNMP traps can be processed into alerts for notification, integration, and recovery.

## Turn on the SNMP Trap Listener

SNMP trap listening is disabled by default. This ensures that ipMonitor properly co-exists with the existing network management software.

1. Launch the ipMonitor configuration program from the ipMonitor program group.
2. Select Communications: Web Server Ports.
3. In the SNMP Trap Listener section, enter a listening IP address and port (UDP) for all SNMP Trap User Experience monitors.
4. Select the Enabled option.

 Any agent you configure to send traps to ipMonitor must use the 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 can conflict with ipMonitor's SNMP Trap Listener. Both are bound by default to port 162.

To resolve conflicts with the Windows SNMP trap service, perform one of the following procedures:

- Change the ipMonitor's SNMP Trap Listener port to an unused port, and then change the outbound port of all SNMP agents that will be sending traps to ipMonitor.
- Disable the Windows SNMP trap service from the Windows Control Panel interface. There are no adverse effects to disabling this service unless you are running another SNMP solution on the ipMonitor server that requires the Windows SNMP trap service.

## Use filters in the SNMP Trap monitor

The Trap Filtering dialog box helps you 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 includes the SNMP community string. If ipMonitor and the agent use the same read-only string, ipMonitor continues filtering traps and progresses to the IP range test.

The SNMP default communities are Private (read-write) and Public (read-only) .

You can use non-default community strings with some SNMP agents to improve the SNMP security model in conjunction with a non-standard SNMP port.

### IP address range

For security purposes, traps can be accepted based on a range of IP addresses.

For an IP address range, enter the start and end IP addresses that will be accepted for SNMP Traps. For a single IP address, enter the same start and end IP address.

Filter using the source address from within the SNMP TRAP packet, and not the IP Header To increase the flexibility of the SNMP Trap QA Monitor IP address filtering, two variations are supported. If you select this option, 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 you do not select this option, the SNMP trap QA monitor uses the IP address entered in the IP Header.

### Generic Type

The incoming Generic Trap field must be one of the predefined SNMPv1 Trap types listed in the following table. See RFC 1157 for details.

TYPE	DESCRIPTION
Any	Indicates that any of the Trap types listed below will be accepted.
coldStart(0)	Signifies that the sending protocol entity is reinitializing itself. As a result, the agent configuration or protocol entity implementation may be altered.
warmStart(1)	Signifies that the sending protocol entity is reinitializing itself. As a result, 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 configuration.
linkUp(3)	Signifies that the sending protocol entity recognizes that one of the communication links represented in the agent configuration is 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 is marked down and the peer relationship no longer exists.


TYPE	DESCRIPTION
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 that occurred.


## 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 the ipMonitor database of precompiled MIBs located in the Tools drop-down menu). MIB Information is provided for common Microsoft Windows and hardware applications.

To expand the default MIB database, use the [Common Database Builder](#) located on the Customer 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.

 The Custom Database Builder is only available to Licensed ipMonitor customers. For detailed instructions on compiling and importing a MIB database, see [Add a Custom MIB Database to your ipMonitor Installation](#) located in the Customer Portal.

 Contact your vendor to acquire MIBs for your various applications and equipment.

## Get Info

Click Get Info to query the ipMonitor built-in SNMP database for details about your OID. Type Information is ideal for determining the type of analysis you can perform in the Analysis of Test Results section.

## To OID

Click To OID to convert the readable label of the OID path into its standard numerical notation. For example, clicking To OID converts sysUpTime.0 to 1.3.6.1.2.1.1.3.0.

You can specify an Enterprise OID prefix 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

Use the Enterprise Specific Kind field 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 Add > Or for any subsequent entries. This makes it possible to send an alert based on more than one specific kind of trap.

# SNPP

The Simple Network Paging Protocol monitor verifies that an SNPP server is available and responsive.

SNPP deliver pages to individual paging terminals without modems and phone lines to deliver alphanumeric pages.

The SNPP monitor uses the following process:

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:

- An SNPP client can open a connection with an 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 verifies that:

- You can log in to an SQL database server or another supported data source
- Ample connection handles are available
- The specified account can log in to the database

Microsoft® ActiveX® Data Objects (ADO) provide 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 helps you configure an ADO monitor with the least amount of initial input by testing all the parameters you enter along the way. This process ensures that the monitor functions as expected before you move to a production environment.


## OLE DB provider requirements

The ADO monitor requires a supported OLE DB provider is 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

 Use the Other database type option to manually configure the ADO monitor and test other data sources, such as SAP DB, FrontBase, FoxPro, and LDAP.

Providers have different implementation requirements and guidelines. SolarWinds recommends consulting the documentation provided by the appropriate third-party vendors before you install the OLE DB providers.

## Verify your OLE DB provider

ipMonitor includes a Universal Data Link file that launches the Windows Data Link Properties dialog box to test connections between the ipMonitor host computer and OLE DB data sources.

The following example procedure shows how to verify that the SQL Server OLE DB provider is properly installed on the ipMonitor host machine and connectivity to the SQL Server can be established:

1. Double-click the `ipm7adotest.udl` file located in the `\ipMonitor` root directory.
2. In the Provider tab, select the correct OLE DB provider. If the required provider does not appear in the list, install the provider to enable ipMonitor to connect.
3. In the Connection tab, select the SQL Server instance and enter the login and database information.
4. Click Test Connection. If the test is successful, a Test Connection succeeded message is displayed.
5. Click OK to save the settings.

## SQL - ADO User Experience

The ActiveX Data Object User Experience monitor monitors an SQL database server or another supported data source from the end-user perspective to:

- Test login ability
- Perform a query
- Retrieve data
- Analyze results for correctness

The wizard helps you configure a monitor with the least amount of initial input by automatically creating the SQL statement using the information you provide. It tests the parameters you enter along the way to make sure that the monitor will work as expected before you transition to a production environment.

If you prefer additional control over the process, you can clone an existing ADO Monitor and apply any required configuration changes.

**i** The ADO - User Experience monitor requires MDAC 2.6 or later 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.

## Test results

The test results include rows dll, which displays 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 administrator interface.
2. Click Monitors > Add a Monitor.
3. Select the ADO-User Experience (SQL Query) monitor and click Continue.
4. Select a Database Type from the list.

**i** Properly-installed OLE DB providers can be selected for monitor configuration. OLE DB providers that are not installed on the ipMonitor host machine are displayed under Unavailable Database Types. Contact your vendor to obtain the correct OLE DB provider for your database type and install it before you continue.

Select the Other database type to manually configure the ADO - User Experience monitor to test other data sources such as SAP DB, FrontBase, FoxPro, and LDAP.

### Step 2: Data source location

Select the server that hosts the SQL Server database you want to monitor.

#### Use TCP/IP versus Named Pipes

Select this option to force ipMonitor to use TCP/IP instead of a named pipe to connect to a Microsoft SQL Server database. Enter the IP address and port of the server database in the Server Address field.

For example, xxx . xxx . xxx . xxx , 1433 where 1433 is the default port number for SQL Servers.

#### Use Data Encryption

Select this option to force ipMonitor to encrypt the data transmitted between the ipMonitor host machine and the database you are querying.

### Specify a Microsoft SQL Server Instance

Select this option to connect to a named instance of Microsoft SQL Server. Enter the instance name in the Server Address field.

