



SysAid™

Monitoring Guide



Introduction	3
Monitoring of Servers.....	4
Server Configuration List	4
New Monitoring Configuration for a server	6
General Details Tab	8
Performance	8
Network Services	10
Software/Hardware Updates	11
Operating System Services	12
Operating System Processes.....	13
Editing existing configurations for a server	14
Monitoring of Workstations	14
Workstation Configuration List	14
New Monitoring Configuration for a Workstation	17
General Details Tab	18
Performance	19
Software/Hardware Updates	20
Operating System Services	21
Operating System Processes.....	22
Editing existing configurations for a workstation	22
Templates	24
Configuring a new template.....	26
Warnings:	28
Notifications	30
Sending Options for a notification	30
General	31
Mail Details.....	31
SMS Details	32
Service Request Details.....	33
Composing Notifications	34
Monitor Settings.....	36
Determining the Monitoring Time Interval Settings.....	36
Checking the connection of the agent to the network.....	37
Monitoring Map	39



Introduction

What is the SysAid Monitoring Module?

Monitoring is an extremely useful IT management tool, that enables you not only to address problems and malfunctions that have already occurred and have been reported on these via service requests, but to be notified about possible failures in your network and thus proactively prevent these in advance. Also, the SysAid Monitoring module will allow you to exercise better control over your network, and keep your assets from unwanted software and hardware. Thus, the monitoring tool can save you a great deal of time, costs and extra work.

The SysAid monitoring tool ensures utmost functionality of all your network components, from your most vital network applications, your servers, and down to each individual workstation on your network.

The monitoring tool is divided into two main sections: servers monitoring and workstations monitoring.


A server is a computer that delivers information and software to other computers on your network, while a workstation is a client computer connected to your network.

Working with our new SysAid Monitoring tool will raise your IT practice to a whole new level. You will be amazed by how many complications can simply be avoided in advance!




You can configure the necessary checks that will be performed on each asset or on a group of assets yourself. You can also create special templates composed of different series of checks that can then be assigned to the relevant assets.

Consult this simple and clear guide, and learn how to exploit your new SysAid monitoring module to your maximum advantage.



If you click one of the plus icons  in the list of servers, you will be able to see beneath the server entry all the tests applied to that particular sever, whether these tests were configured manually or via a server template.

Here you can also see the alert icons, which signify the results of a specific test for this server. The alert icons can appear in three different colors, according to the results of the test:

- If everything is in order, the alert icon will be green. 
- If the test shows the server has reached the threshold value you have defined for a warning, however, the alert icon will be yellow, signifying a warning. 
- In case one of the tests defined for the server indicates an error, the alert icon will be red. 

The color of the general alert icon for this server will be the color of the highest alert which exists for the collection of tests defined for this server. If all the monitoring tests are in order, their color will be green, and so will be the color of the server. However, if one of the tests is yellow, the server will be colored yellow too, and if a test shows an error and turns red, the whole asset will be marked by a red alert icon as well.

*When an alert icon flickers, this means there is no data available from the agent on this asset, for a period which exceeds the time limit you have previously defined.

From the **Server Configuration List** page you can also reach the graphs that show an average of the tests for each of the servers. Simply click the entry of a certain test for a certain server, and a popup screen with the related graphs will open.

Figure 2: Memory Usage Monitoring Tests Graph



The graphs you can see in the popup screen show the daily, weekly, monthly and yearly averages for the particular test performed on the particular server. In figure 2 above, for instance, you can see the daily and the weekly graphs for the memory usage tests performed on a certain server in our network. The vertical axis defines the percentage of memory usage of the server, while the horizontal axis represents the time during which the tests were performed.

Note that the time is calculated as an average, which is different for each of the four graphs: the daily graph is displayed with a five minutes average; the weekly graph with 30 minutes average; the monthly graph with two hours average; and finally, the yearly graph is displayed with an average time of a whole day.

The limits you have defined as a warning threshold and an error threshold for the test appear in the graph as horizontal lines in yellow and in red, respectively.

Test thresholds and many other configurations for a server are made in the **Monitoring Configuration** page. You can reach this page by clicking on one of the servers listed next to the plus icons . Read further in this guide for detailed explanations about this page.

New Monitoring Configuration for a server

⇒ Servers

Server Configuration List

⇒ New ⇒ Monitoring Configurations




When you click the **New** icon:  in the Server Configuration List, you will reach a page called **Monitoring Configurations** (see figure 3 below), which contains six tabs. The first tab is a **General Details** tab. Each of the next five tabs stands for a type of monitoring tests that can be preformed on the server you wish to configure new monitoring definitions for.


Figure 3: Monitoring Configuration New Page



Most of the monitoring definitions are identical for both servers and workstations. You can find the same tabs in the parallel page **Monitor Configuration New** under the **Workstations** section:

⇒ Workstations

Workstation Configuration List

⇒  ⇒ Monitoring Configurations New

Note that workstations, unlike servers, cannot be monitored for network services, and are limited to two monitoring tests per workstation. How to configure monitoring configurations for workstations is elaborated on later in this guide.

In addition, the monitoring configurations available in SysAid are also identical when setting the monitoring tests templates for either servers or workstations. The only difference is that once you configure a monitoring tests template you can then choose to apply the template to a group of servers, or to a group of workstations. To learn more about configuring monitoring templates for your assets, please see the **Templates** section later in this guide.

The different test types available in the SysAid Monitoring Module are:

- Performance: hard disk usage, Central Processing Unit usage, memory usage, memory in use- RAM ratio.
- Network services (available for servers only): TCP/IP, Ping and Http/Https
- Software/hardware updates
- OS Services
- OS Processes

Following is a specific explanation for each of the tabs, and the different Monitoring Guide Draft.doctests available under it.



General Details Tab

Under this tab you should fill in the general details for the server you wish to configure new monitoring definitions to.

1. Browse for the server from the list of assets by clicking the **Change** button.
2. If a template is already defined for this server, you will see the button **Detach Template** enabled, so the template could be detached. However, for a server that is still not connected to any monitoring template, this button will be disabled.
3. Finally, under this tab you can see the 'No Data Notification' dropdown menu. Choose from the menu a notification relevant for the case this computer is not sending any data for a pre-defined amount of time. The time limit before this notification is sent is set in the **Monitor Setting** page, which is elaborated on later in this guide.

Note that unless you have previously composed a suitable notification, this option will not appear in the 'No Data Notification' dropdown menu. The different monitoring notifications can be set in the **Notifications** page, and how set a new notification so is also explained in detail later.

Performance

Under this tab you can configure four different monitoring tests: hard disk (HD) usage, Central Processing Unit (CPU) usage, memory usage, and memory in use/RAM ratio.

All these tests are meant to make sure the server is not overusing its resources. An overuse may result in a breach in the performance of the computer, so all its actions will be slower than the optimal pace.

