MKS AlertCentre Evaluation Guide

MKS Software, Inc.
12450 Fair Lakes Circle, Suite 400
Fairfax VA 22033 USA
Sales: 1-800-637-8034
+1-703-803-3343
http://www.mkssoftware.com

November 2002

Contents

Evaluating the MKS AlertCentre

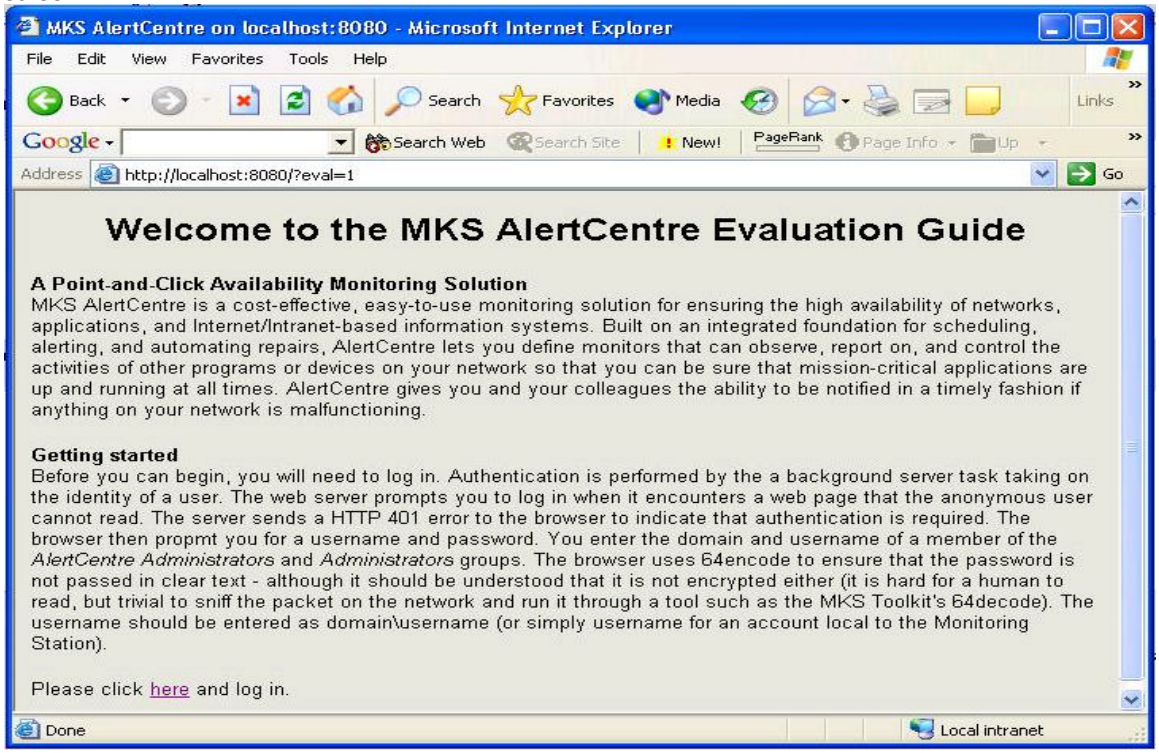
A Web-based Availability Monitoring Solution

MKS AlertCentre™ is a cost-effective, easy-to-use monitoring solution for ensuring the high availability of networks, applications, and Internet/Intranet-based information systems. Built on an integrated foundation for scheduling, alerting, and automating repairs, AlertCentre lets you define monitors that can observe, report on, and control the activities of other programs or devices on your network so that you can be sure that mission-critical applications are up and running at all times. AlertCentre gives you and your colleagues the ability to be notified in a timely fashion if anything on your network is malfunctioning. Automated Monitoring, Alerting and Corrective Actions give you:

- **Higher Availability of Business-Critical Systems –** allows you to maximize revenue and profit and maintain a solid corporate reputation for reliability and service.
- **Better Performance –** allows you to serve more customers
- **Improved Worker Productivity –** results when employees can connect without delay to e-mail and other critical services at any hour and from any location.
- **Management-by-Exception –** enables systems administrators to focus on their day-to-day duties with the peace-of-mind that AlertCentre will notify them of problems whenever and wherever they are.

