CONNECTWISE

Use the Monitor Wizard to Create Monitors in Automate

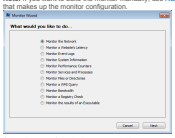
Overview

The Monitor Wizard allows you to easily create any type of monitor (network, system or internal) for a specific computer or group. The Network Device Monitor allows you to easily create any type of network device monitor for a group. This document guides you through using each of the wizards.

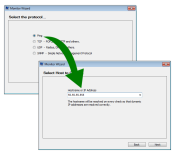
Create Monitor Using Monitor Wizard

To create a monitor using the Monitor Wizard:

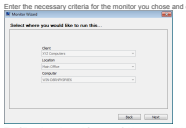
1. From the **Control Center**, click on **Browse** > **Clients** tab, right-click the desired computer and select **Monitors** > **Create Monitor Via Wizard**.
   Note: To create a remote monitor at the group level, open the group and click on the **Remote Monitors** tab and then click **Add**. You can also right-click on the group and select **Monitors** > **Create Monitor Via Wizard**. Both methods start the Monitor Wizard. If you decide not to use the wizard, you need to configure it manually. This is not recommended to use if you do not have a basic understanding of SQL syntax.
   Note: If you want to build the monitor manually, use Remote Agent Monitors for an explanation of each tab that makes up the monitor configuration.



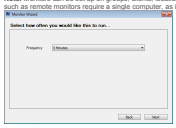
2. Select the type of monitoring you would like to accomplish and click **Next**. The Monitor Wizard requires additional information based on your selection. Refer to Monitor Types and Parameters later in this document for detailed information on each option.
   The remaining steps show the creation of a ping monitor.



3. Enter the necessary criteria for the monitor you chose and click **Next**.

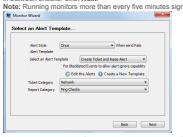


4. The **Client**, **Location** and **Computer** fields are not available for editing when running the Monitor Wizard from a computer. The monitor is created on the selected computer. Click **Next** to advance to the next screen.
   Note: Monitors can be set up on groups, clients, locations or single computers. However, some monitors, such as remote monitors require a single computer, as indicated in the above screen capture.

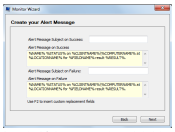


5. Select the **Frequency** in which this monitor should run. If you choose **Custom**, enter the number of seconds

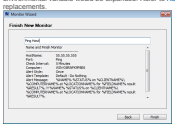
in between checks. Click **Next**.
Note: Running monitors more than every five minutes significantly slows down your network.



6. Alert styles determine the frequency in which you are notified when the monitor fails. Select the **Alert Style** from the drop-down.
   - **Continuous:** The alert action occurs every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket is created and does not get another ticket until the first one is resolved or deleted.
   - **Once:** The alert action occurs one time until the monitor checks and returns a success message.
   - **Second through Tenth:** The alert action occurs on the selected fail count until the monitor checks and returns a success message. For example, if Second is chosen, the monitor must have two consecutive failures before performing the alert action.
     Note: When a monitor returns a success message, the alert is reset and performs the alert action again upon failure.
7. Select the appropriate alert template from the **Alert Template** drop-down and click **Next**. If you need additional information on alert templates, please refer to Create New Alert Templates for more information.
8. Ticket categories are used to classify tickets and are generally used for integration with a PSA. Select a **Ticket Category** to associate with this monitor. If you need additional information on ticket categories, please refer to Using Ticket Categories.
9. Report categories are used to report statistics in the status gauges. Select an appropriate **Report Category** to associate with this monitor. If you need additional information on report categories, please refer to Using Status Gauges.



10. Accept the default message or make any desired changes and click **Next**.
    Note: Use the **[F2]** key to insert custom replacement fields. Replacements can be used anywhere an environmental variable would be expanded. Refer to Replacements (Variables) for the available replacements.



11. Enter a descriptive name for the monitor. Review the choices and select **Back** to make changes or **Finish** to create the monitor. The newly created monitor can be viewed by going to **Browse** > **Clients** and then right-click on the computer and select **Monitors** > **View Monitor**. The monitor does not show up until the monitor has run for the first time.
    Note: If a monitor fails to check in for 20,000 seconds (approximately 5.5 hours) after it was scheduled to check in, ConnectWise Automate uninstalls the monitor and reinstalls it.