How to configure the performance monitoring tests?

1. Choose the test you wish to configure for this asset from the **Description** dropdown menu.
2. Fill in the values for the warning and the error thresholds. The thresholds you are asked to choose refer to the highest value a certain test result can reach before a warning and before an error will be determined.



The values for the threshold fields are calculated in percentages. In case the test result exceeds the threshold value you have entered, a warning or an error will appear for the computer in question.

For example, if you choose the 'Memory in use' warning threshold to be 60%, when the server uses more than 60% of its memory, a warning will appear. To determine this threshold, simply type '60' in the 'Warning threshold' box.

Similarly, you can also decide that an error should appear when this server uses more than 80% of its memory. Simply insert '80' into the "Error Threshold" box.

3. In case of a warning or an error, a notification can be sent as well, according to your choice. If you wish to send warning and error notifications, select an appropriate notification from the 'Warning Notification' and the 'Error Notification' dropdown menus. Such appropriate notifications will be available in the dropdown menus only if you have previously composed them.

To learn how to compose monitoring notifications for different tests please consult the **Notifications** section in this guide.

4. Click **Add**.
5. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

Here is an explanation about the meaning of each of the performance monitoring tests:

- **Hard disk usage**-This is a test that continuously checks the amount of space used in the hard disk of the server, to prevent a situation of flooding the hard disk. For instance, for a windows CPU it is generally recommended that at least one GB will remain free for an ideal performance of the computer.
- **Central Processing Unit usage**- The CPU should also not be overused, and the CPU test can verify this, according to your definitions.
- **Memory usage**- Here you can make sure the computer is not using more memory than it should. The memory usage test refers only to the physical memory which exists in the hardware of the computer.
- **Memory in use/RAM ratio** –This test checks how much is used of both the physical memory which exists in the hardware, and the virtual memory in the hard disk. Since the memory in the hard disk is not as efficient, it is recommended not to rely on it on a regular basis.



Network Services

The network services tests are possible only for servers and not for workstations in the SysAid Monitoring tool. There are three different network services tests in SysAid: Generic TCP/IP, Ping and Http/Https. These tests appear in a dropdown menu under **Protocol** in the **Network Services** tab.

Note that the definitions for the threshold values for these tests can be set in the **Monitor Settings** page. This page can be reached from the left left bar SysAid menu:

Monitoring

⇒ Monitor Settings

Read more about this page later in this monitoring guide.

The **Generic TCP/IP** test checks the availability of a certain port on the server.

1. Choose from the 'Protocol' dropdown menu the 'Generic TCP/IP' test.
2. In the 'Port Number' box insert the number of the port you wish to check the availability of.
3. From the dropdown menu of the error notifications, you can choose one of the notifications you have prepared. An appropriate notification should state that the port you have specified was unavailable on the computer. To learn how to configure such notifications, please consult the **Notifications** section in this guide.
4. Click **Add** to save your Generic TCP/IP monitoring configurations for this asset.
5. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

The **Ping** test checks whether the pings are constantly sent from this server.

1. Choose from the 'Protocol' dropdown menu the 'Ping' test.
2. From the dropdown menu of the error notifications, you can choose one of the notifications you have prepared. An appropriate notification should state that no ping was sent from this server. To learn how to configure such notifications, please consult the **Notifications** section in this guide.
3. Click **Add** to save your Ping monitoring configurations for this asset.



4. Only once you have completed determining the entire monitoring configurations for this server in all the tabs click **OK** or **Apply** to save the configurations.

The **Http/Https** test checks whether a certain vital web application is available on the server. For instance, you may want to make sure the Google search engine is available for your employees and colleagues.

1. Choose from the 'Protocol' dropdown menu the 'http' test.
2. Insert the URL of the website of the vital web application in the 'URL' box. For example, if the application is Google, you can insert the URL: <http://www.google.com>
3. Enter a regular expression that can identify the web application you have chosen to monitor. The regular expression is a string that can be found in the html source of the homepage of the relevant web application. For example, to identify Google the regular expression:
" Sign in"
may be entered.
This will ensure the web application is indeed running for the server.
4. From the dropdown menu of the error notifications, you can choose one of the notifications you have prepared. An appropriate notification should state that the vital web application is not available on this server. To learn how to configure such notifications, please consult the **Notifications** section in this guide.
5. Click **Add** to save your Http/Https monitoring configurations for this asset.
6. Only once you have completed determining the entire monitoring configurations for this server in all the tabs click **OK** or **Apply** to save the configurations.

Software/Hardware Updates

Here you can check whether unwanted or dangerous software or hardware was installed on the computer in question. This is possible both for servers and for workstations. To find the Hardware/Software Updates tab in the parallel page **Monitoring Configurations New** for workstations, follow the **Workstations** link.

Now you can control the software and the hardware installed on all the machines in your network. Simply follow the instructions below:



1. Choose from the dropdown menu whether the test is for software or for hardware updates.
2. To identify the unwanted software or hardware, enter in the filter box a regular expression. For example, if you wish to be notified when an external hard drive is installed on your server, you can look for a regular expression such as "mass storage device". To find an appropriate regular expression that will identify the unwanted hardware it is advisable to check the add/remove section in the control panel of the computer itself.
3. Once the filter is set, you can choose one of the notifications you have prepared for this case from the dropdown menu. An appropriate notification should state that unwanted software or hardware was found on the server.
4. Click **Add**.
In case an unwanted software or hardware is installed on the server, your notification will be sent to the relevant administrator via an automatic service request, an SMS message, or an email, according to the way you have configured the notification. To learn how to compose the appropriate notification and how to configure to whom it will be sent and by what means, you should consult the **Notifications** section in this guide.
5. Once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

Operating System Services

Once you choose to add a computer from your network to the monitoring tool, the SysAid agent on this computer will begin to send constant updates from the computer. The result will be that a list of current OS services and processes for this computer will appear in the dropdown menu under **Service Name** or under **Process Name** in the **OS Services** or the **OS Processes** tabs for the computer in question.

The monitoring tests can be configured for both services and processes for each server or workstation on your network. The difference between processes and services is as follows: services are activated from the operating system, while processes are not necessarily activated from the OS, and can be also operated by the user. For example, Telnet, Tomcat and SysAid are services, while Java, Explorer, Skype and MSN Messenger are processes.



Under the **Operating System Services** tab you can check the services of the operating system for the particular server/workstation.