### Step 3: Assign login credential

Select a credential to use while monitoring. Depending on the data source configured for the ADO monitor, some form of authentication to the data source will be required to connect and log in.

### Step 4: Select database

Select the database you will use 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 an SQL statement to query the database. You can supply your own SQL statement or have ipMonitor generate an SQL statement automatically based on your selected table columns.

#### 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 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, select an operator and number that will be used to test the number of rows returned by the query. Supported numeric tests include:

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

Use this option to perform textual or numeric analysis on the data contained in the specified column.

If the query result set returns more than one row, each row in the result set is examined sequentially from the first to last. All configured tests are performed on the column you select.

The test passes if any condition you select is met.

Examine column

When you select the column to examine, note that column 1 is the first column. Counting is 1-based, not 0-based. The data in the selected column can be a string or a number.

Column Will

Several numeric and text comparison methods are available, including regular expression and string matches. The comparison passes if the content of the column adheres to any method listed below.

METHOD	DESCRIPTION
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

Click Preview to display the data contained within the selected columns. Rows highlighted in red indicate a fail scenario. Clicking Stretch Table in the preview window expands the table to fit the selected content. If you chose to view a large number of columns, some content may be truncated unless you expand the resulting preview table.

## Step 8: Name Monitor

Enter a descriptive name for the new monitor.

Create Monitor Enabled

After the monitor is created, it begins querying the database with the selected configuration options. This option is enabled by default.

Store Monitor Statistics for Recent Activity and Historical Reports

ipMonitor begins to record test results, which are 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 configure the ADO User Experience monitor

The Test Parameters dialog box specifies the parameters used by the ADO User Experience monitor to open a data source connection.

The following example describes how to configure the ADO User Experience monitor to test the connection to a supported Microsoft SQL Server database server.

 See the ipMonitor Installation Guide for a list of supported SQL Server versions.

## Database Type

Select a database type from the ADO - User Experience monitor list of supported OLE DB providers.

## Credential for Monitoring

Based on the data source configured for the ADO - User Experience monitor, some form authentication will be required to connect and log in.

Typically, a credential is created and assigned to the ADO - User Experience monitor to impersonate the account information required to access and query the data source. If a monitoring credential is not assigned, ipMonitor uses the login privileges of the current Windows account assigned to the ipMonitor service.

To select a credential, click Select and select an existing credential from the Windows category. To create a new credential, click New Credential to start the wizard.

## Run this test from an external process

Enable this option to continue monitoring the database even if a temporary OLE DB connection problem occurs.

The following example configures the ADO User Experience monitor to a test Microsoft SQL Server database server. The following authentication methods are possible.

## SQL Authentication

Using SQL Authentication or Mixed Mode:

- Provider = sqloledb
- Data Source = ServerName
- Initial Catalog = DatabaseName

Create and assign a credential for monitoring that includes the user name and password required to authenticate. Select the May be used with ActiveX Data Objects (ADO) option in the Usage Restrictions section of the credential settings.


## Integrated Windows Authentication

Using Integrated Windows Authentication or Trusted Connection:

- Provider = sqloledb
- Data Source = ServerName
- Initial Catalog = DatabaseName
- Integrated Security = SSPI

Click AND to specify the additional Integrated Security = SSPI parameter.

A monitoring credential is required if the ipMonitor service account does not have sufficient rights to connect to the database server. Only select the May be used with Windows Impersonation for use with RPC option within the Usage Restrictions section of the credential settings.

 For specific configuration details about configuring a credential for the ADO - User Experience monitor, see Credentials Manager.

## Additional Connection Types

The ADO - User Experience monitor supports both the 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.

Click AND to specify the Integrated Security = SSPI parameter.

 To connect to an SQL Server 2000 named instance, the ipMonitor host machine must have MDAC 2.6 or later installed.

## TCP/IP Connection to SQL Server 2000

To connect to SQL Server 2000 using an IP address:

- Provider = sqloledb
- Data Source = xxx.xxx.xxx.xxx, 1433
- Initial Catalog = DatabaseName
- Network Library = DBMSSOCN


where:

- xxx.xxx.xxx.xxx is the IP address of the database server.
- 1433 is the default port number for the SQL Server. The IP address and port are separated by a comma.

Click AND to enter Network Library = DBMSSOCN, indicating that TCP/IP should be used instead of named pipes, and to enter Encrypt = yes, indicating that encryption will be used.

### SQL Statement

Enter the query statement that will be issued to the database server or data source.

 Do not end the SQL statement with a semicolon. The semicolon is automatically added by ipMonitor.

### Locking Method

Use the Locking Method menu 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.

Listed below are the locking method options.

OPTION	DESCRIPTION
Optimistic	Simultaneously edit a record, locking it only when an update is attempted.
Batch Optimistic	Required only when updating records in batches.
Pessimistic	Locks a record when the retrieval process is initiated.
Read Only	Prevents data from being modified.

## Analysis of Test Results

This section is used to validate the query results. It controls the number of rows that will be retrieved and the type of analysis the monitor performs on the result set.

Success can be determined strictly by retrieving up to a maximum of x number of rows. Examine the row count and row content for further analysis.

### Retrieve a Maximum of "x" Rows

The Retrieve Maximum Rows parameter controls the maximum number of rows that the query is permitted to return to the ADO - User Experience monitor for analysis. This allows you to:

- Control the impact on the SMP Server or data source being monitored.
- Reduce the network bandwidth consumed.
- Reduce the required amount of processing for ipMonitor.

### Examine the Row Count

Use this option to validate your results based on your configured numeric equation.

### Number of Rows Retrieved Must Be

Select an operator and enter a number used to test the number of rows returned by the query.

### Examine the Row Content

Use this option to perform textual or numeric analysis on the data contained in the specified column.

When the query result set returns more than one row, each row in the result set is examined sequentially from first to last. All configured tests are performed on your specified column.

The test passes if any condition you specify is met.


### Examine Column Number


When you specify 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.

 ipMonitor includes a RegEx wizard to help create regular expressions.

 Click AND or OR 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 dictated by its weakest performing subsystem.

Administrators can use the SQL Server monitor to:

- Use pre-configured performance counters provided by the Windows Management Instrumentation service to test multiple SQL Server subsystems at once
- Identify 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 Microsoft SQL Server, Windows Management Instrumentation (WMI) must be enabled and functioning properly. Additionally, the remote server must be accessible through an RPC connection in order to run the WMI queries.

Enabling cross-domain WMI without local accounts credentials can 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 cannot be exceeded.

Counters are tested in the order that they appear. If you experience multiple counter failures, only the first counter error encountered will be reported.

The SQL Server monitor's built-in internal sampling helps to combat counter spikes. The monitor issues the WMI query five times—once every second—and calculates an average based on the query results.

## TELNET

The TELNET monitor verifies that the TCP/IP-based service can accept incoming sessions and respond in a timely manner.

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 the following:

- 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 not directly supported by a monitor type. To test if the service or device is accepting sessions, select the correct TCP/IP port.

## Temperature

The Temperature monitor uses SNMP communication to check the temperature levels in a specific area. Administrators can use this monitor to:

- Be notified when abnormal temperature levels are detected
- Ensure that temperature levels in a specific area remain within acceptable limits
- Determine current temperature levels

If your server room cooling system fails, the temperature can climb rapidly in a short amount of time. Being aware of a temperature problem and resolving it as quickly as possible ensures that your critical servers and other network components are not damaged.