Monitor Types and Parameters

Type/Description	Options and Parameters
Network: Used to check if connections are active depending on the type of protocol used (e.g., ping, TCP, POP, SMTP, HTTP, UDP, SNMP, etc.).	• Ping: Sends a ping packet to the specified host and returns the response time as the result. Can be used to check localhost or remote hosts. Requires the hostname or IP address to be entered in the Server Address field. • TCP - POP, SMTP, HTTP and others: Sends

Type/Description	Options and Parameters
	a TCP packet, including the data to send (e.g., quit\n), to the specified host and returns the result. Can be used to check localhost or remote hosts. Requires the hostname or IP address to be entered in the Server Address field and the Port number. • UDP - Radius, DNS and others: Sends a UDP packet, including the data to send (e.g., quit\n), to the specified host and returns the result. Can be used to check localhost or remote hosts. Requires the hostname or IP address to be entered in the Server Address field and the Port number. • Simple Network Management Protocol (SNMP): Sends an SNMP query to the specified server address. Can be used to check localhost or remote hosts. Requires the hostname or IP address to be entered in the Server Address field, the SNMP Community String and the Object ID (OID).
Website Latency: Used to check how long a website takes to respond to a request from the Automate server and returns the latency in milliseconds.	• Website Address: Enter the full address of the website, including the http:// or https://. • Comparison Function: Select any of the monitor conditions from the drop-down. For more information about the monitor condition definitions, please refer to Monitor Conditions. • Compare result against: Enter the website response time in milliseconds. Press [F2] in the text to compare box to display a list of escape characters that can be used for special characters.
Event Logs: Used to monitor Windows event logs. Windows event logs can be monitored by any combination of: the event log, the event type, the event source, the event ID or the event message. The asterisk (*) wildcard can be used in the log file, event source, event ID, and event message fields so that all information is gathered from that field respectively.	• LogFile: Select the type of log to monitor from the drop-down (e.g., Application, Security, Setup, System or Windows Update) or leave * for all logs. • EventType: Select the type of event to monitor from the drop-down (e.g., error, warning, information, security audit success, security audit failure or any). • Event Source: Enter the exact source of the log entry (e.g., Desktop Window Manager, MySQL, Microsoft-Windows-WMI, etc.) or leave * for all sources. • Event ID: Enter the Windows Event ID code to monitor.

Type/Description	Options and Parameters
	• Event Message: Enter a keyword or phrase that appears in the log to monitor (e.g., DNS server was unable to complete directory service…). • Monitor Locally on the Agent: Select checkbox to run the monitor on the agent machine to decrease the response time. However, this increases the load on the server. Selecting this option disables the ability to modify the Alert Style to something other than 'Once'. **Note:** By default, only audit security events from the Windows Event Log are monitored when setting up a remote event log monitor. This is to minimize the performance impact on the Automate agent while it searches for relevant event logs on the target system. If you want to monitor non-audit security logs, you must set the agent property "lti_noeventsecilmit" in the Agent Template settings. For more information, please see the Managing Agent Templates documentation. **Note:** The alert template for all Event Log monitors is set to **Once** automatically.
System Information: Used to gather software and hardware information from the Automate database and can be used to alert on various system checks (e.g., drive free space, services not running, expired passwords, etc.).	**Note:** Before you add a system information monitor, go to **Monitors** > **Internal Monitors to see if the monitor already exists**. In most cases, it is already created for you.
Performance Counters: Used to create a hardware or software benchmark to test against (e.g., drive time, exchange queue, drive write queue, etc.).	• Performance Counter Type: Select the type of performance monitor to create (e.g., Memory PageSec, Drive Read Queue, Drive Time, etc.). • Performance Object: The performance counters on the local machine populate the available objects. Select the object to monitor from the drop-down (e.g., memory, process, print queue, etc.). • Performance Counter: Values are based on the performance object selected. Select the value to monitor from the drop-down (e.g., page reads/sec, cache faults/sec, etc.). • Instance: Some performance counters have multiple instances, select a specific instance of the performance counter to monitor or leave blank to monitor them all.