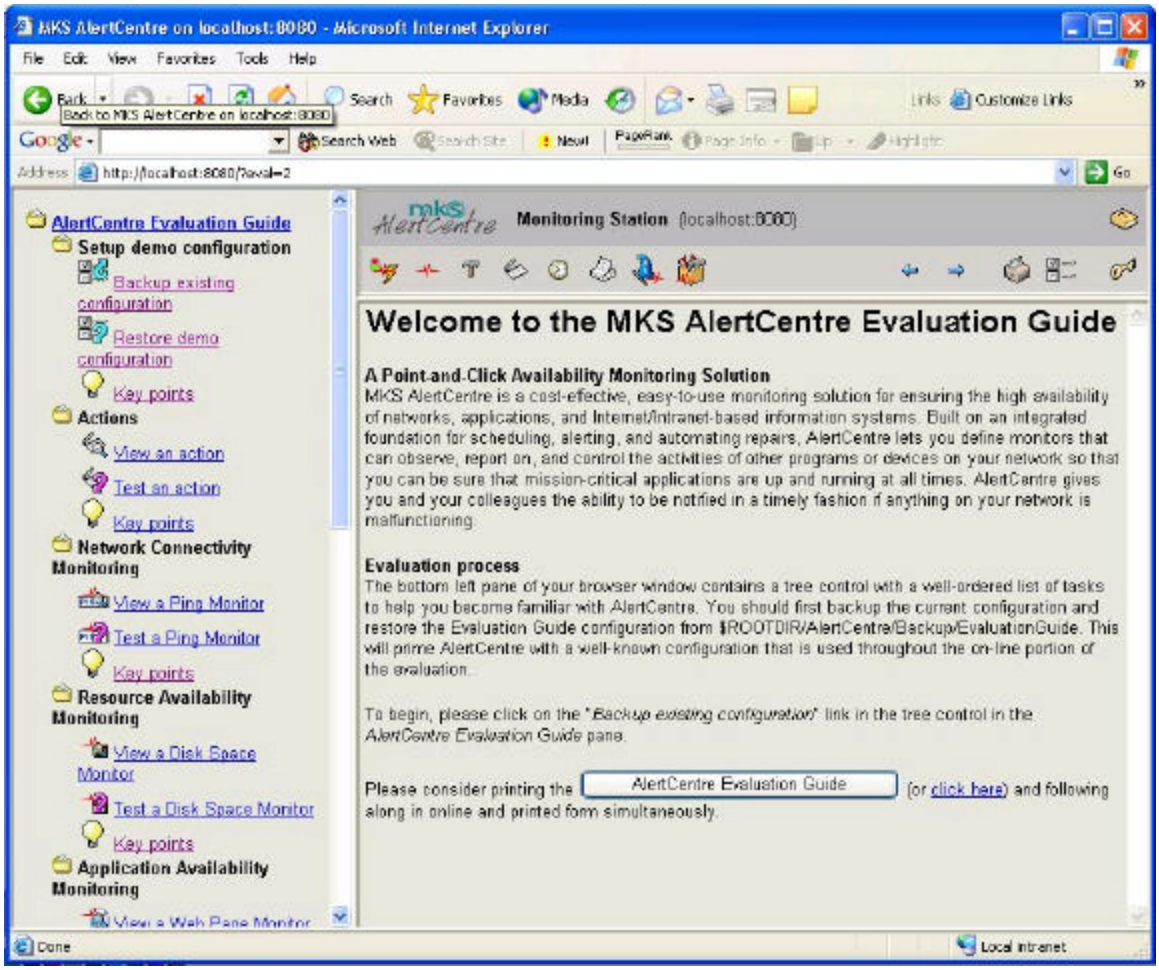
Setting Up The Evaluation Environment

To begin the AlertCentre Evaluation, please launch from the Windows Start Menu: Start →Programs→MKS AlertCentre→Evaluation Guide→AlertCentre Evaluation. You will see this screen:



Then it will be time to log in, and begin the evaluation. In order to log in, you need to know the username and password of a local or (preferably) domain administrator and enter them as shown below.