 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 were reduced from 300 seconds to 60 seconds between tests. The Ping default interval is set to 60 seconds.

The Temperature Monitor wizard can help you configure a temperature monitor with the least amount of initial input by testing all parameters you enter along the way. This process ensures that the monitor functions as expected before you enable it in a production environment. If you require additional control over the process, you can clone an existing temperature monitor and make any required configuration changes,

## Test results

The test results include temperature response received from the sensor, display in 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 Monitors > Add Monitor.
3. Select the Temperature monitor from the Resource Based category.

## Step 2: Select interface and monitoring thresholds

### Communication type

Using Simple Network Management Protocol (SNMP), the monitor can perform a lightweight transaction to communicate with SNMP-enabled network devices. Select the Management Information Base (MIB) that ipMonitor will use to connect to the specified environment sensor.

MIB	DESCRIPTION
SNMP (American Power Conversion)	<p>The PowerNetMIN is specific to American Power Conversion (APC) Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by an APC environment sensor.</p>
SNMP (Dell)	<p>The Dell Environment Monitoring MIB is specific to Dell Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by a Dell environment sensor.</p>
SNMP (IBM)	<p>The IBM MIB is specific to IBM Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by an IBM environment sensor.</p>
SNMP (Hewlett Packard)	<p>The Hewlett Packard MIB is specific to Hewlett Packard Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by a Hewlett Packard environment sensor.</p>
SNMP (Netbotz)	<p>The NetBotz BotzWare MIB is specific to NetBotz Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by a NetBotz environment sensor.</p>
SNMP (Powerware)	<p>The XUPS MIB is specific to PowerWare Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by a PowerWare environment sensor.</p>
SNMP (Sensatronics)	<p>The Sensatronics MIB is specific to Sensatronics LLC.</p>


MIB	DESCRIPTION
	This option is recommended for administrators who want to monitor temperature levels detected by a Sensatronics environment sensor
SNMP (Tripp Lite)	<p>The Trip Lite MIB is specific to Tripp Lite Corporation.</p> <p>This option is recommended for administrators who want to monitor temperature levels detected by a Tripp Lite environment sensor.</p>
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.

Temperature unit

Select whether to view the temperature retrieved by the monitor in either Fahrenheit or Celsius format.


 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 by Fahrenheit. Changing the format from Fahrenheit to Celsius or Celsius to Fahrenheit automatically converts the existing minimum and maximum temperature values to the correct number.

Minimum temperature

Enter the low temperature threshold value that causes 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 causes the Temperature monitor test to fail. By default, the maximum temperature threshold is set to 113 degrees Fahrenheit.

 You 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 descriptive name for the new monitor.

## Windows

The Windows Monitor opens a connection to the specified Microsoft® Windows® station and tests the performance of its subsystems to determine the system's overall health.

The Windows Monitor verifies the following Performance Counter values against a Windows system:

- Disk Read Bytes per Second
- Disk Write Bytes per Second
- Pages per Second
- Page File Percentage Used
- Process Queue Length
- Context Switches
- Number of Processes

You can enable or disable some of the performance counters as required.

If a monitor is not required and you want to prevent Network Scan from creating it, remove it from the SmartMonitor settings when you run the Full network discovery.

## WHOIS

The WHOIS Monitor tests a Remote WHOIS server for availability and responsiveness.

The WHOIS protocol queries WHOIS servers to look up registration information for top-level domains that registered with Domain Name Registrars.


The WHOIS Monitor performs the following steps:

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 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 verify 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.

The Test Parameters dialog box specifies the parameters that the WHOIS Monitor uses to open a connection to the WHOIS server. Specify the location of the WHOIS server you want to monitor and the port number that the WHOIS server responds on. By default, the standard port number used for WHOIS communication is port 43.

 Entering an IP address eliminates any variables introduced by performing a lookup on the DNS server. If your network uses a DHCP server to dynamically assign IP addresses, enter an IP address only if it is reserved. Otherwise enter a Domain Name.

## Test Results

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



The rtt-Round-Trip-Time value indicates the time (in milliseconds) the test packet required to reach the monitored resource and return a response to ipMonitor.

When the Monitor is in a Warn, Down, or Lost state, the Last Result field indicates the encountered problem. Various monitor types generate specific error codes based on the technical capabilities of the monitor.

# Alerts and notifications

An alert is a collection of actions that act on behalf of a set of monitors. Administrators and departments can watch specific monitors and determine when and how they are alerted of monitor failures using alerts.

The alerts and suite of actions provide the required flexibility to accommodate many different types of notification methods and recovery actions.

Using the alert features, you can:

- Configure each alert to be responsible for a single monitor, multiple monitors, or groups of monitors
- Create any number of actions within each alert
- Schedule each action independently
- Specify escalated actions as problems remain uncorrected

If the action occurs during normal business hours, notify the administrator first, and then attempt to resolve the problem using a recovery action (such as rebooting the server or restarting a service).

If the action occurs outside of normal business hours, attempt to fix the problem using a recovery action, and then contact the administrator if the recovery action fails.

## How alerts work when a monitor detects a problem

If a monitor detects that the quality of service has degraded, a predefined threshold is passed, a specific content pattern is detected, or a connection failure occurs, the following events occur in sequence:

1. Each alert is scanned to locate the alert assigned to the failed monitor and to the groups that include the monitor.
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 notifications are not selected, the action does not occur.

## Escalating Alerts

ipMonitor supports escalated alerting. By controlling the number of monitor failures allowed to accumulate before triggering each action, you can share alerts with administrators in different areas of responsibility, between various recovery actions, or both.

## Scheduling Alerts

Each action supports an independent schedule based on a week-long calendar. You can configure the time periods 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

Also known as Ordered Alerting, the ability to escalate alerts makes it easy to share problem resolution with administrators in various levels of your organization.

The Alert Range parameter is located in the Availability section of each configured action. This parameter determines exactly which failure notifications an action will handle.

### How to notify a supervisor after the sixth alert

You can configure an alert to send notifications when very specific failure instances occur.

For example, a supervisor asks to be informed when a resource does not recover after the 6th failure, but may not be interested in prior failures because the supervisor delegates IT staff to handle such problems. When the supervisor is alerted, the problem should be detrimental to business operations or the IT staff did not respond to the alerts in a timely manner.

To address this example:

- Set the Maximum Alerts To Send setting so the monitor triggers six or more alerts when a failure occurs.
- Set the Alert Range setting for the IT staff to 1-5 so they receive the first five alerts. Configure the alerts so they are received by two or three IT staff members.
- Set the Alert Range setting for the supervisor to 6 so this individual receives the sixth alert.

By default, the Alert Range parameter is set to 1-, indicating either of the following:

- Send all alerts
- Send 1 through to n as determined by the monitor's Maximum Alerts to Send parameter

## Timing considerations

When you configure your test duration setting, be sure to consider time delays required for a resource to process.

For example, if you set the Maximum Test Duration setting for a POP3 User Experience monitor to 60 seconds, the setting may generate a premature alert. For example, the mail server could take up to 15 minutes to move an incoming message from the inbound queue to the mailbox during peak times. This example illustrates how important timing considerations can be to alert escalations.

