CONNECTWISE

Create Remote Monitors

Overview

This page walks you through the process of creating remote monitors as well as editing the remote monitor configuration and creating overrides.

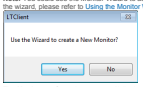
Create Remote Agent or System Monitors

While most monitors can be set up on groups, clients, locations or single computers, remote monitors which include Remote Agent Monitors and System Monitors require a single agent enabled computer. Remote Monitors can be created manually or by using the Monitor Wizard; however, creating a monitor manually does require a basic understanding of SQL syntax for some monitor types.

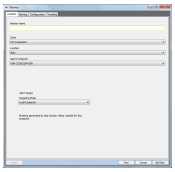
Note: Remote monitors can be created at the group level using the Monitor Wizard.
This section will walk you through the steps to create a remote monitor manually; however, it is recommended that if you are not familiar with SQL syntax to use the Monitor Wizard. Refer to Using the Monitor Wizard to Create Monitors for more information.

To create a remote monitor on an agent computer manually:

1. From the **Control Center**, click **Browse** > **Clients** node, right-click on the desired **Computer** and select **Monitors** > **Create Monitor**.
   Note: You could use the Monitor Wizard to assist in creating a new monitor, for more information regarding the wizard, please refer to Using the Monitor Wizard to Create Monitors.

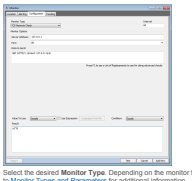


2. The **Monitor** configuration screen will display. Initially, not all monitor tabs (Status, History and Data Collector) will display until the new monitor has been saved.



3. Enter a descriptive name to identify the monitor in the **Monitor Name** field.
4. The **Client**, **Location** and **Agent Computer** will default to the computer that was selected. Make the desired changes if you want the monitor to be associated with a different computer.
5. The **Alert Target** controls where alerts are generated. For example, your network probe is pinging another computer but you want alerts to show up for that specific computer instead of the probe computer. By default, any alerts will be created on the local computer. Change the **Alert Target**, if desired. Refer to Set Alert Targets for more information.
6. Click on the **Alerting** tab.

7. Select an **Alert Template** from the drop-down. Refer to Configuring Alert Templates for more information.
8. Select the **Alert Style** from the drop-down. Alert styles determine the frequency in which you will be notified when the monitor fails.
   - **Continuous:** The alert action will occur every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket will be created and will not get another ticket until the first one is resolved or deleted.
   - **Once:** The alert action will occur one time until the monitor checks and returns a success message.
   - **Second through Tenth:** The alert action will occur 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 will perform the alert action again upon failure. On first creation, the monitor must return a success status before it will send alerts.
9. Enter a subject for successful alert messages sent via email in the **Alert Message Subject on Success**. When used with a custom failure message, this subject will only be used for the successes. Leave blank for a default subject.
   Tip: To embed ticket comments when a normal ticket update is posted, simply place a tag <COMMENT><COMMENT> and this will put the text in the tags into a comment attached to the ticket. This will make the Ticket alert action create two entries: one client facing and one technician facing.
10. A generic success alert message is created for you. Make any desired changes. Press **[F2]** for available Automate replacements.
11. Enter a subject for failure alert messages sent via email in the **Alert Message Subject on Failure**. Press **[F2]** for available variables. Leave this blank to use the success message instead.
    Note: If the alert action will be used to create an alert or to open a ticket, the **Alert Message Subject on Success** and **Alert Message Subject on Failure** should be the same. If not, the alerts will not be cleared correctly and the tickets will not auto-close as expected. The subject string can be copied and pasted from one subject field to the other to ensure consistency.
12. The **Ticket Category** is used to classify tickets and is leveraged by your PSA software (if supported) to route common types of tickets to different service boards in the PSA. New monitors will need to be assigned to the proper ticket category. Refer to Using Ticket Categories for more information.
13. Select a script from the **Script To Run** drop-down to run a script when the monitor fails.
    Important: If you select a script from the **Script To Run** drop-down, you must use an alert template that has the **Script Error** alert action checkbox selected as well as **Not Selected** selected from the **Script Action** drop-down. Refer to Configuring Alert Templates for more information on alert actions.
14. Statistics can be recorded for this monitor and combined with other monitors with the same report category and reported in the status gauges. To record the statistics from this monitor, select a **Report Category** from the drop-down. Refer to Using Status Gauges for more information.
15. Click on the **Configuration** tab.