This will start AlertCentre in evaluation mode and you will see a three-pane browser window as shown on the next page.



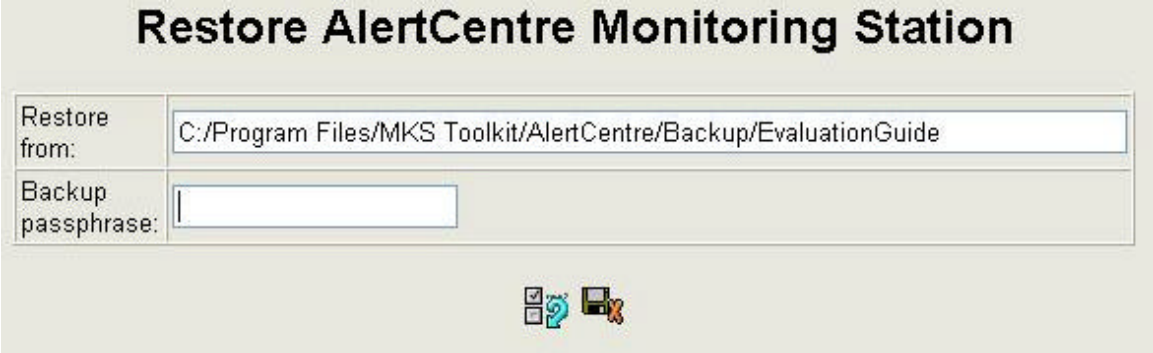
The top/left pane is the same as would be seen in AlertCentre in standard mode. The bottom/left pane is a navigation window added to guide you through this evaluation. Please start by reading the text in the right pane, and then it will be time to click a link in the bottom/left pane.

If you have already started to use AlertCentre and have created Monitors or Actions you wish to save, you should first backup your current configuration by clicking on the link *Backup existing configuration;* otherwise please skip forward to *Restoring demo configuration*. AlertCentre ships with two sample configurations: one totally empty; the other for use in this evaluation. They reside in $ROOTDIR/AlertCentre/Backup.

Backing up the existing configuration

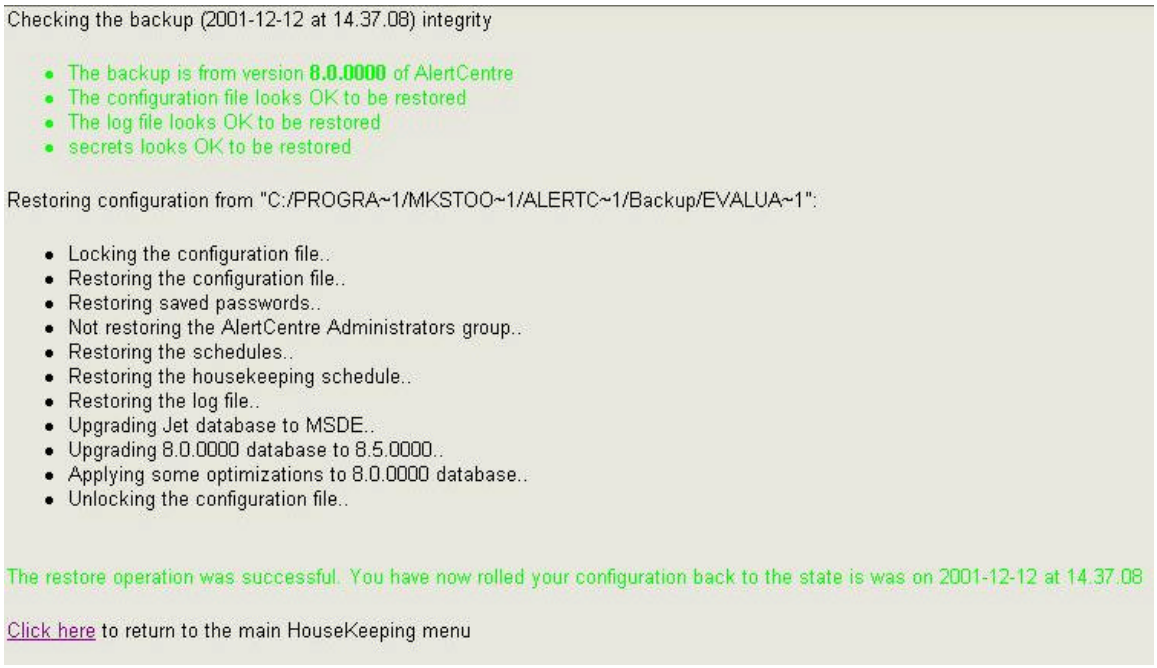
Enter a Backup passphrase that you can remember to restore your current state at the end of the evaluation and press the "Backup" button. You should see the details of the backup in the right pane including the statement: The backup was successful.