When you create a reboot server alert to follow a restart service alert, consider the time required to restart the service and for ipMonitor to confirm the recovery. If your selected time period is too short, the computer might be rebooted without cause.



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 configuration settings.

## Failure and alerting process

Each alert is processed based on your monitor configuration settings. You can restrict or expand testing during each monitor state by adjusting the parameters in the Timing section. .

The Notification Control settings determine how many test failures must occur before sending an alert, as well as the maximum number of alerts that will be sent.

### Timing Settings : Delays Between Tests While

The following example illustrates how the Timing and Notification Control settings affect the failure and alerting process.

ALERT	SETTING
Warn	30 seconds
Down	60 seconds
Lost	30 seconds

### Notification Control

NOTIFICATION	ACCUMULATED FAILURES PER ALERT
Maximum Alerts to Send	3

The following table 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 are 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

FAILURE COUNT	STATE	ACTION	TIME ELAPSED
8	Fail	None	6:00
9	Fail	Alert	7:00
10	Lost	None	7:30

## Preview the process with the Downtime Simulator

Each monitor includes a Downtime Simulator that simulates the alerting process from a configured start time and duration. Use the Downtime Simulator to process every action that can be triggered by the monitor across all alerts. The simulator can help you test the alert coverage for a monitor at a specific time of day.

## Schedule alerts

Independent scheduling is supported on a per-action basis. The schedules are based on a seven-day calendar. You can configure the time periods in 15-minute blocks and schedule any combination of time interval you require.

This independent scheduling system provides you a high degree of flexibility. During your normal business hours, you can configure actions within the same alert to be sent directly to your email or pager so you can respond resolve the issue. Outside of normal business hours, you can run additional diagnostic scripts, automatically launch a recovery action, and log the event.

### Seven-day availability calendar

The graphical availability screen displays your configured time intervals. The green blocks indicate active time periods. The gray blocks indicate the inactive time periods.

Click a day of the week or a time block to display the week-long calendar. You can toggle individual 15-minute intervals or entire horizontal rows. Click Morning or Afternoon to select the entire day or a portion of the day.

To choose another day of the week, click Select Day to Overwrite list to choose another day of the week. Click Copy to duplicate your settings and fill in the time blocks for the remaining days of the week.

## Customize notifications with tokens

Using tokens (such as %date%), you can customize your alert actions. When ipMonitor executes an action, the tokens are replaced with dynamic content. When you configure your alert, use the Token List and Token Selector to build dynamic alert strings

### 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)	03-02-18
%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)	2018
%yyyear%	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 2018 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

TOKEN NAME	DESCRIPTION	SAMPLE RETURN VALUE
%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 2018 17:29:10 -500
%monitordowndate%	Date / Time Monitor Reported Failure	Sun, 21 Dec 2018 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 Configuration Data from the Branch found in Popup XML	10.25.0.10
%monitor[port]%		53
%monitor[target]%		INTRANETSRV

TOKEN NAME	DESCRIPTION	SAMPLE RETURN VALUE
%monitor[info/logfile]%	These may contain other values in the branch displayed using the Popup XML feature. These fields are specific to the monitor.	Security
%monitortag[...]%	Value of Tag Name Specified.  This will display the value of a custom tag for the specific monitor. The Name of the Tag is entered within the square brackets [ ].	Brian Smith, cell: 555-9876

## Alert and action tokens

Insert the following tokens into your alerts to obtain alert-specific information.

TOKEN NAME	DESCRIPTION	SAMPLE RETURN VALUE
%parentalertname%	Alert name that corresponds with the action.	Night Crew
%actionname%	Action name.	Internal Helpdesk - Simple Email
%action [sendmail/emailto]%	Specified configuration data for the action.	admin@xyzcompany.com
%action[emailfrom]%	This 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 contains a list of values, only the first value is retrieved.  For example: %alert[sendmail/emailto]%	ipm7@xyzcompany.com
%actiontag[...]%	Value of the specified action tag.  This displays the value of a custom tag for the specific action. The tag name is entered within the square brackets [ ].	http://intranet. xyzcompany.com/ recovery.aspx

## 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%
%systememavail%	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 can access %monitor[...]%, %monitortag[...]%, but cannot access %alert[...]% or %alerttag[...]%.

# Action types

Actions can be scheduled based on a week-long calendar. For more information, see [Schedule alerts](#).

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 selected user or group of users. The Recent Activity report includes uptime and downtime information, as well as any failure events for the last 24 hours.

The alert displays the network behavior leading up to the triggered alert and before responding to the problem. You can send the alert to multiple users and to different types of email-enabled devices.

The alert supports ipMonitor alert tokens. You can set up an optimal SMTP relay server withing the server settings to ensure that emails are delivered to the correct users.

Use the Automatic Report alert to:

- Examine a Recent Activity report to analyze a problem immediately after it has occurred.
- Send custom failure and recovery alerts using text and ipMonitor tokens.


ipMonitor does not store the email alert messages. If a mail server cannot receive the email alert, the email is discarded. In Server Settings, you can configure the Optimal SMTP relay server field to ensure that email alerts are delivered and received by the targeted users. Messages are released first through this server.

If the SMTP relay server connection fails for any reason, ipMonitor uses MX records through DNS queries to locate a list of potential mail servers. If a DNS server is specified in the Optional DNS override server (for MX records) section under Server Settings, ipMonitor connects to this DNS server to retrieve MX record information for the recipient domain.

If you do not specify a server in Server Settings, ipMonitor uses the DNS servers configured for the ipMonitor server network connection. When the MX records are retrieved, ipMonitor attempts to connect to each listed server listed in order of MX preference. The relay procedure finishes with a successful transmission to a potential relay server or exhausts the MX records and fails to relay the message.

## Custom Email

The Custom Email alert sends a fully-configured email message to a list of recipients. You can customize the message body, subject line, and email headers in accordance with the RFC 822 specification. You can also create messages with formally-structured components of information or with minimum information.

 RFC 822 defines a standard format for electronic messages consisting of a set of header fields and an optional body.

You can send the Custom Email alert to multiple recipients using the RFC 822 Standard for the format of ARPA text messages. The Custom Email alert supports ipMonitor alert tokens and an optional SMTP relay server in the server settings. This ensures that the email alerts are delivered and received by the user.

Use the Custom Email alert to:

- Integrate email alerts into the internal help or 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 Application Event Log of the ipMonitor host machine. Use the Event Log alert to log fully customized failure notifications, recovery notifications, and information messages using text and ipMonitor alert tokens.

The Event Log alert stores events on the ipMonitor host system for security reasons. The alert does not require additional configuration.

The alert supports designating Error, Success, Warning, and Information Event Types, as well as passing ipMonitor alert tokens to define the Event Description string.

## External Process

The External Process alert runs a third-party executable program or script with any required parameters. If you do not define an alerting credential, the alert uses the current Windows account assigned to the ipMonitor service.



The External Process alert allows you to set the environmental variable names and values that may be read by the executable when started. You can use a credential to transmit account and password information and pass alert tokens on the command line to control the execution of the executable file, batch file, or script. You must have administrator privileges to configure the alert.

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 enables alert messages to pop up on the desktop on a specified network computer. You can send custom failure, recovery, and information messages using text and ipMonitor alert tokens.