16. Select the desired **Monitor Type**. Depending on the monitor type you select, the parameters will vary. Refer to Monitor Types and Parameters for additional information.
    Note: Running monitors more frequently than every five minutes can significantly slow down your network.
17. Complete the parameters for the chosen monitor type.
18. Select the **Condition** to use from the drop-down. Refer to Monitor Conditions for additional information.
    Note: If choosing a state based monitor condition, three fields named Normal, Warning and Error will appear. The three state fields should be completed using the same conditions you would for a normal pass/fail monitor. Refer to Using State Based Monitoring for more information about state based conditions.
    Note: 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).
19. Select the **Use Expressions** checkbox if using expressions in your syntax.
20. Enter a value to compare the returned value to in the **Result** field. 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.
    Note: The **Language Override** button allows for localization of the monitor. If configuring a monitor to use in varying language cultures, please refer to Localize Monitors for assistance.

Monitor Types and Parameters

Monitor Type	Parameters
Ping Check	The Ping Check will send 4 rapid pings to the target and return the Round Trip Average (RTA) for the ping packets. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the hostname or IP address of the host to ping into the Server Address field.

Monitor Type	Parameters
	c. Select or enter the port number to ping in the Port combo box. d. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Website Latency Check	The Website Latency Check returns the time (in ms) it takes to retrieve the website. a. Enter the full address of the website, including the http:// or https:// in the Website Address field. b. Select any of the monitor conditions from the Comparison Function drop-down. For more information about the monitor condition definitions, please refer to Monitor Conditions. c. Enter the website response time in milliseconds in the Compare result against field. Press [F2] in the text to compare box to display a list of escape characters that can be used for special characters.
TCP Network Check	The TCP Network Check sends a TCP packet, including the data to send (e.g., quit\n), to the specified host and returns the result. This can be used to check localhost or remote hosts. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the IP address of the server into the Server Address: field. c. Enter the port number into the Port: field. d. Enter the data to send in the Data to Send: field. Press [F2] to bring up a list of replacements to use. 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.
UDP Network Check	The UDP Network Check sends a UDP packet, including the data to send (e.g., quit\n), to the specified host and returns the result. This can be used to check localhost or remote hosts.

Monitor Type	Parameters
	a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the IP address of the server into the Server Address:field. c. Enter the port number into the Port: field. d. Enter the data to send in the Data to Send: field. Press [F2] to bring up a list of replacements to use. 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.
SNMP OID Check	The SNMP OID Check sends an SNMP query to the specified server address. Can be used to check localhost or remote hosts. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the IP address of the server into the Server Address: field. c. Enter the community string (e.g., public) into the Community String: field. d. Enter the object identifier (OID) into the Object Identifier: field. An OID is a period separated series of numbers that identifies a component in the SNMP tree (e.g., 1.2.840.10006.300.43.1.3 is for the 'dot3adTablesLastChanged' object of a Cisco router). You can use the Preloaded SNMP Checks section to add any OIDs already stored in Automate or use the OID Lookup link to open the mibsearch webpage to find the OID number of an object you want to check. e. If you are not using SNMP protocol v2, deselect the Use SNMP Protocol v2 checkbox. **Note:** The following parameters are not necessary if you have already provided the OID. If the OID is already stored in Automate, you may use the fields in the Preloaded SNMP Checks section to choose an object you want to check and it will fill out the Object Identifier field with the OID for the object.

Monitor Type	Parameters
	f. Select a group from the Group drop-down. The drop-down contains very generic types (e.g., Routers) to begin refine your search for an object. g. Select a manufacturer from the Manufacturer: drop-down. Depending on the group chosen, the Manufacturer drop-down will populate with manufacturers with objects that have been added to Automate (e.g., Cisco). h. Select the model from the Model: drop-down. Based on the manufacturer chosen, the drop-down populates with models for which Automate has OIDs (e.g., Catalyst 6509). i. Select a check from the Check: drop-down. This will be the actual object you are interested in checking (e.g., FanState). j. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Performance Counter Check	The Performance Counter Check creates a hardware or software benchmark to test against (e.g., drive time, exchange queue, drive write queue, etc.). a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Select a counter option from the Performance Counter Preset: drop-down. When a performance counter is selected, the Performance Object and Performance Counter automatically populate. If Custom Performance Object is selected then you will need to select a performance object from the Performance Object: drop-down and Select a performance counter from the Performance Counter: drop-down. c. If applicable, select an instance from the Instance: drop-down. If there are no instances listed, try loading them by clicking Load list from Agent. d. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
File\Directory Check	The File\Directory Check is used to monitor files and directories to see if they exist. Additionally, files can be