1. Choose the name of the service you wish to monitor from the dropdown menu called 'Service Name'. The list of the operating system services of this asset will appear in the dropdown menu under **Service Name**, if the SysAid agent is appropriately installed on the computer.
2. In this dropdown menu you can also find the option: "All Auto Started Services". If you choose this option, the SysAid Monitoring tool will check whether the services that are supposed to go up in the startup of the computer run as they should.
3. Choose an appropriate error notification that will indicate that a certain OS service is not running as it should on this computer. To learn how to compose such a notification, please consult the **Notifications** section in this guide.
4. Click **Add**
5. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

Operating System Processes

Under this tab you can check whether the processes of the particular workstation/server are running appropriately. Processes are the .exe files on the computer. For instance, AVG antivirus is an OS process. The list of processes is sent to SysAid Monitoring tool from the task manager of the computer which is being monitored. It is advisable to click the **Refresh List** button occasionally, in case a new process was added to the computer.

1. Choose the name of the process you wish to monitor from the dropdown menu called 'Process Name'. The list of the operating system processes of this asset will appear in the dropdown menu under **Process Name**, if the SysAid agent is appropriately installed on the computer.
2. Choose an appropriate error notification that will indicate that a certain OS process is not running as it should on this computer. To learn how to compose such a notification, please consult the **Notifications** section in this guide.
3. Click **Add**



4. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations

Editing existing configurations for a server

Editing existing monitoring configurations for a server is done in the same page as when you define new configurations for a server. In Figure 4 below you can see the page for editing existing configurations for a server in our network.

Figure 4: Monitoring existing configurations for a server



1. In the SysAid Monitoring Module go to:
⇒Servers
Servers Configuration List
2. Choose from the list of servers a server you wish to edit the monitoring configurations for.
3. See the explanations in the section **Monitoring Configurations for a New Server** above to learn about each of the available test types.
4. Modify the configurations that should be changed.
5. Only once you have completed modifying the entire monitoring configurations for the server in all the tabs click **OK** or **Apply** to save the changes.

Monitoring of Workstations

Workstation Configuration List

Go to: ⇒Workstations
Workstation Configuration List



This is the first page in the SysAid Monitoring module. This page is parallel to the Server Configuration List page, and almost identical to it.

Figure 5: Workstation Configuration List

Alert	Last update	Check type	Description
	4/16/07 10:20 AM	Software/Hardware Updates	Software, Filter: 01\02\07, Error Notification: none
	4/16/07 10:20 AM	Software/Hardware Updates	Software, Filter: 1\1\2007, Error Notification: none
	4/16/07 10:20 AM	Software/Hardware Updates	Software, Filter: 1\3\2008, Error Notification: none
	4/16/07 10:20 AM	Software/Hardware Updates	Software, Filter: 324, Error Notification: none

For the **Workstation Configuration List** page to contain any data about workstation monitoring, you first need to configure monitoring preferences for your assets. To learn how to do so, please go to **New Monitoring Configuration for a Workstation** section in this guide.

If you click one of the plus icons in the list of workstations, you will be able to see beneath the workstation entry all the tests applied to that particular computer, whether these tests were configured manually or via a workstation template.

Here you can also see the alert icons, which signify the results of a specific test for this workstation. The alert icons can appear in three different colors, according to the results of the test:

- If everything is in order, the alert icon will be green.
- If the test shows the workstation has reached the threshold value you have defined for a warning, however, the alert icon will be yellow, signifying a warning.
- In case one of the tests defined for the workstation indicates an error, the alert icon will be red.

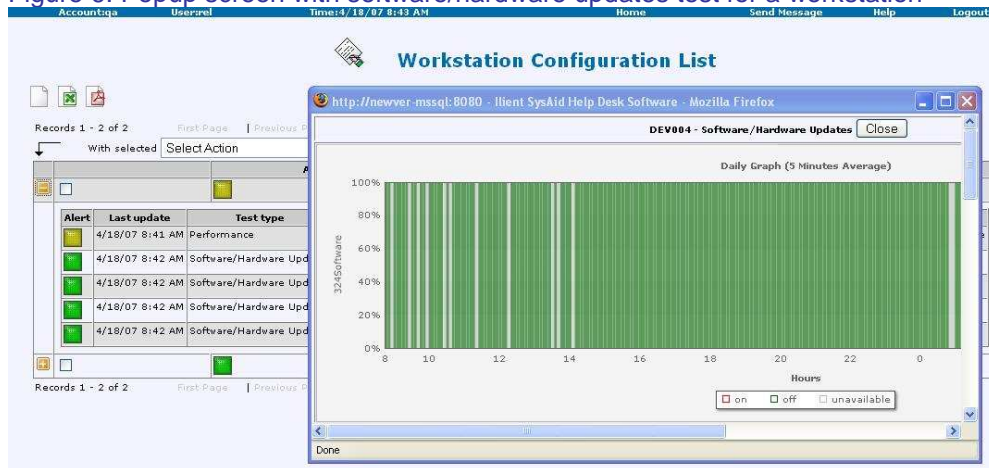
The color of the general alert icon for this workstation will be the color of the highest alert which exists for the collection of tests defined for this workstation. If all the monitoring tests are in order, their color will be green, and so will be the color of the workstation, as you can see in figure 5 above. However, if one of the tests is yellow, the whole workstation will be colored yellow too, and if a test shows an error and turns red, the whole asset will be marked by a red alert icon as well.



*When an alert icon flickers, this means there is no data available from the agent on this asset, for a period which exceeds the time limit you have previously defined.

From the **Workstation Configuration List** page you can also reach the graphs that show an average of the tests for each of the workstations. Simply click the entry of a certain test for a certain workstation, and a popup screen with the related graphs will open.

Figure 6: Popup screen with software/hardware updates test for a workstation



The graphs you can see in the popup screen show the daily, weekly, monthly and yearly averages for the particular test performed on the particular workstation.

For instance, in figure 6 above you can see the popup screen with a daily graph for a software test made on one of the workstation in our network. Since the unwanted software was not installed on this workstation during the day represented by the graph, the color of the graph is mainly green. Correct results for the tests will be marked green. A failure in the tests will be marked red, and no data due to a disconnection from the network will be marked grey in the graph.

Note that the time is calculated as an average, which is different for each of the four graphs: the daily graph is displayed with a five minutes average; the weekly graph with 30 minutes average; the monthly graph with two hours average; and finally the yearly graph is displayed with an average time of a whole day.