Restoring the demo configuration



Enter the Backup passphrase "ACEval" and click the restore button. You will be prompted to overwrite the current configuration with this backup. Be sure that if you have an important configuration on the Monitoring Station that you have first backed it up and then click the Restore button to restore the demo configuration.

Restoration should look something like:



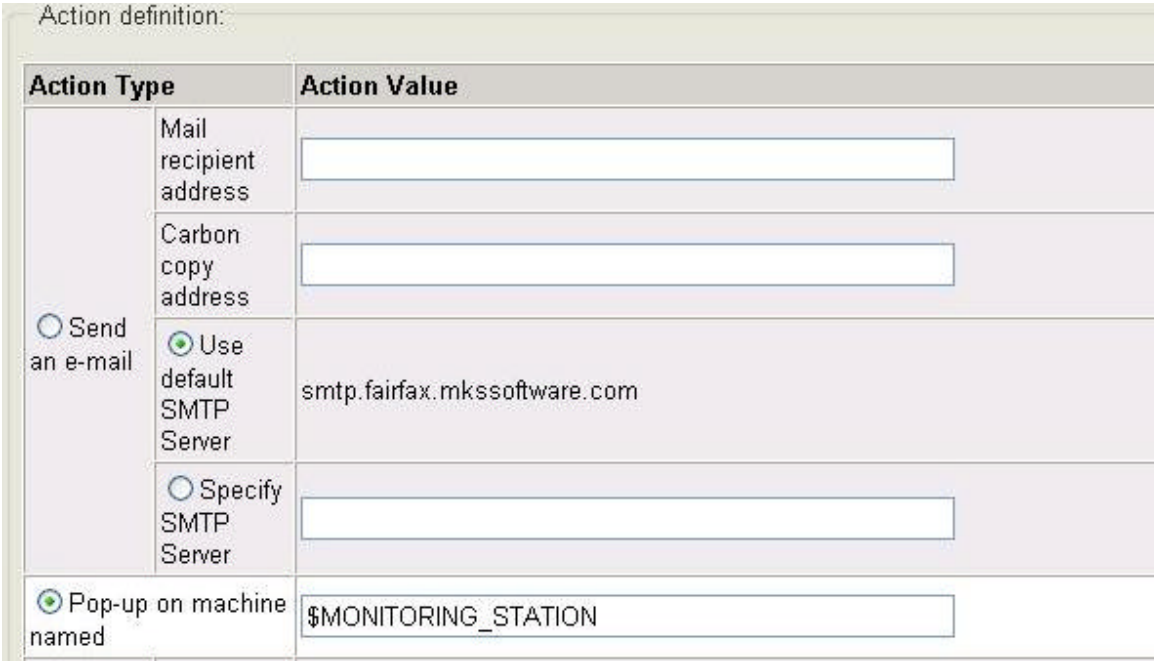
KEY POINTS

Monitoring Station Configurations

1. Are only accessible to authorized users
2. Can be backed up and restored to protect valuable data
3. It's important to backup before restoring the Evaluation Guide configuration