Monitor Type	Parameters
	monitored for their size and their contents. Directories can be monitored for the number of files. This requires the full path to the file or directory. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the full path to the file or directory in the Path to File or Directory: field. c. Ensure that Sample is selected in the Value To Use drop-down. File\Directory Check does not use any smoothed values.
Service Check	The Service Check is used to determine if a service is stopped or running. Result for comparison: 1 if running, 0 if stopped and -1 if unknown. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Select the service to check in the Service Name drop-down. c. Ensure that Sample is selected in the Value To Use drop-down. Service Check does not use any smoothed values.
Disk Space Check	The Disk Space Check returns the amount of free space on the drive in MB. This monitor cannot be applied to a group. Instead, group monitors use the DRV - Free Space Remaining monitor to regulate this. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Select the drive to check into the Drive Letter drop-down. c. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Registry Check	The Registry Check is used to check the registry for a specific key or value. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor

Monitor Type	Parameters
	should ping the host into the Interval field. b. Select the registry hive (e.g., HKey Local Machine) from the Registry Hive drop-down. c. Enter the registry key into the Registry Key field. • Enter the value name in the Value Name field. d. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Process Check	The Process Check is used to determine if a process is stopped or running. Result for comparison: 1 if running, 0 if stopped and -1 if unknown. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Select the process to check into the Process Name: drop-down. c. Ensure that Sample is selected in the Value To Use drop-down. Process Check does not use any smoothed values.
Event Log Check	The Event Log Check is 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 will be gathered from that field respectively. a. Select which log file to monitor into the Log File Name: drop-down or use (*) for all logs. b. Select an event type to monitor from the Event Type drop-down. c. Enter a source to monitor into the Source: field or use (*) for all. The source used must be the Automate source, not the Windows source. d. Enter an event ID to monitor into the Event ID: field. e. Enter a message to monitor for into the Message Regular Expression: field. f. Select the Monitor Locally on the Agent checkbox to run the monitor on the agent

Monitor Type	Parameters
	machine to decrease the response time. However, this will increase the load on the server. Selecting this option will disable the ability to modify the Alert Style to something other than 'Once'.
External EXE Check	The External EXE Check will run executables on agent computers and return the results as an alert message. Arguments can be passed to these executables. The file will run and the results will be 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 will download from the LTShare\Transfer\Monitors. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the full path to the EXE to run in the Executable: field or use the drop-down arrow to choose from an executable in the LTshare folder. If the executable does not have a path, it is assumed to be in the LTSVC directory and if it is not there, it will attempt to download from the LTShare\Transfer\Monitors directory. c. If applicable, enter any additional arguments for the EXE in the Arguments: field. d. If applicable, enter any .NET regular expressions to use in the results into the Regular Expression for Results: field. e. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
WMI Query Check	The WMI Query Check is used to run WMI queries. A working knowledge of SQL and WMI is recommended before attempting to create this monitor. If the query returns only one row then the first value of the row will be the tested result. A query that returns multiple rows, the count will be the tested result. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter or select the query in the Windows

Monitor Type	Parameters
	Management Query combo box. c. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Web-Based Enterprise Management Check	The Web-Based Enterprise Management Check is used to run Web-Based Enterprise (WBEM) queries on network devices. A working knowledge of the WBEM for the targeted device is recommended before attempting to create this monitor. This monitor is only available when creating a Remote Network Monitor on a network device. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the query in the WBEM field. c. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Bandwidth Monitor Check	The Bandwidth Monitor Check will monitor various bandwidth to identify slowness and bottlenecks. Various data elements can be monitored (e.g., number of inbound packets containing errors, number of packets delivered, number of packets requested to be transmitted, number of inbound packets which were chosen to be discarded, etc.). a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the IP address of the device into the Device IP Address: field. c. Select the version of SNMP from the Version: drop-down. • Enter the community string into the Community String: field. d. If you have selected SNMP version 3, you will 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 device into the Auth Password:field and select the type of