The differences between applying the monitoring tool to servers and to workstations:



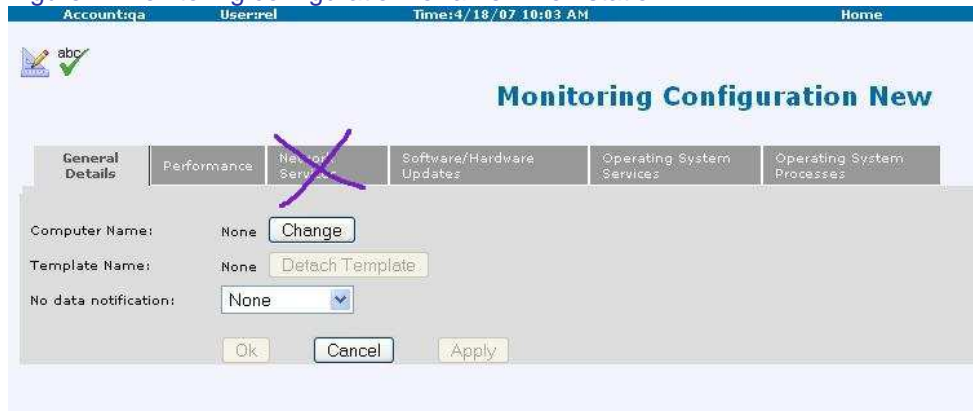
- While the monitoring of servers can be configured to include the network services tests for ping, http/https or generic TCP/IP, the monitoring of workstations cannot include these network services.
- In SysAid you can add an unlimited number of Operating System processes and Operating System services to your servers. To your workstations, however, you can only add up to two OS processes and two OS services at the most.

New Monitoring Configuration for a Workstation


Most of the monitoring definitions are identical for both servers and workstations. Therefore, this section is mostly a repetition of **New Monitoring Configuration for a Server**, which appears earlier in this guide.

Note, however, that workstations unlike the servers cannot be monitored for network services, and are limited to two OS processes and two OS services tests per workstation. See in figure 7 below the page for configuring new monitoring definitions for a workstation.

Figure 7: Monitoring configuration for a new workstation




In addition, the monitoring configurations available in SysAid are also identical when setting the monitoring tests templates for either servers or workstations. The only difference is that once you configure a monitoring test template you can then choose to apply the template to a group of servers, or to a group of workstations. To learn more about configuring monitoring templates for your assets, please see the **Templates** section later in this guide.

When you click the **New** icon:  in the **Workstation Configuration List**, you will reach a page called **Monitoring Configurations**, which contains five activated tabs. Note that the 'Network Services' tab is disabled for the workstation monitoring configuration.



⇒Workstations

Workstation Configuration List

⇒New  ⇒Monitoring Configurations New

The first tab is a **General Details** tab. Each of the next four tabs stands for a type of monitoring checks that can be preformed on the workstation you wish to configure new monitoring definitions for.

The different test types available in the SysAid Monitoring Module for workstations are:

- Performance: hard disk usage, Central Processing Unit usage, memory usage, memory in use\RAM ratio.
- Software/hardware updates
- Operating System Services (limited to two tests per workstation)
- Operating System Processes (limited to two tests per workstation)

Following is a specific explanation for each of the tabs, and the tests available under it.

General Details Tab

Under this tab you should fill in the general details for the workstation you wish to configure new monitoring definitions to.

1. Browse for the workstation from the list of assets by clicking the **Change** button.
2. If a template is already defined for this workstation, you will see the button **Detach Template** enabled, so the template could be detached. However, for a workstation that is still not connected to any monitoring template, this button will be disabled.
3. Finally, under this tab you can see the 'No Data Notification' dropdown menu. Choose from the menu a notification relevant for the case this computer is not sending any data for a pre-defined amount of time. The time limit before this notification is sent is set in the **Monitor Setting** page, which is elaborated on later in this guide.

Note that unless you have previously composed a suitable notification, this option will not appear in the 'No Data Notification' dropdown menu. The different monitoring notifications can be set in the **Notifications** page, and how set a new notification so is also explained in detail later.



Performance

Under this tab you can configure four different monitoring tests: hard disk (HD) usage, Central Processing Unit (CPU) usage, memory usage, and memory in use/RAM ratio.

All these tests are meant to make sure the workstation is not overusing its resources. An overuse may result in a breach in the performance of the computer, so all its actions will be slower than the optimal pace.

How to configure the performance monitoring tests?

1. Choose the test you wish to configure for this asset from the **Description** dropdown menu.
2. Fill in the values for the warning and the error thresholds.
The thresholds you are asked to choose refer to the highest value a certain test result can reach before a warning and before an error will be determined.

The values for the threshold fields are calculated in percentages. In case the test result exceeds the threshold value you have entered, a warning or an error will appear for the computer in question.

For example, if you choose the 'Memory in use' warning threshold to be 60%, when the workstation uses more than 60% of its memory, a warning will appear. To determine this threshold, simply type '60' in the 'Warning threshold' box.

Similarly, you can also decide that an error should appear when this workstation uses more than 80% of its memory. Simply insert '80' into the "Error Threshold" box.

3. In case of a warning or an error, a notification can be sent as well, according to your choice. If you wish to send warning and error notifications, select an appropriate notification from the 'Warning Notification' and the 'Error Notification' dropdown menus. Such appropriate notifications will be available in the dropdown menus only if you have previously composed them.

To learn how to compose monitoring notifications for different tests please consult the **Notifications** section in this guide.

4. Click **Add**.
5. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.



Here is an explanation about the meaning of each of the performance monitoring tests:

- Hard disk usage-This is a test that continuously checks the amount of space used in the hard disk of the workstation, to prevent a situation of flooding the hard disk. For instance, for a windows CPU it is generally recommended that at least one GB will remain free for an ideal performance of the computer.
- Central Processing Unit usage- The CPU should also not be overused, and the CPU test can verify this, according to your definitions.
- Memory usage- Here you can make sure the computer is not using more memory than it should. The memory usage test refers only to the physical memory which exists in the hardware of the computer.
- Memory in use/RAM ratio –This test checks how much is used of both the physical memory which exists in the hardware, and the virtual memory in the hard disk. Since the memory in the hard disk is not as efficient, it is recommended not to rely on it on a regular basis.

Software/Hardware Updates

Here you can check whether unwanted or dangerous software or hardware was installed on the computer in question.

Software and hardware updates tests for workstations can be useful in many cases. For instance, if you do not wish your users to illegally download music or video files with a file sharing software, or if you wish to forbid using USB keys on your network assets, in case your computers contain qualified information that should not be copied.

Now you can control the software and the hardware installed on all the machines in your network. Simply follow the instructions below:

1. Choose from the dropdown menu whether the test is for software or for hardware updates.
2. To identify the unwanted software or hardware, enter in the filter box a regular expression. For example, to keep your employees from installing file sharing programs on their workstations, look for the regular expression "kazaa" or "emule" in the software updates of the specific computer.
To find an appropriate regular expression that will identify the unwanted software, it is advisable to check the add/remove section in the control panel of the computer itself.
3. Once the filter is set, you can choose one of the notifications you have prepared for this case from the dropdown menu. An appropriate



notification should state that unwanted software or hardware was found on the workstation.

4. Click **Add**.

In case an unwanted software or hardware is installed on the workstation, your notification will be sent to the relevant administrator via an automatic service request, an SMS message, or an email, according to the way you have configured the notification. To learn how to compose the appropriate notification and how to configure to whom it will be sent and by what means, you should consult the **Notifications** section in this guide.

5. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

Operating System Services

Once you choose to add a computer from your network to the monitoring tool, the SysAid agent on this computer will begin to send constant updates from the computer. The result will be that a list of current OS services and processes for this computer will appear in the dropdown menu under **Service Name** or under **Process Name** in the **OS Services** or the **OS Processes** tabs for the computer in question.

The monitoring tests can be configured for both services and processes for each server or workstation on your network. The difference between processes and services is as follows: services are activated from the operating system, while processes are not necessarily activated from the OS, and can be also operated by the user. For example, Telnet, Tomcat and SysAid are services, while Java, Explorer, Skype and MSN Messenger are processes.

Under the **Operating System Services** tab you can check the services of the operating system for the particular workstation.

1. Choose the name of the service you wish to monitor from the dropdown menu called 'Service Name'. The list of the operating system services of this asset will appear in the dropdown menu under **Service Name**, if the SysAid agent is appropriately installed on the workstation.
2. In this dropdown menu you can also find the option: "All Auto Started Services". If you choose this option, the SysAid Monitoring tool will check whether the services that are supposed to go up in the startup of the computer run as they should.



3. Choose an appropriate error notification that will indicate that a certain OS service is not running as it should on this computer. To learn how to compose such a notification, please consult the **Notifications** section in this guide.
4. Click **Add**
5. Only once you have completed determining the entire monitoring configurations for this workstation in all the tabs click **OK** or **Apply** to save the configurations.

Please Note that workstations are limited to two OS Services tests.

Operating System Processes

Under this tab you can check whether the processes of the particular workstation are running appropriately. Processes are the .exe files on the computer. For instance, AVG antivirus is an OS process. The list of processes is sent to SysAid Monitoring tool from the task manager of the computer which is being monitored. It is advisable to click the **Refresh List** button occasionally, in case a new process was added to the computer.

1. Choose the name of the process you wish to monitor from the dropdown menu called 'Process Name'. The list of the operating system processes of this asset will appear in the dropdown menu under **Process Name**, if the SysAid agent is appropriately installed on the workstation.
2. Choose an appropriate error notification that will indicate that a certain OS process is not running as it should on this computer. To learn how to compose such a notification, please consult the **Notifications** section in this guide.
3. Click **Add**
4. Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations

Please Note that workstations are limited to two OS Processes tests.

Editing existing configurations for a workstation

Editing existing monitoring configurations for a workstation is done in the same page as when you define new configurations for a workstation. In figure 8 below you can see the page for editing existing monitoring configurations for one of the workstations in our network.



Figure 8: Editing existing monitoring configurations for a workstation



1. In the SysAid Monitoring Module go to:
⇒ Workstations
Workstation Configuration List
2. Choose from the list of workstations a workstation you wish to edit the monitoring configurations for.
3. See the explanations in the section **Monitoring Configurations for a New Workstation** above to learn about each of the available test types.
4. Modify the configurations that should be changed.
5. Only once you have completed modifying the entire monitoring configurations for the workstation in all the tabs click **OK** or **Apply** to save the changes.



Templates

Templates are collections of a few monitoring tests that can be applied at once to several assets in your network. There are two parallel list pages for monitoring tests templates: one for templates that can be applied to servers, and the other for templates that can be applied to workstations. Before you configure monitoring tests templates for your network assets these list pages will be empty. However, once you configure server or workstation templates, you will see a list similar to the one in figure 9 below:

Figure 9: Workstation Template List

Workstation Templates List

View: MonitorTemplate

Records 1 - 2 of 2 | First Page | Previous Page | Next Page | Last Page | Show All | [Toggle All](#) | [Expand All](#)

With selected Select Action

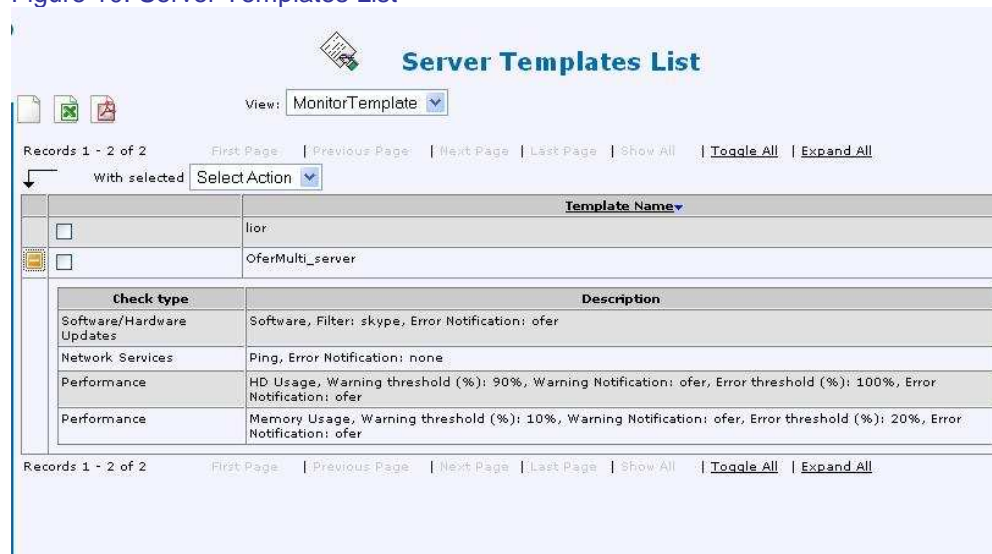
Template Name	
<input type="checkbox"/>	Israel
Check type	Description
Performance	CPU Usage, Warning threshold (%): 10%, Warning Notification: none, Error threshold (%): 20%, Error Notification: none
<input type="checkbox"/>	ofer workstation
Check type	Description
Software/Hardware Updates	Software, Filter: icq, Error Notification: ofer
Performance	CPU Usage, Warning threshold (%): 40%, Warning Notification: ofer, Error threshold (%): 80%, Error Notification: ofer
Performance	HD Usage, Warning threshold (%): 10%, Warning Notification: ofer, Error threshold (%): 30%, Error Notification: ofer


Records 1 - 2 of 2 | First Page | Previous Page | Next Page | Last Page | Show All | [Toggle All](#) | [Expand All](#)




A parallel page is the Server Template List you can see in figure 10 below:

Figure 10: Server Templates List



Click the plus icons  to see a list of the different tests that each of your templates includes.

To edit an existing template, click the entry of the template. You will reach the **Workstation Monitoring Template** or the **Server Monitoring Template** page of the asset you have chosen. Here you can follow the same instructions as for adding a new template, which are specified below.


To configure a new template, click the **New**  icon in the **Server** or the **Workstation Template Lists**.