Using the Net Send Broadcast alert, you can:

- Pass ipMonitor alert tokens to define the message string
- Use a NetBIOS name or IP address for the Net Send message destination
- Use a credential to transmit account and password information

The Net Send Broadcast alert requires administrator privileges on the target computer.

## Reboot Server

The Reboot Server alert recovery action reboots a Microsoft Windows workstation or server computer when a monitor encounters a problem.

The alert uses the recovery parameters you defined during the monitor configuration. Using a credential that you define when you configure the monitor, the alert can service several monitors because the 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 running a recovery application to restore service or after executing the Restart Service action.


The target machine to reboot is defined in the Recovery Parameters section under the monitor configuration settings. If a specific user account and password is required to perform the Reboot Server action, ipMonitor uses the recovery credential you selected when you configured the monitor.

## Restart Service

The Restart Service alert recovery action attempts to restart a service or list of services on the targeted Microsoft Windows workstation or server computer when a monitor encounters a problem. Use the Restart Service alert to remotely restart a Windows service or list of services with or without dependencies.

The action restarts the services you defined in the Recovery Parameters section when you configured the monitor. Using a credential you defined when you configured the monitor, the action can service several monitors because the recovery parameters are passed to the Recovery alert by the failing monitor.

You can define the workstation or server host name and the Windows services to restart in the monitor configuration settings under Recovery Parameters. If a specific user account and password is required to perform this action, ipMonitor uses the recovery credential you entered when you configured the monitor.

 If a service includes assigned dependencies, they must be included in the list of services. Otherwise, the Recovery action will not complete successfully.

## Simple Beeper

The Simple Beeper alert sends a numeric message to a simple numeric pager by simulating the touch-tone key presses. Use the Simple Beeper alert to send failure and recovery notifications to a simple beeper using numerical values, spaces, and ipMonitor alert tokens that contain only numeric data.

The alert uses TAPI or Direct Port Access to communicate with a modem. You can set a delay period after the modem connects with the provider before it keys in the message. The alert supports selectable COM ports and ipMonitor alert tokens.

### Beeper hardware requirements

The Simple Beeper alert requires the following hardware on the ipMonitor host computer:

- COM port for your modem
- Hayes-compatible modem 2400 baud or faster
- Dedicated telephone line that allows ipMonitor to page administrators

The dedicated telephone line cannot be shared with a Remote Access Server (RAS). Even at idle, the RAS owns the communication port to watch for and connect to incoming callers.


## Simple Email

The Simple Email alert sends a dynamically formatted email to one or more users 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.

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 or monitors
- Send custom failure notifications, recovery notifications, and information messages using text and ipMonitor tokens

The Simple Email alert supports ipMonitor alert tokens, message formatting from a list of options (such as To, From, and Message Body), and individual body content configuration for failed, recovery, and information messages. Additionally, the alert supports ipMonitor alert tokens and an optional SMTP relay server to ensure that email alerts are delivered to the correct users.

 ipMonitor does not store the email alert messages. If a mail server is not available to receive the email alert, it will be discarded. You can use the Optional SMTP relay server field located in Server Settings to ensure that email alerts are successfully delivered to the intended users. You can access Server Settings in the Configuration tab.

## SMS Numeric Pager

The SMS Numeric Pager alert sends a numeric message through a mobile service provider to a pager device that can receive SMS messages. The messages can include numbers, spaces, and a limited number of punctuation characters (based on your pager model and wireless provider).

 Most pagers can only accept simple punctuation (such as dashes, commas, and periods). Accented characters and other special symbols will not display properly.

The alert uses TAPI or Direct Port Access to communicate with a modem. You can enter a password (if required) and pause the dial sequence while your phone service selects an outgoing phone line. The alert supports ipMonitor alert tokens and full control over modem settings, including COM port, baud rate, data bits, parity, init string and dial string, and forcing the modem to behave as a low-speed modem.

## Supported paging protocols

The SMS Numeric Pager alert supports Telocator Alphanumeric Input Protocol (TAP) and Universal Computer Protocol (UCP).

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 or SMS numerical paging.

UCP is the primary paging protocol used by European network providers. This protocol is implemented to run over TCP/IP and X.25 networks.

## Hardware requirements

The SMS Numeric Pager alert requires the following hardware installed on the ipMonitor host computer:

- COM port for your modem
- Hayes-compatible modem that is 2400 baud or faster
- Telephone line that will not be used by any other device when ipMonitor needs to page administrators

If the telephone line is in use when ipMonitor sends an alert, ipMonitor will retry the connection based on the value you specify 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 to watch for and connect to incoming callers.

Before you configure the SMS Numeric Pager alert, contact your paging service provider to obtain the required configuration details. Paging services most often accept pages using operator dispatch. The operator enters a message, transmits it to their server, and then to your pager. Most paging services can receive messages by modem, which are broadcast by their wireless telecommunications equipment. Ensure that pages generated by ipMonitor are sent to a modem and not a human operator.

## About SMS

SMS is a text message service that enables short messages of 160 characters or less to be sent and transmitted to and from a pager, cell phone or IP address. Unlike paging but similar to email, short messages are stored and forwarded at SMS centers. You can retrieve these messages 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 alert to send custom failure notifications, recovery notifications and information messages to an alphanumeric pager or cell phone using text and ipMonitor alert tokens.

SMS Text Pager supports the following SMS text pager protocols are supported:

- SMS Text Pager (GSM)
- SMS Text Pager (TAP and UCP)

## SMS Text Pager - GSM

Global System for Mobile communications (GSM) was originally developed as the European communication standard for digital mobile and cellular service. Currently, GSM is used 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), allowing you to make 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. It is widely used to take advantage of GSM and SMS mobile communications.

GSM can send a maximum of 5,049 characters per message. It uses direct port access to communicate with a model, and allows you to pause the dialing sequence to select an outside phone line, and supports ipMonitor alert tokens. Additionally, GSM supports full control over your modem settings, including COM port, baud rate, data bits, parity, init string, and dial string, as well as forcing the modem to behave as a low-speed modem.

## Hardware requirements

The SMS Text Pager: GSM alert requires the following installed on the ipMonitor host computer:

- GSM mobile network subscription
- COM port for your modem
- Hayes-compatible GSM or GPRS modem capable of supporting AT commands

## 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.

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 email, short messages are stored and forwarded at SMS centers, and you can be retrieved 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 uses TAPI or Direct Port Access to communicate with a modem. You can enter a password (if required) and pause the dial sequence while your phone service selects an outgoing phone line. The alert supports ipMonitor alert tokens and full control over modem settings, including COM port, baud rate, data bits, parity, init string and dial string, and forcing the modem to behave as a low-speed modem.

## Hardware requirements

The SMS Text Pager alert requires the following hardware on the ipMonitor host computer:

- COM port for your modem
- Hayes-compatible modem that is 2400 baud or faster
- Telephone line that will not be used by any other device when ipMonitor needs to page administrators

## SNMP Trap

The SNMP Trap alert sends an SNMP trap to the specified SNMP manager. 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 any SNMP management application. The alert supports ipMonitor alert tokens, as well as enterprise-specific and generic trap types such as Cold Start, Warm Start, Link Down, and so on.

