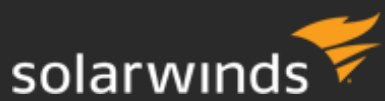




GETTING STARTED GUIDE

ipMonitor

Version 10.8.2



Last Updated: Friday, August 10, 2018

Retrieve the latest version from: https://support.solarwinds.com/Success_Center/ipMonitor/ipMonitor_Documentation

Table of Contents

Get Started with ipMonitor	3
Run the ipMonitor configuration program	4
Run ipMonitor in First Run mode	4
Run the ipMonitor configuration program	4
Scan your network and select the monitors	5
Add the ipMonitor accounts	7
Add ipMonitor administrator accounts	7
Add ipMonitor user accounts	7
Delete an administrator account	8
Enable guest login	8
Connect ipMonitor to your network	10
Configure the TCP settings on the HTTP server	10
Configure the SNMP Trap Listener	11
Monitor a specific port	11
Resolve SNMP Trap Listener conflicts	11
Connect ipMonitor to your network components	11
Install an SSL certificate	12
Generate a self-signed certificate	12
Assign a Windows account to host the ipmonitorsrv service	13
About the LocalSystem account	14
Disable the LocalSystem account	14
Beyond Getting Started	15

Get Started with ipMonitor

This guide picks up right after the ipMonitor installation process and walks you through the first steps you need to take to monitor your IT infrastructure.

i If you have not installed ipMonitor yet, start with the [ipMonitor Installation Guide](#).

Who this guide is for

NEW IPMONITOR USERS	EXISTING IPMONITOR USERS
This guide is meant for you and is the best place to start with ipMonitor.	You will find more advanced information in the ipMonitor Administrator Guide .

Get started

To get started with ipMonitor, complete the following tasks:

<input type="checkbox"/>	<p>Configure ipMonitor.</p> <p>Log in to ipMonitor in First Run mode and run the ipMonitor configuration program.</p>
<input type="checkbox"/>	<p>Scan your network and select the monitors.</p> <p>Run Discovery Express Scan to scan your network, locate and select the hardware and software components you want to monitor, and apply the appropriate monitors to the application.</p>
<input type="checkbox"/>	<p>Set up the user accounts.</p> <p>Add the administrator and user accounts. When you are finished, enable guest login.</p>
<input type="checkbox"/>	<p>Assign IP address and port combinations to communicate with ipMonitor.</p> <ol style="list-style-type: none"> Assign one or more IP address and port combinations to ipMonitor to enable ipMonitor communications using the HTTP and HTTPS protocols. Configure the SNMP Trap Listener to listen for incoming SNMP traps. Connect ipMonitor to the network components that will communicate with the application.
<input type="checkbox"/>	<p>Install an SSL certificate.</p> <p>Install an SSL certificate or generate a self-signed certificate.</p>
<input type="checkbox"/>	<p>Assign a Windows account to run the ipmonitorsrv service.</p> <p>When you assign a Windows account to host the ipmonitorsrv service, decide whether to host the service by creating a new Windows account or using the LocalSystem account.</p>

Run the ipMonitor configuration program

The ipMonitor configuration program helps you configure several key parameters for the ipmonitorsrv service.

The configuration program prompts you to:

- Enter an IP address and port number for the web interface
- Select an SSL certificate for secure communication
- Change the Windows Service account context

Run ipMonitor in First Run mode

After you first install ipMonitor, the configuration program automatically runs in First Run mode. This mode runs only once, automatically providing default parameters and requiring you to configure an ipMonitor administrator account.


During the initial configuration process, you can set up the following default monitors to begin testing your system resources:

- CPU usage monitor
- Memory usage monitor
- Drive space monitor

The First Run mode creates a default group, alert, and email action, and associates them with the new monitors.

Run the ipMonitor configuration program

1. Click Start > All Programs > SolarWinds ipMonitor > Configure ipMonitor.
If the ipMonitor service is not running, you are prompted to launch the ipMonitor service.
2. Click Yes to start the service.