From the SysAid left menu bar go to:

Monitoring

⇒ Server Templates

Server Templates List

⇒ New  ⇒ Server Monitoring Template New

Or:

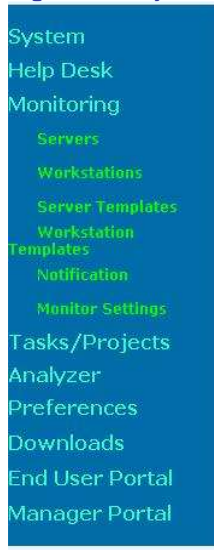
⇒ Workstation Templates

Workstation Templates List

⇒ New  ⇒ Workstation Monitoring Template New



Figure 11: SysAid left menu bar



Configuring a new template

Configuring a new server or workstation template is basically the same as configuring new monitoring tests for individual servers or workstations, only the collection of tests you define as a template can be then attached to any number of servers or workstations on your network.

In the **Server Monitoring Template New** page you will see six tabs. Under the first tab you can define the general details of the new server template you wish to configure. The other five tabs include the different monitoring test types available for servers.

In the **Workstation Monitoring Template New** page, however, only five tabs are enabled. This is since the tests for network services are unavailable for workstations.

In the **General Details** tab:

1. Insert the new template name. Notice that the buttons **Select Assets** and **Remove Assets** are only enabled once you have entered a name for the new template, and clicked the **OK** or the **Apply** button.
2. Click the **Select Assets** button to choose the servers/workstations your new template will be applied to. A popup screen with a list of your assets will open.
3. Check the boxes next to the assets you wish to apply the new template to.
4. From the **Action** dropdown menu located at the top of your asset list, choose "Add Assets". See figure 12 below.



- Please beware when you choose to add an asset to your new template! Adding an asset will remove all previous monitoring definitions for the selected asset. You will not be able to restore the previous monitoring definitions! For more information, please read the **Warnings** section below.

Figure 12: Select Asset Popup Screen



- If you are editing an already existing template, click the **Remove Assets** button to choose the servers/workstations you wish to detach the template from. A popup screen with a list of your assets will open.
- Check the boxes next to the assets you wish to detach the template from.
- From the **Action** dropdown menu located at the top of your asset list, choose "Add Assets". See figure 12 above.
- Please beware when you choose to detach an asset from a template. Removing an asset will cancel the connection of this asset with the template, and any updates in the template will not be applied to this asset. For more information, please read the **Warnings** section below.
- From the dropdown menu, choose a notification that will be sent in case the agents on the assets are not sending any data. To learn how to create and edit such a notification, please consult the **Notifications** section in this guide.
- Only once you have completed determining the entire monitoring configurations for this asset in all the tabs click **OK** or **Apply** to save the configurations.

To configure your new server or workstation template according the following tabs: Performance, network Services (available only for servers), SW/HW



Updates, OS Services, and OS Processes, please follow the instructions specified earlier in this guide in the section:

- **New Monitoring Configuration for a Server**

Or in the section:

- **New Monitoring Configuration for a Workstation**

The only difference is you are now configuring these tests for a group of servers or for a group of workstations, instead of configuring these tests for each asset individually.

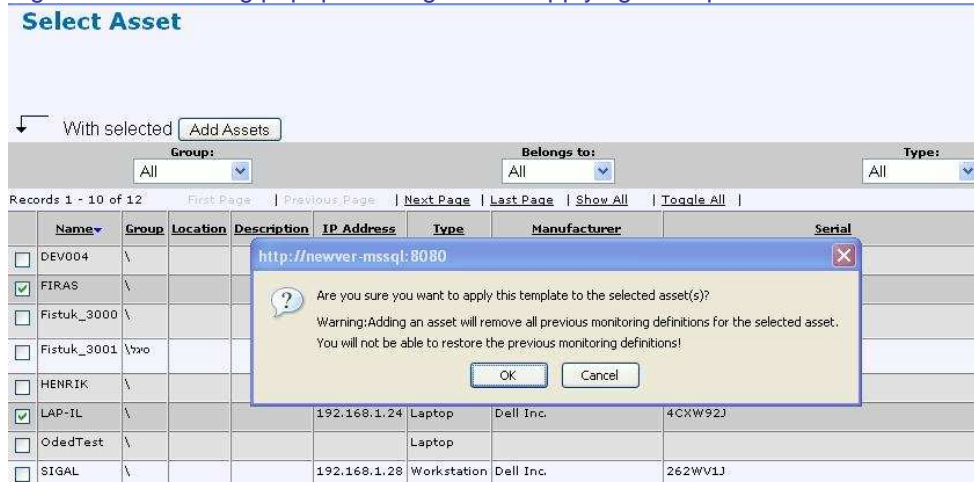
Warnings:

What you should know before you apply a template to an asset!

- It is crucial to realize before applying a template to an asset that monitoring configurations can be only either individually set for each asset or set in a template. A template and other monitoring configurations cannot co-exist on any computer. Therefore, if you apply a template to a certain asset, you in fact delete all the previous monitoring configurations that were determined for this asset!

Please do not add an asset to any template before making sure there are no previous monitoring definitions for this asset.

Figure 13: A warning popup message about applying a template to assets



- When you configure a monitoring template to apply to several assets in your network, be careful to choose OS services and processes that are general and exist in all the assets you choose to apply the template to. Otherwise, the result will be a constant error notification sent from those



assets which do not include that particular OS service/process defined in your template.

For example: suppose you define in your template the monitoring of a particular OS process, such as Internet Explorer. Then you apply this template to 100 workstations on your network. Yet, 40 of the users in these workstations do not use Internet Explorer at all, but prefer to use another browser instead. This may result in a constant error message regarding Internet Explorer from these 40 computers.

- If you wish most of your network assets to go through the same monitoring tests, yet for one (or more) specific asset you wish to add another special test (or more), it is possible.

For example, assume you have 300 workstations in your organization, and you wish to monitor them all for Memory Usage. Yet, there are 50 workstations that you also wish to check in particular, since they include classified information, and you do not want any of the users to copy information into portable storage devices.

Create a workstation template that will include the Memory Usage test, and apply it to all of your 300 workstations.

Then, detach the template from the 50 workstations that contain the classified information. The settings of the template will be saved for these workstations.

Now you will be able to add a Hardware Update test for these particular assets, and be notified whenever a portable storage device is installed on any of these 50 workstations.

Yet, note that if you update the template, future changes in the template will not be updated for the detached assets.

For instance, if you choose to replace the Memory Usage test defined in the template with the Memory in use/RAM ratio test, the change will be updated only for the 250 workstations which are still connected to the template. The 50 workstations for which you have defined the extra test will continue to be monitored for Memory Usage rather than for Memory in use/RAM ratio, since they have already been detached from the template.

Notifications

From the SysAid left menu bar you can reach the **Monitor Notification** page (See Figure 14 below).