Use the SNMP Trap alert to:

- Integrate ipMonitor into any existing network management software in your organization
- Send custom failure notifications, recovery notification, and information messages using text and ipMonitor alert tokens


## Set up the alert

Enable the SNMP Trap alert 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

## HP OpenView

 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 allows you to use local or UNC paths to the directory where the log file is created or located. You can also pass ip Monitor alert tokens to define the event string.

Use the Text Log alert to:

- Create a log file that records activity for a single monitor or 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.

# 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 can 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.

You can configure information alerts by adding one or more search scenarios in the monitor configuration interface.

A search scenario is a search pattern articulated through a regular expression, and is used when parsing the data source to locate patterns of information. Create the regular expressions using the IpMonitor Regex Wizard.

After your search scenario captures information from the data source, it is passed to the [Content Generator](#). The content generator sends formatted data to information alerts. It is assigned in the monitor settings and formats captured data for readability or layout.

## Content Generator

The Content Generator format data into messages for Information actions.

The [Event Log](#), [SNMP Trap](#) and [File Watching](#) monitors support 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 passed to a Content Generator and parsed into a message. Additional information relating to the monitor (such as the event time stamp or the source IP address of a received SNMP trap) can be included in the message.

After the message is structured, it can 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, Value, and Coalesce Separator.



The Name identifies the Content Generator. The Value defines the layout of the captured data. This will be the format of the alert message. The Coalesce Separator specifies the string used to terminate each capture 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.

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, email actions, text logs or SNMP traps.

## Information action messages

Within the configuration interface for actions, the Notification Content - Information Messages section controls the 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
- 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 was entered:

```
ERROR\: (.*) REASON\: (.*)
```

In this example, the %capture[1]% Token resolves to: "The application failed to start." and the %capture[2]% Token resolves to: "Required resource myapp.dll could not be located."

Assuming an information action was configured correctly, this information would be included in the body of the message.

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

 %capture[1.3.6.1.2.1.1.0]% displays the value of the specified OID entered within the square brackets []. A wildcard character (\*) cannot be used to specify an OID prefix.

# Log files

ipMonitor records several separate log files to provide administrators with the necessary information 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 occurred internally within ipMonitor. You can record the following optional events 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

For diagnostic purposes, you could run IpMonitor 7.x and earlier at the command line in Desktop Mode. When you run ipMonitor in this mode, some diagnostic information is written to the console. Recent versions of ipMonitor include the `runtime.log` file that provides the same diagnostic information.

## runtime\_bkg\_reports.log

The `runtime_bkg_reports.log` file is created by the background report generator to track all generated reports. The log file is overwritten each night with updated information.

## snmptrap.log

The `snmptrap.log` file records information relating to SNMP traps that were received by ipMonitor 8. It will only be displayed if there are entries in the log file.

You can record the following optional events 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`

# Maintenance schedules

Maintenance schedules allow administrators to temporarily disable monitoring of certain resources—for example, performing data backups or service restart actions.

Using maintenance schedules, you can identify all groups and monitors impacted by the scheduled downtime. Prior to maintenance, ipMonitor suspends the affected monitors, ensuring that planned maintenance does not trigger alerts or display negatively in historical reports. When the scheduled maintenance is completed, ipMonitor reactivates the affected monitors.

You can schedule maintenance based on rules (such as Microsoft Outlook rules) or while ipMonitor performs routine actions. This allows you to define a list of actions using the reboot server, restart service, or pause commands. You can configure credentials as required on a per-action basis, as well as schedule maintenance to disable monitors while actions outside of ipMonitor occur.

## Suspend monitors while ipMonitor reboots services and computers

1. Open ipMonitor.
2. Click the Automation menu option.
3. Choose Maintenance Schedules > Add a Maintenance Schedule.
4. Enter a unique name for the maintenance schedule.
5. Choose Disable Monitors while ipMonitor performs routine actions.  
This maintenance mode allows you to configure any combination of reboot server, restart service or pause actions.
6. Click Reboot Server to select the Reboot Server configuration options.  
This action reboots the targeted Windows host computer.
7. Click Restart Service and select the Restart Service configuration options.  
This action restarts the supplied list of services on the specified Microsoft® Windows® host computer.
8. Click Pause and select the Pause configuration options.  
This action disables testing during the specified time period for any monitors or groups of monitors assigned to the maintenance schedule.
9. Click Browse and select the server machine name to populate this field.  
If elevated credentials are required to reboot a machine, enable the Usage Restrictions option.
10. Click Select.
11. In the Credentials for Network Control dialog box, select an existing credential from the Windows Category
12. Click New Credential to create a new credential.
13. In the Services List, click Select.

14. Select a service to populate this field.
15. Under Pause Duration, enter the length of time that testing will be disabled.
16. Complete the wizard.

## Suspend monitors during network maintenance

1. Open ipMonitor.
2. Click Automation > Maintenance Schedules and select Add a Maintenance Schedule.
3. Enter a unique name for the Maintenance Schedule.
4. Choose Disable Monitors while actions outside of ipMonitor occur.  
This maintenance mode allows you to disable monitor testing while routine external maintenance is completed on resources being monitored.
5. In Disable Duration Action, specify the length of time necessary for maintenance to occur.
6. Complete the wizard.

## Internal Maintenance

Internal Maintenance allows you to perform recurring maintenance actions, such as rolling log files and backing up the configuration settings.

You can schedule Internal Maintenance tasks to occur on specific days of the week. If you need to encrypt the Credentials database for backup purposes, you can create a credential for this purpose.

Internal Maintenance allows you to use ipMonitor tokens to designate file names. All log files are compressed in ZIP format and can be automatically rolled on a daily basis.

## Standalone backup

To archive your ipMonitor configuration settings without scheduling recurring internal maintenance, click Backup Now button located on the Internal Maintenance submenu bar.



# Security model

The ipMonitor Security Model encompasses authentication, authorization, encryption and protection against intrusion. This security model is designed to:

- Provide security to the ipMonitor application and the stored data
- Provide a safe network monitoring environment through secure network monitoring techniques and standard practices


ipMonitor tests key resources such as operating systems, SQL databases, file servers, mail systems, commerce solutions and infrastructure equipment around-the-clock. The tests can include logging in to resources and generating synthetic transactions to measure quality of service.

## Authentication methods

Authentication is the process of validating the identity of a user or client. Typically, clients 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. You can apply each credential to any monitor, alert, or feature that requires special permission to access restricted network resources.

The following section lists the options you can choose in Credential Manager.


METHOD	DESCRIPTION
Secure Sockets Layer (SSL)	ipMonitor performs authentication if SSL encryption method is used.
Digest authentication schemes	<p>Digest authentication is a challenge/response mechanism 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 key and password, the server authenticates the client.</p> <div><p> 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.</p></div>
Windows Impersonation for use with Remote	RPC is a programming interface that allows one program to

METHOD	DESCRIPTION
Procedure Call (RPC)	use the services of another program on a remote machine. The Usage Restriction option allows the ipMonitor Service to impersonate the security context of a separate Account before carrying out the RPC call.
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.
ActiveX Data Objects (ADO)	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.
Encrypt Data	This Usage Restriction option allows ipMonitor to encrypt and export the credentials database when used to archive configuration data within the <a href="#">internal maintenance</a> feature.
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, you can restrict access to the ipMonitor web interface to specific IP addresses or ranges of IP addresses.

Using IP address ranges allows you to 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.

 IP Access restrictions cannot be configured for individual portions of the ipMonitor application.