Type/Description	Options and Parameters
Services and Processes: Used to watch a service or process.	• Type: Select 'Services' or 'Processes'. • Service Name: The list of services and processes are populated from the agents. Select the service or process to monitor. • Alert When Not Running: This checkbox is selected by default. When selected, an alert automatically generates when the selected process or service is not running. Some processes or services might be threatening; therefore, alerts should be generated if the service or process starts running. Deselect this checkbox to turn this feature off.
Files or Directories: Monitors files and directories to see if they exist. Additionally, files can be monitored for their size and directories can be monitored for the number of files.	• Path: Enter the full path for the directory or file. • Is Directory: Select this checkbox if the path leads to a directory. • Check if file exists: Select this checkbox for the monitor to generate an alert if the file exists in the selected path. • Check file size: Select this checkbox for the monitor to generate an alert based on the file size of the file in the selected path.
WMI Query: This monitor is used to run WMI queries. A working knowledge of SQL and WMI is recommended before attempting to create this monitor.	• Windows Management Query: Enter a WMI query or select one from the target. If the query returns only one row then the first value of the row is the tested result. In a query that returns multiple rows, the count is the tested result. • Click the Run Query on My Workstation button to run a test of the query on the machine you are currently using.
Bandwidth: Monitors the bandwidth of the network device, not the network the device is on.	• Device IP Address: Enter the IP address of the device. • Version: Select the SNMP version. If you have selected version 1 or 2, enter a Community String, if necessary (e.g. public, private, etc.). If you have selected version 3, you need to provide the credentials for accessing the device. Optionally, you may select the Reveal Passwords checkbox to show the entered password in plain text. Enter the username with access to the device into the Username field. Enter the password for accessing the

Type/Description	Options and Parameters
	device into the Auth Password field and select the type of encryption from the corresponding Method drop-down. Enter the password for encryption into the Enc Password field, select the type of encryption from the corresponding Method drop-down. • Data to Watch: Select the desired type of data to monitor (e.g., ifInOcets, ifInErrors, etc.) A description for each data type displays below the drop-down. • Index to Watch: Select the index to watch or browse for the index by clicking the … ellipsis button.
Registry Check: Monitors the registry to see if the specified registry key exists in the Local Machine or Users registry hive.	• Registry Hive: Select the desired registry hive (e.g., HKey Local Machine). • Registry Key: Enter the key or sub-key to search for (e.g., Software\LabTech\Agent). • Value Name: Enter the value (e.g., User)
Results of an Executable: Runs executables on agent computers and return the results as an alert message. Arguments can be passed to these executables. The file runs and the results are used in the checks. If the executable does not have a complete path it is assumed to be in the LTSVC directory and if the executable does not exist in the LTSVC directory it downloads from the LTShare\ Transfer\Monitors.	• Executable: Select an executable from the drop-down. This information is updated when agents check-in to update that table. If you are manually entering the executable, the name of the executable needs to be one word and not contain any spaces (e.g., dctest.bat, repadmin64.exe, etc.). • Arguments: Enter any arguments to supply to the executable when it is called.

Create Network Device Monitor Using Monitor Wizard

The Network Device Monitor Wizard allows you to easily create any type of network device monitor for a group. Network device monitors can also be created for a specific device by right-clicking the desired device from the navigation tree and selecting Add New Monitor.

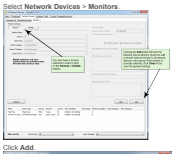
Note: If you want to manually build a monitor for a network device, refer to the Configuring Remote Monitors for more information on setting up and/or modifying remote monitors.

Business Case

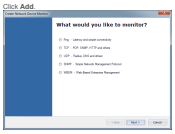
The Technician has numerous printers (identified as network devices in their Automate system) that seem to have persistent connection issues. The Technician uses the Network Device Monitor Wizard to create Ping monitors that can alert them if the printers go offline.

To create a network device monitor using the Network Device Monitor Wizard:

1. From the **Control Center**, click on **Browse** > **Groups** node, right-click on the group and select **Open**. Otherwise, add the new group using the steps in Creating and Populating Groups.
2. Select **Network Devices** > **Monitors**.