Figure 14: SysAid Monitor Notification List




Here you can create the notifications that can then be attached to different warnings and errors in the monitoring tests of your network assets. You can also configure here the way in which these notifications will be sent, and to whom.

Note however that for the notifications to be actually sent, after creating them you should add the relevant notification for each of the possible events. Adding the notifications you will create here, is done while configuring monitoring preferences for servers or workstations.

To learn how to attach an existing notification to the appropriate case, please see the previous sections in this guide:

- **New Monitoring Configuration for a Server**
- **New Monitoring Configuration for a Workstation**

Sending Options for a notification

When you click the New  icon, or, in case you already have existing notifications that you wish to edit, when you click one of the entries in the **Monitor Notification** list, you will reach the **Monitor Notification** editing page. This editing page includes four tabs:

General
Send Email
Send SMS
Service Request Details

Following is a detailed explanation for each tab in the **Monitor Notification** editing page.



General

1. Go to the **General** tab and insert a name for the new notification (See Figure 15 below).

Figure 15: Monitor Notification New-General

The screenshot shows a dialog box titled "Monitor Notification New" with a tabbed interface. The "General" tab is selected. It features a "Name:" label and an empty text input field. Below the input field are three checked checkboxes: "Send SMS", "Send Mail", and "Insert a Service Request". At the bottom of the dialog are three buttons: "Ok", "Cancel", and "Apply".

2. Check the relevant boxes to choose the ways for sending your new notification. You may choose one, any two or all three options. The available options are SMS message, email message and you may also order SysAid to automatically open a service request regarding the warning or the error that occurred.

Choose the sending options according to the urgency of the particular warning or error that should be addressed. For a very urgent error, such as a disconnected server, you may want to send both SMS and email to the responsible administrator, while for a less crucial event you may choose to send only an email, or open an automatic service request that will be queued with all other service requests arriving at your helpdesk.

3. Only once you have finished configuring the notification, should you click the **OK** or the **Apply** button to save the changes.

Mail Details

1. Go to the **Mail Details** tab (see Figure 16 below)



Figure 16: Monitor Notification- Mail Details.

2. Click 'Browse' to choose the names of the mail recipients in your list of administrators.
3. A popup screen with a list of your network administrators will open. Check the boxes next to the names of the administrators you wish to send the monitoring notification email to, and click the 'Select' button at the bottom of the list to save your choices.
4. Insert the subject of the mail notification. See the next section in this guide: **Composing Notifications** to learn how to compose the subject for your notification.
5. Insert the body of the mail notification. See the next section in this guide: **Composing Notifications** to learn how to compose your notification.
6. Only once you have finished configuring the notification, should you click the **OK** or the **Apply** button to save the changes.

SMS Details

1. Go to the **SMS Details** tab (see Figure 17 below).

Figure 17: Monitor Notification- SMS Details.



2. Click 'Browse' to choose the names of the SMS recipients in your list of administrators.
3. A popup screen with a list of your network administrators will open. Check the boxes next to the names of the administrators you wish to send the monitoring notification SMS to, and click the 'Select' button at the bottom of the list to save your choices.
4. Insert the body of the SMS message. See the next section in this guide: **Composing Notifications** to learn how to compose your notification.
5. Only once you have finished configuring the notification, should you click the **OK** or the **Apply** button to save the changes.

Service Request Details

1. Go to the **Service Request Details** tab (see Figure 18 below).

Figure 18: Monitor Notification- SR Details.

The screenshot shows a web application window titled "Monitor Notification asaf". It has four tabs: "General", "Mail Details", "SMS Details", and "Service Request Details". The "Service Request Details" tab is selected. The form contains the following fields:

- Title:** The asset \$asset.computerName has failed in the test
- Category:** Please select a category. (dropdown), Please select a sub-category. (dropdown), Select Third Level Category (dropdown)
- Status:** New (dropdown)
- Urgency:** Please select an urgency. (dropdown)
- Priority:** Please select a priority. (dropdown)
- Description:** \$alertType: The asset \$asset.computerName has failed the \$testName test in the \$testType field .\nPlease address the matter in the near future.
- Notes:** (empty text area)
- Solution:** (empty text area)

At the bottom of the form are three buttons: "Ok", "Cancel", and "Apply".

2. Insert the title for the service request. See the next section in this guide: **Composing Notifications** to learn how to compose the title for your notification.



3. Choose a category, sub-category and a third level category for the request SysAid will open automatically.

For example, the category can be "Monitoring Error Notification", the sub-category can be "Workstation Monitoring" and the third-level category can be "Unwanted Hardware found". Such a service request could be opened automatically once unwanted hardware will be found on one of your workstations.

Note, however, that you should also configure the monitoring tests themselves and attach this notification to the workstation test definitions, for the service request to be actually opened.

To learn how to configure monitoring tests for your network assets, please see the detailed explanations provided earlier in this guide in the sections: **Monitoring Configurations for a Server / Monitoring Configurations for a Workstation**.

4. From the dropdown menu, choose an appropriate urgency for the service request.
5. From the dropdown menu, choose an appropriate priority for the service request.
6. You may add a description to the service request that will specify the details of the failure of the asset in the monitoring test. To learn how to compose this description, please see the next section in this guide: **Composing Notifications**.
7. Only once you have finished configuring the notification, should you click the **OK** or the **Apply** button to save the changes.

Composing Notifications

How to compose your monitoring notifications?

It is recommended to use tags when composing your different monitoring warning and error notifications. The advantage of the use of tags is that they can vary according to the different circumstances to suit each individual notification.

The available tags in SysAid for monitoring warning and error notifications are:

[\$asset.computerName]- The name of the asset that has failed the monitoring test.

[\$testName]- The name of the monitoring test the asset has failed in (for instance, a Ping test for a certain server).



[\$testType] – The name of the test type, for instance, a Ping monitoring test is of 'Network services' type.

[\$alertType] -This tag can accept two values: either the alert is a warning notification, or an error notification. Note that the vales here can be either "Error" or "Warning".

[\$alertSentence]- This tag can accept two values: either the alert is a warning notification, or an error notification. Note that the values here can be either "an error" or "a warning".