See [Communications: Lockout](#) for details about how to grant or deny access to IP addresses.

## User accounts

All users must enter a username and a [strong password](#) to access the ipMonitor web interface. These credentials are part of an internal proprietary ipMonitor account and do not belong to a Microsoft Windows account. RSA 512/1024 bit encryption is used internally to store all account information.

You can create three types of user accounts in ipMonitor:

- Administrator
- User
- Guest

## Administrator accounts

Administrator accounts have full access to all ipMonitor features. They can create, edit, and delete user accounts and can access and administrate user credentials. Administrator accounts cannot be deleted unless they are demoted to a user account.

## User accounts

User accounts can access all non-administrative features in ipMonitor, but cannot create, edit, or delete user accounts. You can promote a Guest account to User status by clicking the Promote to Normal User option in the Edit Account page.

## Guest accounts

Guest accounts can only read or view data. Guests cannot access the Administration Interface, nor do they have the ability to change or save their own settings beyond the current session.

Guest accounts provide a common user name and password to access the reporting Interface. This allows an administrator to post the account credentials on an intranet site or distribute the user name and password to those who require access.

To create a Guest account, create a User account and select the Guest option.

## Account Permissions


Each user account has its own List, Read, Write, Create, Delete, and Attributes settings. These settings include:

- Real-time statistics
- Recent activity
- Historic reports
- Monitors
- Monitor filters
- Groups
- Notifications
- Logs
- Tools
- Maintenance
- Report generators
- Server settings

## Strong passwords

You can enable strong passwords system-wide to enforce system security. When you enforce strong passwords, the password must contain the following:

- One or more lowercase characters
- One or more uppercase characters
- One or more numeric characters
- One or more non-alphanumeric characters
- Six or more total characters

 ipMonitor maintains an internal data hive 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, install a Secure Socket Layer (SSL) certificate.

SSL allows 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 the ipMonitor host computer. SolarWinds recommends using the ipMonitor's Self-Signed Certificate option as a minimum requirement.

## Certificate requirements

Certificate types must be server certificates install to the Local Machine Store.

### Obtain an SSL certificate

Install SSL certificates on the ipMonitor host computer in the Local Machine Store. After the certificate is installed, 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. In the main menu, select the Communications: Web Server Ports option.
3. Click Add to enter a new IP address and port combination.
4. Enter an IP address or enter 0.0.0.0 to have ipMonitor listen on all available IP addresses.
5. Enter a Port number and select the SSL check box.  
Port 443 is the default port number for HTTPS communications.
6. Click OK.  
ipMonitor begins listening on the new SSL IP address and port.

ipMonitor supports three types of SSL certificates:

- Self-signed certificates
- Trusted Certificate Authority
- Microsoft Certificate Authority

## Self-signed certificates

When you install ipMonitor for the first time, the application prompts you to automatically generate a self-signed certificate. You can change this selection at any time by using the ipMonitor Configuration program.

Self-signed certificates are economical because they are free. However, self-signed certificates installed by ipMonitor do not include a Trusted Authority that issues and verifies the certificate. As a result, you must instruct your web browser to trust the self-signed certificate installed by ipMonitor.

## Trusted Certificate Authority

ipMonitor provides the tools to generate a Certificate Signing Request (CSR) and install a certificate after it is acquired from a Trusted Certificate Authority. Certificates issued by VeriSign, FreeSSL™, and InstantSSL™ are tested and work well with ipMonitor. Prices vary from under a hundred dollars to a few hundred dollars based on the organization. Contact the Trusted Certificate Authority for details and pricing.

## Microsoft Certificate Authority

You can request a certificate from a Stand-Alone Certificate Authority using the Microsoft Windows Certificate Services web interface.

Networks that use a Stand-Alone Certificate Authority server require you to submit certificate requests using the web interface provided by the Certificate Authority server. Certificate requests may have to be approved prior to installation. You can obtain policy information from your Network Administrator.

You can request a certificate from an enterprise certification authority using the Microsoft Management Console (MMC) Certificates snap-in. This depends on whether a Certificate Authority server exists in Active Directory. If a Certificate Authority server exists in Active Directory, generate certificate requests from the ipMonitor host computer using the MMC.

# Credentials

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. Network monitoring solutions support one account, which must be a network Administrator-level account to access resources throughout the network. This model is contrary to good security practices, as it potentially exposes all the resources accessed by the Administrator account.


ipMonitor resolves this problem using [Credentials Manager](#). Credentials Manager allows the ipMonitor Service to run under the context of an account with the least privileges, and then impersonate accounts with elevated permissions when required by monitors, alerts and features accessing Windows file system objects or services through the network.

Using Credentials Manager, you can tailor the credentials to the exact authentication credentials required by the targeted resource. You can reuse the credential to access several target resources. The ipMonitor [Credentials Wizard](#) automatically categorizes the credentials for reuse. You can limit the credential to the administrator who created the credential, or other administrators can be permitted to use it.

You can apply user restrictions 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 to start an external process
- Used with ActiveX Data Objects (ADO)
- Used to encrypt data
- Transmitted in clear text


If you decide not to use SSL to log in to ipMonitor, the Credentials Manager will allow only limited viewing of credentials. It will not allow configuration or management, and will not allow account-based information to be visible or accessible.

 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, you cannot modify the Account, Password and Secret (for Radius) fields.

# Credentials wizard

The Credentials Wizard helps you create credentials you can use with monitors, alerts, and maintenance actions. You can apply restrictions on how the credentials can be used during this configuration process.

1. Configure a monitor, alert, or other feature that requires access to Windows file system objects or services through the network.
2. During the configuration process, click Select when prompted to choose a credential.
3. If the credential you want to use does not exist, click New Credential located in the pop-up window.

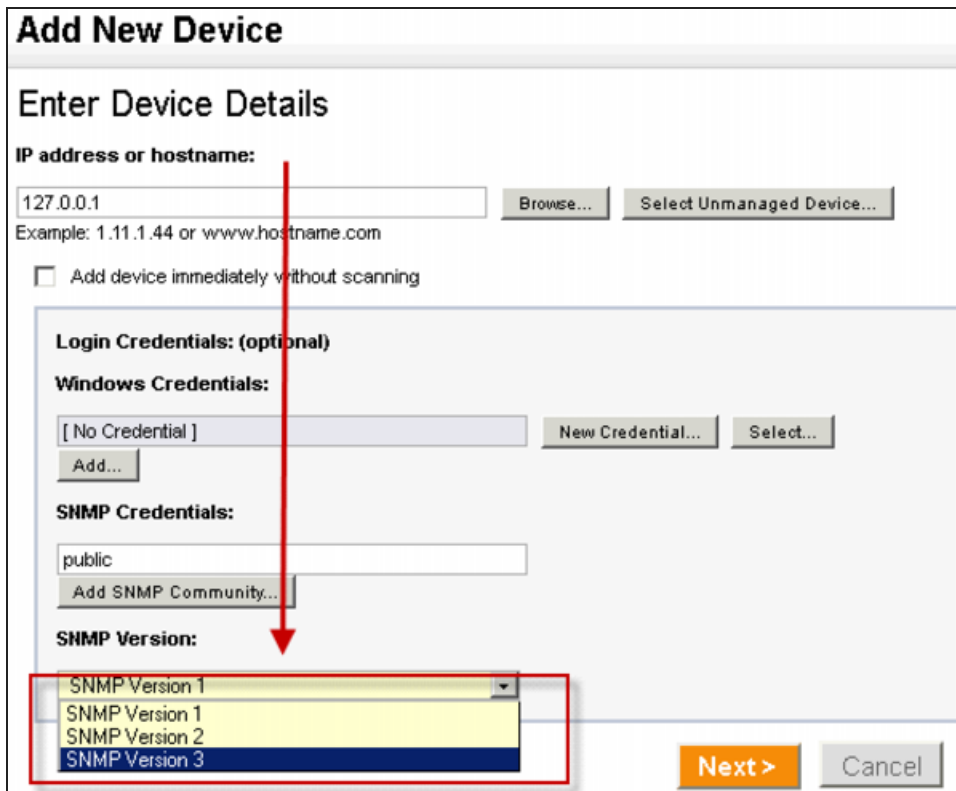
 Your credential is saved in Credentials Manager. To edit or delete credentials, go to the Configuration tab and click Credentials Manager.