 The configuration program is not used to add or configure monitors, alerts, or actions. You can add or modify these elements in the ipMonitor web interface.


Scan your network and select the monitors

Discovery Express scans your network using a wizard and selects the correct monitors for your selected hardware and software components. By default, ipMonitor uses the following common monitors:

- CPU Usage
- Memory
- Usage
- Drive Space
- Bandwidth Usage
- Ping
- HTTP
- HTTPS
- Windows
- Exchange Server 2000/2003
- Exchange Server 2007/2010
- SQL Server
- Active Directory

For new installations, Express Discovery begins after you log in to the ipMonitor Web Interface for the first time.

1. Log in to the ipMonitor Web Interface as an administrator.
2. Click Devices and select Discovery Express Scan.
3. Select the applications and resources you want to monitor, and then click Next.
4. Enter an IP address range to scan for devices, and click Next.


 The scan may take several minutes to complete. SolarWinds recommends that you select only a small IP address range of 100 addresses or fewer for your initial scan.

5. If you have Windows network credentials that you want to use for discovering Windows network resources, complete the following procedure. Otherwise, go to step 6.
 - a. Click Next to open the Credentials window.
 - b. Click New Credential to launch the Credentials wizard.
 - c. Enter a name for the credential, and then click Next.
 - d. Enter the details of your Windows network credential, and then click Next.
 - e. Click Credential may only be used by my Account, and then click Next.
 - f. Click Finish > Apply.

6. If you have SNMP community strings that you want to use for discovering SNMP devices and resources, complete the following procedure. Otherwise, go to step 7.
 - a. In the SNMP Credential text box, enter the SNMP community string.
 - b. If you want to specify additional SNMP community strings, click Add SNMP Community.

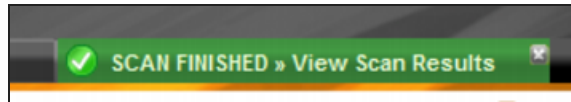
7. Click Next.

The device scan begins.

 Wait for the device scan to complete. The scan is completed when the device state changes from Scanning Device to Scanning Complete.


8. When the scan is completed, click Add All Scanned Devices.

A tab displays on the dashboard that displays the scan results summary.



9. Select Show Alert List to review the added alerts.
10. Click Go to Dashboard.

The Dashboard page opens, summarizing the current network state.

 You must manually add experience monitors because critical information in each monitor is specific to each network environment.

Add the ipMonitor accounts

You can manage ipMonitor accounts using the Administrator Account window and the Configuration tab. To add the accounts:

1. [Add ipMonitor administrator accounts](#)
2. [Add ipMonitor user accounts](#)
3. [Enable guest login](#)


Add ipMonitor administrator accounts

Any accounts you add using the Administrator Account window are internal to the ipMonitor software. These accounts are not associated with the Windows local machine or domain accounts.

Use the ipMonitor configuration program to create the first administrator account. The following rules apply to administrator accounts:

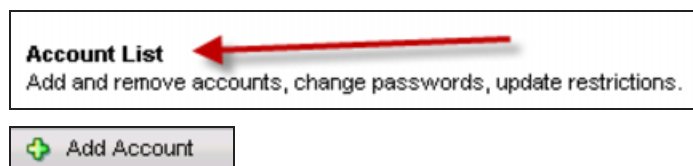
- Administrator accounts cannot be deleted until they are demoted within the ipMonitor Administration web Interface to a general user.
- At least one administrator account must be present at all times.
- Administrator accounts cannot delete nor demote themselves.

To create a new administrator account, click Add Account and [add the account](#) to ipMonitor.