You can find these tags in **Preferences**⇒**Customize**⇒**Translate** list. See Figure 19 below:

Figure 19: Tags for monitoring notifications in the **Translate** page

monitor.warning	Warning
monitor.warning.sentence	a warning
monitor.notification.email.subject	<code>\$alertType</code> notice regarding the asset <code>\$asset.computerName</code> : failure in a <code>\$testName</code> test
monitor.notification.email.body	This is <code>\$alertSentence</code> notification. \nThe asset <code>\$asset.computerName</code> has failed the <code>\$testName</code> test in the <code>\$testType</code> field. \nPlease address the matter in the near future.
monitor.notification.sr.title	The asset <code>\$asset.computerName</code> has failed in the test <code>\$testName</code>
monitor.notification.sr.description	<code>\$alertType</code> : The asset <code>\$asset.computerName</code> has failed the <code>\$testName</code> test in the <code>\$testType</code> field . \nPlease address the matter in the near future.
monitor.notification.sms.text	<code>\$alertType</code> : asset <code>\$asset.computerName</code> , failure in a <code>\$testName</code> test



Monitor Settings

Determining the Monitoring Timeout Settings

From the SysAid left menu bar, follow the link Monitoring⇒Monitor Settings. You will reach the page **Monitor Settings**. (See Figure 20 below)

Figure 20: SysAid Monitor Settings Page

The screenshot shows the 'Monitor Settings' page in SysAid. It features a light blue background and a title 'Monitor Settings' in the top right corner. There are four configuration rows, each with a label on the left and a control on the right. The first three rows have dropdown menus, and the fourth has a text input field. At the bottom, there are two buttons: 'Save' and 'Return to Default'.

Here you can set up the timeout limit for the network services tests of your servers: the ping, TCP/IP and the http/https test. Setting up the timeout limit for the network services tests will determine an error when the server has failed these tests for the period of time you will specify here.

1. Go to **Monitoring**⇒**Monitor Settings** and choose from the dropdown menus the time limit for a warning to be sent for each different network services test on all your network servers.

The Ping test simply verifies that the connection of your servers to the network is in order. The TCP/IP test verifies the availability of a certain port on the servers, while the Http/https test makes sure that a certain vital web application is available on your servers.

2. Click **Save** to save your preferences.
3. Alternatively, you may go back to the default time limits defined for these tests, which are 20 seconds for each network services test, before an error is generated.

Determining other qualities of the network services tests should be performed either individually for each server, or in a server template. You can choose which notifications will be sent for each test, which port to check for each server, and which web applications are the most vital for your servers, and how to identify them.



To learn how to do so, please return to the section **New Monitoring Configuration for a server** in this guide, and consult specifically the instructions under the **Network Services** tab.

In addition, you should create the notification for a server which failed one of the available tests. You may want to send a warning notification via SMS message, automatic service request or an email, or any combination of these notification options. To learn how to create such notifications, please return to the previous section which elaborates about **Notifications**.

Checking the connection of the agent to the network

For each asset on your network, the SysAid Monitoring module allows you to be notified in case no data is sent from the agent during a pre-set amount of time. This may be useful for several purposes: to be able to know whether the agent for this computer is in order, to find out whether the asset itself is functioning properly and whether it is still connected to your network.

For instance, this monitoring feature can be very useful since it allows you to be notified immediately in case some of your assets were damaged or even stolen.

How to set the warning about a disconnected asset?

1. In the **Monitor Settings** page, Insert a number that signifies the maximum amount of time before a notification that the agent on an asset is unavailable will be generated.
2. Your definition for the 'Maximum time with no data from the agent' will be applied to all of your network assets, workstations as well as servers.
3. Note that the minimum time that can be defined here is an hour.
4. Click **Save**.

You should consider carefully your choice for the 'Maximum time with no data from the agent' field, since in some cases a warning or an error which appears after only a few hours for a workstation may cause confusion and increase your workload unnecessarily.




For instance, if the employees in your organization turn their computers off when they go on a holiday, there is no reason for a warning to appear after only a few hours. In this case, you may set the alert for a disconnected agent to appear for an asset only after a week.



In addition, you may create the notification that will be sent when a computer is no longer available on your network. You may want to send a warning notification via SMS message, automatic service request or an email, or any combination of these notification sending options. To learn how to create the relevant notification, go to the **Notifications** section in this guide.

A notification is not mandatory, though. If you choose not to send any notification when an agent on an asset is unavailable, you may choose to limit the alerts to the **Server Configuration List** or the **Workstation Configuration List** pages only. This means you should be responsible for checking the alerts for unavailability of different agents in your network on these pages yourself. In this case you will see the alert icons in different colors next to each asset flickering.

Note that a flickering alert icon always means the agent on this asset is not available for the period you have defined, regardless of the color of the icon.

The different colors signify only the results of the monitoring tests made on each asset. If the icon is green: , all the tests are in order. If the icon is yellow: , one or more monitoring test has reached the warning level. In case the alert icon is red: , this asset has failed one or more monitoring tests.

However, when an alert icon *flickers*, this means there is no data available from the agent on this asset, for a period which exceeds the time limit you have previously defined.



Monitoring Map

Left side bar menu ⇒ Monitoring

⇒ Servers

Server Configuration List

⇒ New  ⇒ Monitoring Configurations

Tabs:

General Details

Computer Name

Template Name

No Data Notification

Performance

HD Usage

CPU Usage

Memory Usage

Memory in use/RAM ratio

Network Services

Generic TCP/IP

Ping

Http

Software/Hardware Updates

Update Type

Filter

Error Notification

Operating System Services

All auto started services

Error notification

Operating System Processes

Error notification

Action

Refresh List button

⇒ Workstations

Workstation Configuration List

⇒ New  ⇒ Monitoring Configurations New

Tabs:

General Details

Computer Name

Template Name

No Data Notification

Performance

HD Usage

CPU Usage

Memory Usage

Memory in use/RAM ratio

Software/Hardware Updates

Update Type

Filter

Error Notification

Operating System Services

All auto started services

Error notification

- 39 -

Monitoring Guide

Ilient Ltd., 6 Hamasger St. P.O.BOX 1010, Or-Yehuda, 60223, ISRAEL

Email: info@ilient.com www.ilient.com



Operating System Processes
Error notification
Action
Refresh List button

⇒Server Templates

Server Templates List

⇒ New  ⇒Server Monitoring Template New

Tabs:

General Details

Template Name
Add/Remove Assets
No Data Notification

Performance

HD Usage
CPU Usage
Memory Usage
Memory in use/RAM ratio

Network Services

Generic TCP/IP
Ping
Http

Software/Hardware Updates

Update Type
Filter
Error Notification

Operating System Services

All auto started services
Error notification

Operating System Processes

Error notification
Action
Refresh List button

⇒Workstation Templates

Workstation templates List

⇒ New  ⇒ Workstation Monitoring Template New

Tabs:

General Details

Template Name
Add/Remove Assets
No Data Notification

Performance

HD Usage
CPU Usage
Memory Usage
Memory in use/RAM ratio

Software/Hardware Updates

Update Type
Filter
Error Notification

Operating System Services

All auto started services
Error notification

Operating System Processes

- 40 -

Monitoring Guide



Error notification
Action
Refresh List button

⇒Notifications

⇒ New  ⇒ Monitor Notification New

Tabs:

General

Mail Details

SMS Details

Service Request details

⇒Monitor Settings

Ping Time out

TCP/IP connection time out:

HTTP connection time out:

Minimum Time for unavailable agent notification (in hours)