## Required permissions

When you supply your credentials, ensure they include the required permissions to access the monitored resources. For example, if you intend to monitor an administrative share (such as C\$), ensure that your credential is a member of the Windows Administrators group.

## SNMPv3 authentication

SNMPv3 is a supported protocol. All monitors that support SNMPv3 will have the option available in the Add New Device screen, including the Credential and SNMP Wizards and Add Device Wizard.



**Add New Device**

**Enter Device Details**

**IP address or hostname:**

127.0.0.1 Browse... Select Unmanaged Device...

Example: 1.11.1.44 or www.hostname.com

☐ Add device immediately without scanning

**Login Credentials: (optional)**

**Windows Credentials:**

[ No Credential ] New Credential... Select...

Add...

**SNMP Credentials:**

public Add SNMP Community...

**SNMP Version:**

SNMP Version 1  
SNMP Version 1  
SNMP Version 2  
SNMP Version 3

Next > Cancel

**Add Monitor : SNMP Monitor:**

Cancel / Back   Downtime Simulator   <>   Popup XML

**Identification**

Monitor Name

☒ Enabled

☐ Store Monitor Statistics for Recent Activity and Historical Reports

**Test Parameters**

IP Address / Domain Name

UDP Port

OID  (sysUptime.0)

Community

SNMP Version

SNMPv3 Credentials

Below is an example from the Credentials wizard.

The Credentials Wizard has selected the following Display Categories for this Credential:

☐ HTTP (HTTP and HTTPS)

☐ FTP

☐ Mail (SMTP, POP3, and IMAP4)

☐ ADO (Standard (SQL) Authentication)

☐ Windows (Impersonation, Network Control, and ADO using SSPI / Trusted Connections)

☐ RunAs (External Process Monitor and Actions)

☐ Encryption

☐ Radius

☒ **SNMPv3 Authentication**

## Local security policies and credentials

If the `ipmonitorsrv` service is running under a specific user account instead of the Local System account, ensure that the following Local Security Policies are enabled for this specific user account.

THIS CREDENTIAL TYPE...	...REQUIRES THESE LOCAL POLICIES
ADO	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> </ul>
Directory	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> </ul>
Drive Space	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> </ul>



THIS CREDENTIAL TYPE...	...REQUIRES THESE LOCAL POLICIES
Event Log	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> <li>• Act as part of the operating system</li> </ul>
Exchange Server	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> <li>• Replace a process level token</li> </ul>
External Process	<ul style="list-style-type: none"> <li>• Bypass traverse checking</li> <li>• Bypass traverse checking</li> <li>• Bypass traverse checking</li> </ul>
File Property	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> </ul>
File Watching	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> </ul>
FTP User Experience	<ul style="list-style-type: none"> <li>• None</li> </ul>
HTTP-based	<ul style="list-style-type: none"> <li>• None</li> </ul>
IMAP4 User Experience	<ul style="list-style-type: none"> <li>• None</li> </ul>
MAPI User Experience	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> <li>• Replace a process level token</li> </ul>
Net Send	<ul style="list-style-type: none"> <li>• Act as part of the operating system</li> <li>• Bypass traverse checking</li> <li>• Log on as a Service</li> </ul>
POP3 User Experience	<ul style="list-style-type: none"> <li>• None</li> </ul>

THIS CREDENTIAL TYPE...	...REQUIRES THESE LOCAL POLICIES
RADIUS	<ul style="list-style-type: none"><li>• None</li></ul>
Reboot Server	<ul style="list-style-type: none"><li>• Act as part of the operating system</li><li>• Bypass traverse checking</li><li>• Log on as a Service</li></ul>
Restart Service	<ul style="list-style-type: none"><li>• Act as part of the operating system</li><li>• Bypass traverse checking</li></ul>
Log on as a Service	<ul style="list-style-type: none"><li>• Act as part of the operating system</li><li>• Bypass traverse checking</li><li>• Log on as a Service</li></ul>
Service	
Text Log	<ul style="list-style-type: none"><li>• Act as part of the operating system</li><li>• Bypass traverse checking</li><li>• Log on as a Service</li></ul>

After you modify any of these settings, you refresh the applied Local Security Policy settings.

To refresh the applied Local Security Policy settings in Windows Server 2003:

1. Open a command prompt.
2. Run the following command:  
`gpupdate /target:computer /force`
3. Open the Application Event log.
4. Verify that the new settings were correctly applied.  
If an error was encountered, it will be recorded here.
5. Restart the `ipmonitorsrv` service.

## Credentials Manager

Use the Credentials Manager to create and manage ipMonitor Credentials.

When you create your credentials using the [Credentials Wizard](#), the credentials are stored in [Credential Manager](#). ipMonitor uses RSA 512/1024 bit encryption used internally to store all sensitive parameters and data.

The Credentials interface is restricted to Administrators only. The access control options allow administrators to specify users who can use the credentials and determine their use.


To use Credentials Manager, 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 only permit you to view the credentials and not allow you to make configuration changes.

## Adding a credential

You can add credentials using the Credentials Manager or the Credentials Wizard. The Credentials Wizard allows you to create a new credential while you configure a Monitor, Alert, or Recovery Action, and apply it immediately. You cannot use the Credentials Wizard to edit or manage credentials.

## Orphaned credentials

When a credential is not associated with an administrator account, it is considered to be orphaned. This is a security precaution. It occurs when the administrator account that created the credential was deleted, or when the password for the administrator account was force-changed through the account configuration page.

 Administrators can change the password in another account in the Accounts List page located in the Configuration view. Force-changing your password or another user password in this configuration area 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. If you use the My Settings configuration panel to change your password, this issue will not occur.

A warning message displays at the top of the Edit Credential page for any Orphaned Credential.

### Reinitialize an orphaned credential

1. Click Enable to reenter the Account Name and Password information.
2. Click OK to save your changes and associate this credential with the current ipMonitor administrator account.

## Change monitoring credentials in bulk

Perform the following steps to assign a credential to multiple Monitors in bulk.

1. Click the Configuration tab.
2. Click Credential List.
3. Click the Credential you wish to use.
4. Under the Monitors using this Credential for monitoring section, click Add Monitors.
5. Add the Monitors you want to assign to the Credential.
6. Click OK.