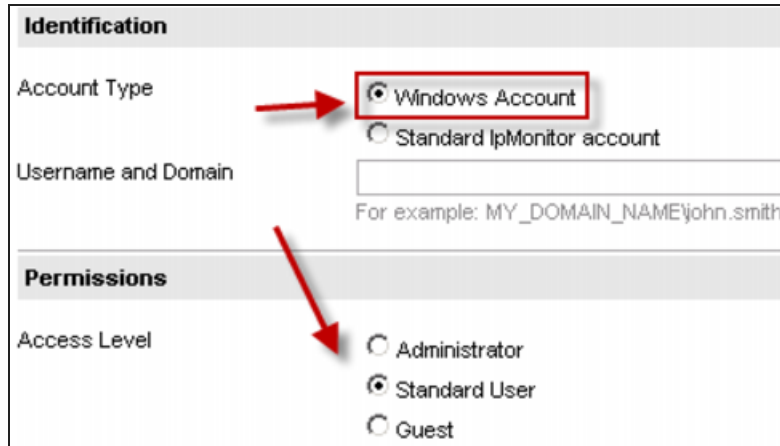
 All account information is stored internally using RSA 512/1024 bit encryption.

Add ipMonitor user accounts

1. Go to the Configuration tab and click Account List > Add Account.




2. Select the account type and define the access level.



The screenshot shows a configuration window with two main sections: **Identification** and **Permissions**. In the **Identification** section, the **Account Type** is set to **Windows Account** (indicated by a red box and an arrow). Below it is a text field for **Username and Domain** with the example `MY_DOMAIN_NAME\john.smith`. In the **Permissions** section, the **Access Level** is set to **Standard User** (indicated by a red arrow).

3. Click OK.
4. In the Advanced section, customize the Guest and Standard accounts, selecting the rights for each user.

 To manage existing user accounts, go to the Configuration tab and click Account List.

Advanced	List	Read	Write	Create	Delete	Attributes
Dashboard	<input checked="" type="checkbox"/>		<input type="checkbox"/>			
Groups, Devices & Monitors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuration						
Scheduled Maintenance Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scheduled Reporting Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Alerts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Tools	<input checked="" type="checkbox"/>					
Notes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

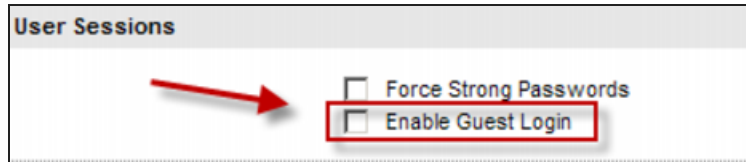
Delete an administrator account

1. Access the targeted account through the Account list.
2. Demote the account to a Standard or Guest account.
3. Delete the account.

Enable guest login

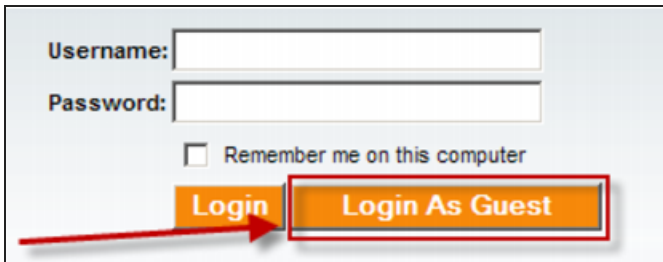
The guest login account is ideal for network operation center (NOC) views because the user can log in with one click and view the dashboards. You can create a guest account that does not require login credentials.

1. Follow the steps in [Add ipMonitor user accounts](#) to create a Guest account.
2. Click Configuration > System Settings.
3. Under the User Sessions section, select Enable Guest Login.



4. Click Save.

When you log out of all sessions, a Login as Guest button displays in the user interface.



Connect ipMonitor to your network

Use the Communications: Web Server Ports window to connect ipMonitor to the network devices and applications you want to monitor in your organization.

1. [Configure the TCP settings on the HTTP server](#) by assigning one or more IP address and port combinations to ipMonitor.
2. [Configure the SNMP Trap Listener](#) to enable ipMonitor to listen for SNMP traps sent to it by any SNMP agent on the network.
3. [Add the IP addresses](#) of network devices, servers, and applications that you want to monitor in your organization.