Monitor Type	Parameters
	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. e. Select the data to watch from the Data to Watch: drop-down. f. Select the index to watch into the Index To Watch: drop-down or browse for the index by clicking the ... button. g. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
Sensor Check	The Sensor Check is used to pull information from hardware sensors on the agent (e.g., temperature, fan, voltage, current and power. Refer to Sensor Monitors for more information. a. From the Monitor Configuration screen, enter a frequency (in seconds) in which the monitor should ping the host into the Interval field. b. Enter the sensor number to monitor into the Sensor Number field. c. Select the type of sensor from the Sensor Type: drop-down. d. If necessary, select a value option from the Value To Use drop-down. The value options are for using intelligent baselining for monitor data. Refer to Trending Tab for information on these options.
PowerShell Monitors	PowerShell Monitors are supported as part of the EXE remote monitor. To configure a PowerShell monitor, upload your PS1 script to the LTShare\Transfer\Monitors directory on the Automate server. Then call your PS1 file as an executable with any required parameters for your script.

Monitor Conditions

Condition	Description
Anything	Monitor is successful on any result. Useful for data collection monitors.
Between xx and yy	Monitor is successful on anything that is in between the entered values to compare. The values are entered in

Condition	Description
	lowercase following the format 'xx and yy'.
Contains	Monitor is successful on anything that contains the entered value to compare.
Data Collection Only	Not for the purpose of alerting, shows 'Data Collection Only'.
Does Not Contain	Monitor is successful on anything that does not contain the entered value to compare.
Does Not Regex Match	Monitor is successful on anything that does not contain a specific regular expression match.
Equals	Monitor is successful on exact matches of the entered value to compare. If an exact match is not returned, it will trigger a failure.
Exists	Monitor is successful on any result except -1 (unknown). -1 will trigger a failure. For example, File/Directory Check monitors will always be in a success state when using 'Exists', since the check result is -1 which is for missing files.
Greater Than	Monitor is successful on anything that is greater than the entered string or data type (e.g., date).
Greater Than/Equal	Monitor is successful on anything that is greater than or equal to the entered string or data type (e.g., date).
In Set aa,bb	Monitor is successful when the value exists in a set of values (e.g., "aa,bb" where bb would be InSet, but cc would not). The monitor will fail if not in all specified sets. Do not include parenthesis/brackets/quotes, etc. within the monitor condition.
Less Than	Monitor is successful on anything that is less than the entered value to compare. The monitor will fail if the result equals or is greater than entered value.
Less than/Equal	Monitor is successful on anything that is less than or equal to the entered value to compare.
Missing	Monitor is successful if the value is not present.
Not Equals	Monitor is successful on anything that does not exactly match the entered value to compare. An exact match will trigger a failure.
Not In Set aa, bb	Monitor is successful when the value does not exist in a set of values (e.g., "aa,bb" where bb would be InSet, but cc would not).The monitor will fail if in specified sets. Do not include parenthesis/brackets/quotes, etc. within the monitor condition.
Regex Match	Monitor is successful on anything that contains a specific

Condition	Description
	regular expression match.
State Based	State Based changes the mode to a three stage check. The three stage check has Normal State, Warning State and Error State. Each stage can be configured with a condition and result to compare.

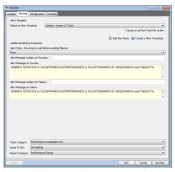
Create a Remote Network Monitor

Remote Network Monitors provide you with comprehensive monitoring of your clients' networks and allow you to track and manage the status of various network devices. These monitors run on the probe that is located on the same network as the devices being monitored. As with other monitors, you may have these monitors alert you if thresholds are exceeded. This section will walk you through the steps to manually create a remote monitor on a network device.

Note: Remote Network Monitors may also be added to a group by using the Remote Network Monitor Wizard. Refer to Create Network Device Monitors for more information.
To manually create a remote monitor on a network device :

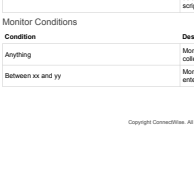
1. From the **Control Center**, click on **Browse** > **Clients** tab > **Network Devices** tab, right-click on the desired network device and select **Add Monitor**.