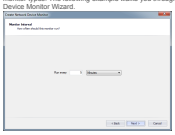


3. Click **Add**.

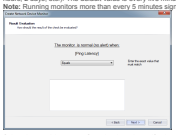


4. Select the type of monitoring you would like to accomplish and click Next. For the following example, select the Ping monitor.
   - **Ping:** Sends 4 rapid pings to the network device and return the Round Trip Average (RTA) for the ping packets.
   - **TCP:** Sends a TCP packet, including the data to send (e.g., quit\n), to the network device and returns the result. This option requires a port to be selected in the TCP Port drop-down and the text that to be sent in the Text to send on connect field.
   - **UDP:** Sends a UDP packet, including the data to send (e.g., quit\n), to the network device and returns the result. This option requires a port to be selected in the UDP Port drop-down and the text that is sent in the Text to send on connect field.
   - **SNMP:** Sends an SNMP query to the network device. This option requires an OID to be entered for the query. To help determine the OID, click the OID Lookup button to open the OID Selector screen. Additionally, the Group, Manufacturer, Model and Check can all be selected from their respective drop-downs.
   - **WBEM:** Runs a Web-Based Enterprise (WBEM) query on the network device. A working knowledge of the WBEM for the targeted device is recommended before attempting to create this monitor.

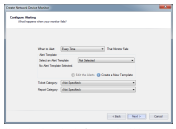
Requires a Namespace for the query and the WBEM Query to be entered.
Refer to the Creating Remote Monitors for more detailed information on each of these different monitor types. The following example walks you through creating a ping monitor using the Network Device Monitor Wizard.



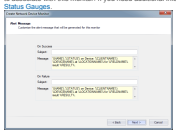
5. Enter the frequency that this monitor should run in the **Run every** field and drop-down (e.g., 10 minutes, 12 hours, 2 days, etc.). The default value is every five minutes. Click **Next**.
   Note: Running monitors more than every 5 minutes significantly slows down your network.



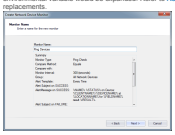
6. Select the condition to use from the drop-down. If using 'Between' as a condition on any of the monitors, the result should be entered in lowercase as, 'value x and value y' (e.g., 2 and 5). For more information on conditions, please refer to Monitor Conditions.
7. Enter a value to **Compare** the returned value to in the **Result** field, if necessary. Escape special characters with \xNN = Any hex character, where NN is A-F or 0-9. For system checks, use -1 (Missing),0 (False), 1 (True). Use **[F2]** to bring up a list of escape characters that can be used for special characters. Click **Next**.



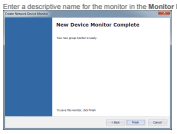
8. Alert styles determine the frequency in which you are notified when the monitor fails. Select the alert style from the **When to Alert** drop-down.
   - **Every Time:** The alert action occurs every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket is created and does not get another ticket until the first one is resolved or deleted.
   - **Once:** The alert action occurs one time until the monitor checks and returns a success message.
   - **Second through Tenth:** The alert action occurs on the selected fail count until the monitor checks and returns a success message. For example, if Second is chosen, the monitor must have two consecutive failures before performing the alert action.
     Note: When a monitor returns a success message, the alert is reset and performs the alert action again upon failure.
9. Select the appropriate alert template from the **Alert Template** drop-down and click **Next**. If you need additional information on alert templates, please refer to Configuring New Alert Templates for more information.
10. Ticket categories are used to classify tickets and are generally used for integration with a PSA. Select a **Ticket Category** to associate with this monitor. If you need additional information on ticket categories, please refer to Using Ticket Categories.
11. Report categories are used to report statistics in the status gauges. Select an appropriate **Report Category** to associate with this monitor. If you need additional information on report categories, please refer to Using Status Gauges.



12. Accept the default message or make any desired changes and click **Next**.
    Note: Use the **[F2]** key to insert custom replacement fields. Replacements can be used anywhere an environmental variable would be expanded. Refer to Replacements (Variables) for the available replacements.



13. Enter a descriptive name for the monitor in the **Monitor Name** field and click **Next**.



14. Review the choices and click **Back** to make changes or **Finish** to create the monitor. The newly created monitor can be viewed by:
    - Double-clicking on the group the monitor was created in and selecting **Network Devices** > **Monitors**.
    - Double-clicking on the network device and selecting the **Monitors** tab.
    - The monitor also appears under the main list of monitors and can be viewed by clicking **Automation** > **Monitors** > **View Monitors** > **Remote Network Monitors** tab.
      Note: If a monitor fails to check in for 20,000 seconds (approximately 5.5 hours) after it was scheduled to check in, Automate uninstalls the monitor and reinstall it.