Configure the TCP settings on the HTTP server

ipMonitor is a stand-alone HTTP server. The application does not integrate into or require other web server services (such as Microsoft Internet Information Services [IIS]).


To enable communications using the HTTP and HTTPS protocols, assign one or more IP address and port combinations to ipMonitor. You will use one or both protocols to log in and manage ipMonitor.

Use the Communications: Web Server Ports window to enter any port combination for ipMonitor to listen on.

For each HTTP entry, enter a unique IP address and port combination that is not used by any other server application. For each HTTPS entry, enter an IP address and port combination that is not used by any other server application, and then select Enable SSL.

 See [Port requirements for all SolarWinds Products](#) for ipMonitor port requirements.

To enable ipMonitor to listen on all IP addresses bound to the host machine on a specific port, enter an IP address of 0.0.0.0. For example, `https://0.0.0.0:8080` enables ipMonitor to listen on every IP address assigned to the machine on port 8080 using HTTPS.

 If additional HTTP services are installed on the server hosting ipMonitor, verify that their IP address and port settings do not conflict with the ipMonitor port settings. For example, another HTTP service might use the default port 80.

You can generate and assign a [self-signed certificate](#) using the Secure Socket Layer Certificate options in the configuration program. Self-signed certificates are free.

 HTTPS requires an SSL server certificate assigned to your ipMonitor installation.


Configure the SNMP Trap Listener

The SNMP - User Experience Trap monitor is an event-based, non-polling monitor. This monitor listens for SNMP traps received by any SNMP agent in your monitored network. Each incoming trap is parsed and compared to the settings of the existing SNMP trap monitors to determine whether the application should trigger an information alert action.

All SNMP trap monitors you create in ipMonitor use the IP address and port combination that you enter in the SNMP Trap Listener section to listen for incoming SNMP traps.

Monitor a specific port

To monitor all IP addresses on a specific port, enter an IP address of 0.0.0.0. ipMonitor listens to every IP address on the port. For example, `https://0.0.0.0:162` enables ipMonitor to listen on every IP address assigned to the machine on port 162 using HTTPS. Port 162 is the standard SNMP listening port.

 Any SNMP agent that is expected to send traps to ipMonitor must be configured to send traps to the IP address and port specified here.

If the SNMP Trap Listener is not enabled, SNMP trap monitors will not work, even if the monitor is enabled.

Resolve SNMP Trap Listener conflicts

If the Windows SNMP Trap service is enabled on the ipMonitor host computer, this service may conflict with the ipMonitor SNMP Trap Listener. Both services 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 SNMP Trap Listener port to an unused port, and then change the outbound port of all the SNMP agents sending traps to ipMonitor.
- Disable the Windows SNMP Trap service from the Windows Control Panel interface. There are no adverse effects to disabling the Windows SNMP Trap service unless you are running another SNMP solution on the ipMonitor server that requires the Windows SNMP Trap service.

Connect ipMonitor to your network components

Use the Communications: Lockout dialog box to specify the IP addresses for network devices, servers, and applications that you want to monitor using ipMonitor.

IP access filters are an optional security feature that allow you to:

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

Click Add to add a new entry and then enter single IP addresses or ranges of IP addresses. To enter a single IP address, enter the same IP address into the Starting IP Address and Ending IP Address fields.


Install an SSL certificate

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

The following methods are supported for acquiring an SSL certificate:


- [Generate and install a self-signed certificate](#)
- Acquire a certificate from a trusted certificate authority
- Request a certificate using the Microsoft Windows Certificate Services Web interface
- Request a certificate from an enterprise certification authority using the MMC Certificates snap-in


This section describes how to [generate a self-signed certificate](#), which represents the easiest installation method at no cost.