2. Enter a descriptive name to identify the monitor in the **Monitor Name** field.
3. The **Client**, **Location** and **Network Device** will default to the device that was selected. Make the desired changes if you want the monitor to be associated with a different device.
4. The **Alert Target** controls where alerts are generated. For example, your network probe is pinging another computer but you want alerts to show up for that specific computer instead of the probe computer. By default, any alerts will be created on the local computer. Change the **Alert Target**, if desired. Refer to Set Alert Targets for more information.
5. Click on the **Alerting** tab.



6. Select an **Alert Template** from the drop-down. Refer to Configuring Alert Templates for more information.
7. Select the **Alert Style** from the drop-down. Alert styles determine the frequency in which you will be notified when the monitor fails.
   - **Continuous:** The alert action will occur every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket will be created and will not get another ticket until the first one is resolved or deleted.
   - **Once:** The alert action will occur one time until the monitor checks and returns a success message.
   - **Second through Tenth:** The alert action will occur 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 will perform the alert action again upon failure. On first creation, the monitor must return a success status before it will send alerts.
8. Enter a subject for successful alert messages sent via email in the **Alert Message Subject on Success**. When used with a custom failure message, this subject will only be used for the successes. Leave blank for a default subject.
   Tip: To embed ticket comments when a normal ticket update is posted, simply place a tag <COMMENT><COMMENT> and this will put the text in the tags into a comment attached to the ticket. This will make the 'Ticket' alert action create two entries: one client facing and one technician facing.
9. A generic success alert message is created for you. Make any desired changes. Press **[F2]** for available Automate replacements.
10. Enter a subject for failure alert messages sent via email in the **Alert Message Subject on Failure**. Press **[F2]** for available variables. Leave this blank to use the success message instead.
    Note: If the alert action will be used to create an alert or to open a ticket, the **Alert Message Subject on Success** and **Alert Message Subject on Failure** should be the same. If not, the alerts will not be cleared correctly and the tickets will not auto-close as expected. The subject string can be copied and pasted from one subject field to the other to ensure consistency.
11. The **Ticket Category** is used to classify tickets and is leveraged by your PSA software (if supported) to route common types of tickets to different service boards in the PSA. New monitors will need to be assigned to the proper ticket category. Refer to Using Ticket Categories for more information.

12. Select a script from the **Script To Run** drop-down to run a script when the monitor fails.
    Important: If you select a script from the **Script To Run** drop-down, you must use an alert template that has the **Script Error** alert action checkbox selected as well as **Not Selected** selected from the **Script Action** drop-down. Refer to Configuring Alert Templates for more information on alert actions.
13. Statistics can be recorded for this monitor and combined with other monitors with the same report category and reported in the status gauges. To record the statistics from this monitor, select a **Report Category** from the drop-down. Refer to Using Status Gauges for more information.
14. Click on the **Configuration** tab.



15. Select the desired **Monitor Type**. Depending on the monitor type you select, the parameters will vary. Ping Check, SNMP OID Check, TCP Network Check, UDP Network Check and Web-Based Enterprise Management Check are the only available monitors when creating a Remote Network Monitor. Refer to Monitor Types and Parameters for additional information.
    Note: Running monitors more frequently than every five minutes can significantly slow down your network.
16. Complete the parameters for the chosen monitor type.
17. Select the **Condition** to use from the drop-down. Refer to Monitor Conditions for additional information.
    Note: If choosing a state based monitor condition, three fields named Normal, Warning and Error will appear. The three state fields should be completed using the same conditions you would for a normal pass/fail monitor. Refer to State Based Monitoring for more information about state based conditions.
    Note: 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).
18. Select the **Use Expressions** checkbox if using expressions in your syntax.
19. Enter a value to compare the returned value to in the **Result** field. 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.
    Note: If a monitor fails to check in for 20,000 seconds (approximately 5.5 hours) after it was scheduled to check in, Automate will uninstall the monitor and reinstall it.

Edit Group Remote Monitors

Remote Monitors run external from the Automate server on an agent-enabled computer or network device (e.g.,

Perf-Network Bandwidth, Perf-Total CPU Processor Time, etc.). These monitors should correspond with your SLAs and business needs. Remote Monitors assigned to a group are accessed by double-clicking on the group; whereas, the Remote Network Monitors, Remote Agent Monitors and System Monitors tab of the Monitors screen will show a list of all remote monitors by device.

Note: When a computer joins or is removed from the group, the monitor is installed or removed. These monitors are controlled by the server and will automatically be recreated if they are deleted or changed. As with scripts, you can determine what computer type to run the monitor on. This allows you to define exchange monitors that only monitor exchange servers.

To edit the group remote monitors:

1. From the **Groups** node, double-click on the **Group** to open the **Group** screen. New groups that you create will not have any remote monitors assigned and will have to be created.
2. Select **Computers** > **Remote Monitors** (or if the group is managing network devices, select **Network Devices** > **Monitors**).

All Remote Monitors associated with the group will display.

Column	Description
Name	Displays the descriptive name of the monitor. This is the name that will display on the Network and System tabs of Monitors.
Check Type	Displays the check action of the monitor (e.g., perf, system, ping, etc.) For a list of the different Check Actions refer to the Monitor Types and Parameters table in this document.
Host	Displays the performance category of the monitor (e.g., memory, physical disk, service, etc.). This is available on the Computers tab only.
Service	Displays the service (e.g., HTTP, Disk Transfers/ sec, % Idle Time, etc.).
Interval	Displays the amount of time in between monitor checks (in seconds).

Column	Description
Limit to	Displays the search, if any, that will limit the computers that this monitor is installed on. For example, an ESET® antivirus search would limit the monitor to only those computers in the group that meet the ESET search criteria. ESET search criteria.
Alert Template	Displays the alert template associated with the monitor.
Alert Script	Displays the alert script associated with the monitor, if any.
Monitors Installed	Displays the number of computers in this group that have the monitor.
Ticket Category	Displays the ticket category associated with the monitor.
Report Category	Displays the report category associated with the monitor.

Tip: You can filter the results based on the check type, alert template or both. For example, if you want to limit the results to only remote monitors with the 'PERF' check type and using the 'Default - Create LT Ticket' alert template, you select those values in the **Check Type** and **Alert Template** drop-downs.

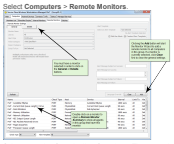
3. Select a monitor from the list of monitors. The general settings will populate based on the selected monitor.
Tip: You can multi-select multiple monitors to make bulk changes. Simply highlight the monitors you want to change. A checkmark will display next to the field to indicate which fields will be saved. If the field does not have a checkmark, the unchecked item will retain its original value. Select or deselect desired fields. Make the desired changes and click **Update**.
4. The **Monitor Name** is the descriptive name of the monitor that appears in the Network Monitors or System Monitors tab of the Monitors screen. Make any desired changes.
5. The **Limit to** field allows you limit the group to run this monitor on, by only those computers that meet the search criteria. Select **All** from the drop-down to run this monitor on all agents in this group; otherwise, select the appropriate search to limit the group to only agents that meet the search criteria.
6. Select the **Alert Style** from the drop-down.
   - **Continuous:** The alert action will occur every time the monitor checks and fails with the exception of the ticket alert action. Only one ticket will be created and will not get another ticket until the first one is resolved or deleted.
   - **Once:** This will perform the alert action defined in the alert template one time until the monitor returns a success message.
   - **Second thru Tenth:** This will perform the alert action defined in the alert template on a specific fail count until the monitor returns a success message. For example, if this is set to 'Third', the alert action will be performed after the third consecutive failure.
7. The **Ticket Category** is used to classify tickets and when tickets are generated by the monitor, the ticket will be routed to your PSA software (currently ConnectWise® and Autotask® plugins) to different service boards/ queues based on the ticket category. Most monitors have already been assigned a default ticket category but you can select a different category from the drop-down.
8. The **Report Category** is used to separate this monitor into a group for reporting and used by the status gauges. Most monitors have already been assigned a default report category but you can select a different category from the drop-down.