 The Credentials Manager requires you to log in using a secure SSL (HTTPS) connection. If you log in using a non-secure channel (such as HTTP), the Credentials Manager displays a limited view of credentials and prohibits any changes to your credential configuration.

Generate a self-signed certificate

1. Open the Communications: SSL window.
2. Click the SSL Certificate Mode menu and select Self-Signed.
3. Click Create New Self-Signed Certificate.
4. Enter the fully qualified domain name of your ipMonitor server into the Common Name text box.
5. Click Create.
The certificate is created in the Local Machine certificate store and information regarding the newly generated self-signed certificate is displayed.
6. Click OK to accept the certificate.

 You must accept the certificate. Otherwise, the certificate is added to the store and not assigned to ipMonitor.

 After the SSL certificate is installed, configure ipMonitor to listen for HTTPS traffic by changing the Communications: Web Server Ports options in the ipMonitor configuration program.

Assign a Windows account to host the ipmonitorsrv service

You can use the Service Settings window to assign a Windows account that runs the ipmonitorsrv service.

When you choose an account, consider the Credentials Manager as a key element of the security model. The ipmonitorsrv service runs under an account with minimum permissions. The Credentials Manager impersonates accounts with elevated permissions when required to execute monitors, alerts, and features such as:

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

The following table lists the minimum permission requirements for any Windows Account assigned to the ipmonitorsrv service.

FOLDER NAME	PERMISSIONS
\ipMonitor\	READ + WRITE + EXECUTE
\ipMonitor\config*	READ + WRITE
\ipMonitor\db*	READ + WRITE if storing Monitor Statistics
\ipMonitor\historic*	READ + WRITE if storing Monitor Statistics
\ipMonitor\internal*	READ ONLY
\ipMonitor\logs\	READ + WRITE
\ipMonitor\state	READ + WRITE
\ipMonitor\wwwroot*	READ ONLY

To assign an account to the ipmonitorsrv service:

1. Decide whether to create a new Windows account or use the existing [LocalSystem account](#) to host the ipmonitorsrv service.
2. In the Service Settings window, click Browse.
3. Select an account from the local computer account container or the domain account container.
4. Verify that the startup type is set to Automatic.
5. Complete the wizard.

About the LocalSystem account


The LocalSystem account is the default Windows account assigned to the ipmonitorsrv service when you installed the application

You can use the LocalSystem account to host the ipmonitorsrv service. However, the privilege level of this account on the local machine is greater than the privilege level required by the ipmonitorsrv service. To harden your security model, SolarWinds recommends that you create a Local User account to specifically host the ipmonitorsrv service.

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

Disable the LocalSystem account

ipMonitor can function without Credentials Manager. For improved security, SolarWinds does not recommend disabling this feature.

 If you choose not to use Credentials Manager, assign a Domain Administrator class account to the ipmonitorsrv service. If a security breach occurs, this configuration can expose all resources that can access the high privileged account.

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

Beyond Getting Started

Now that ipMonitor is up and running, check out the ipMonitor Administrator Guide to customize your deployment. Additionally, the ipMonitor [Documentation website](#) contains additional documentation and training resources to help you get started.

The following table provides additional resources to help you move beyond getting started.

IF YOU WANT TO...	GO TO...
View the ipMonitor logs for troubleshooting	ipMonitor logs for troubleshooting
View all ipMonitor Knowledge Base (KB) articles	ipMonitor Knowledgebase Articles
Review the ipMonitor port requirements	Port requirements for all SolarWinds products
Watch an ipMonitor guided tour	SolarWinds ipMonitor Guided Tour
View the top five benefits of SolarWinds ipMonitor	Top 5 Benefits of SolarWinds ipMonitor
Access the SolarWinds Customer Success Center	SolarWinds Customer Success Center
Participate in discussions with SolarWinds ipMonitor professionals	SolarWinds THWACK
Get help resolving issues	
Learn more about SolarWinds products	
Contact Technical Support	SolarWinds Customer Support Information
Access the Customer Portal	SolarWinds Customer Portal