9. Select a script from the **Script To Run** drop-down to run a script when the monitor fails.
Important: If you select a script from the **Script To Run** drop-down, you must use an alert template that has the **Script Error** alert action checkbox selected as well as **Not Selected** selected from the **Script Action** drop-down. Refer to Configuring Alert Templates for more information on alert actions.
10. Select the desired **Alert Template** from the drop-down. If an appropriate template does not currently exist, click on **Create a New Template** to create a new template. If you need instructions on how to create an alert template, please refer to Configuring Alert Templates.
Note: Alert templates can be edited from this screen; however, please note that any changes you make to existing alert templates will affect all monitors that are associated with that alert template.
11. Enter a subject for successful alert messages sent via email in the **Alert Message Subject on Success**. When used with a custom failure message, this subject will only be used for the successes. Leave blank for a default subject.
Tip: To embed ticket comments when a normal ticket update is posted, simply place a tag <COMMENT><\COMMENT> and this will put the text in the tags into a comment attached to the ticket. This will make the 'Ticket' alert action create two entries: one client facing and one technician facing.
12. A generic success alert message is created for you. Make any desired changes. Press **[F2]** for available Automate replacements.
13. Enter a subject for failure alert messages sent via email in the **Alert Message Subject on Failure**. Press **[F2]** for available variables. Leave this blank to use the success message instead.
Note: If the alert action will be used to create an alert or to open a ticket, the **Alert Message Subject on Success** and **Alert Message Subject on Failure** should be the same. If not, the alerts will not be cleared correctly and the tickets will not auto-close as expected. The subject string can be copied and pasted from one subject field to the other to ensure consistency.
14. Make any desired changes and click the **Update** button. To view the monitor configuration details, refer to the next section.

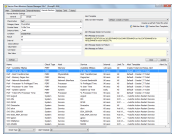
Edit Remote Monitor Configuration Details

To view/edit the remote monitor configuration details:

1. From the **Groups** node, double-click on the **Group** to open the **Group** screen.
2. Select **Computers** > **Remote Monitors**.



3. Select a monitor from the list of monitors. The general settings will populate based on the selected monitor.
4. Click **Details**.



5. There are different check actions that can be performed from a monitor. Each of the check actions require different parameters. Select the desired **Check Action** from the drop-down. For a description of each check action and the required parameters, refer to Monitor Types and Parameters. Depending on the type of monitor you are creating, some monitor types may not be available from the **Details** tab.
6. Select the **Condition** from the drop-down. This is the condition that must be met (e.g., equals, not equals, less than, etc.). If using 'Between' as a check condition, the result should be entered in lower case as, 'value x and value x' (e.g., 2 and 5).
7. Enter the **Result** to compare.
8. Enter the **Interval** between monitor checks. The default value is 300 seconds (5 minutes).
9. The **Data Collector** section is used to create data collector monitors. These keep a history of every check performed and the results for the past 90 days. If you want to keep the history for more than 90 days, you will need to add a 'RetentionDataCollector' property. Refer to Using Properties for Advanced Configuration for more information on how to add properties. A data collector monitor is only created if the Value, Unit and Max are all set.
   - **Value:** the name of the value you are graphing (e.g., 'Memory Avail' or 'Latency').
   - **Unit:** the type of measurement being collected (e.g., KB, MB or ms).
   - **Max:** the maximum value this monitor can reach. This is used for scaling on the graph on the **Monitor** > **Data Collector** screen. For example, if you have a Max of 100 but all your values are 200+, then your graph will be maxed out and show no definition.
   Note: When setting up Data Collector monitors, it will take up to 30 minutes for any data to appear and data is updated every 30 minutes.
10. Select the desired **Alert Template** from the drop-down.
Tip: If you are using the Ignite® plugin for configuration, you can change the alert template for multiple monitors at once in (**Dashboard** > **Config** > **Integration** > **Ignite** > **Group Monitor Management**).
11. Make any desired changes to the alert message subject and body for both success messages and failure messages.
Note: If the alert action will be used to create an alert or to open a ticket, the **Alert Message Subject on Success** and **Alert Message Subject on Failure** should be the same. If not, the alerts will not be cleared correctly and the tickets will not auto-close as expected. The subject string can be copied and pasted from one subject field to the other to ensure consistency.
Note: The **Language Override** button allows for localization of the monitor. If configuring a monitor to use in varying language cultures, please proceed to Localize Monitors for assistance.
12. Click **Update**. This remote monitor will be updated for all agents in the selected group.