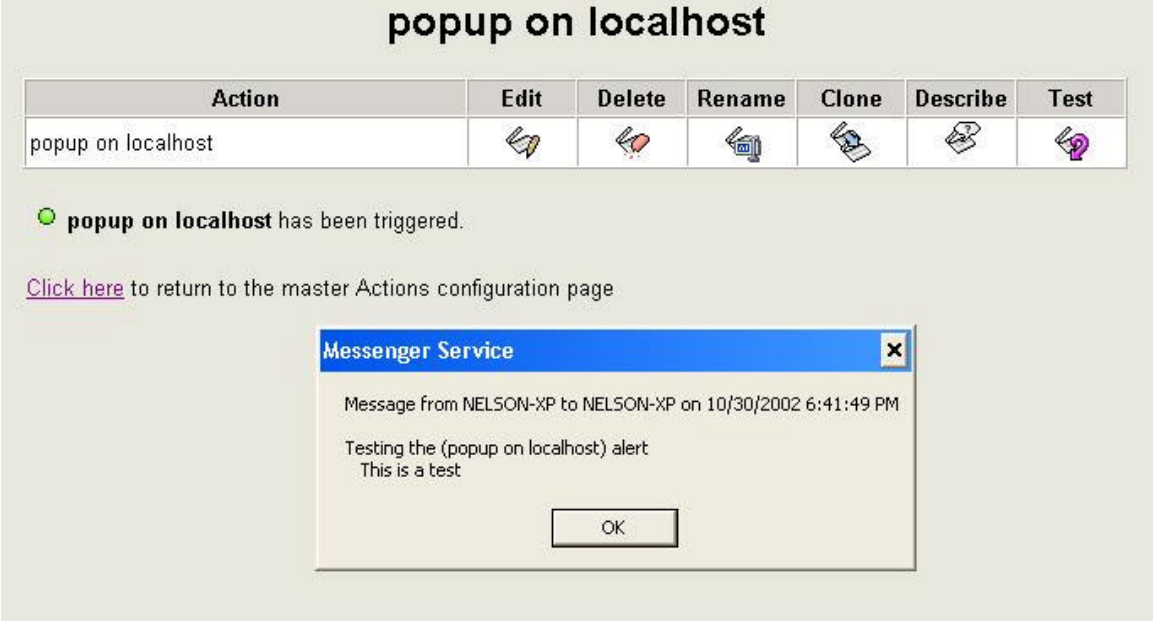
Actions

Click on the *View an Action* link in the *AlertCentre Evaluation Guide* frame to see the Edit Action page for an Action named: **popup on localhost.** In AlertCentre, an Action is used to alert specific people about the status reported by a Monitor. Alerts can be delivered using a variety of media (e.g., email, page, popup, SNMP Trap, etc.). Actions can also be used to automate corrective actions (e.g., reboot a machine, run a program, etc.) This particular Action pops up a dialog box on the Monitoring Station. Scroll the right pane to see the range of Actions that can be used.



Now click the *Test an Action* link in the *AlertCentre Evaluation Guide* frame. After reading about Actions in the right pane, press *Click here* to test the Popup on localhost Action.

AlertCentre will display a Test complete message in the right pane like below, and you will see a popup dialog on the console of your AlertCentre Monitoring Station which looks something like this.



Of course the Windows Messenger Service must be started on the Monitoring Station for this dialog box to work. If it is not started, you can start it through the services interface or from the command line using *service start messenger*.

KEY POINTS

AlertCentre Actions

1. Alert key people via: e-mail, popup dialogs, paging, SNMP Traps and much more.
2. Automate corrective actions by rebooting machines, running programs or scripts and more.
3. Actions are key to **Management by Exception**. System managers and administrators do not need to monitor consoles all day, because Actions will alert them of problems when they occur, thus their time is freed up for other pressing needs.

Monitors

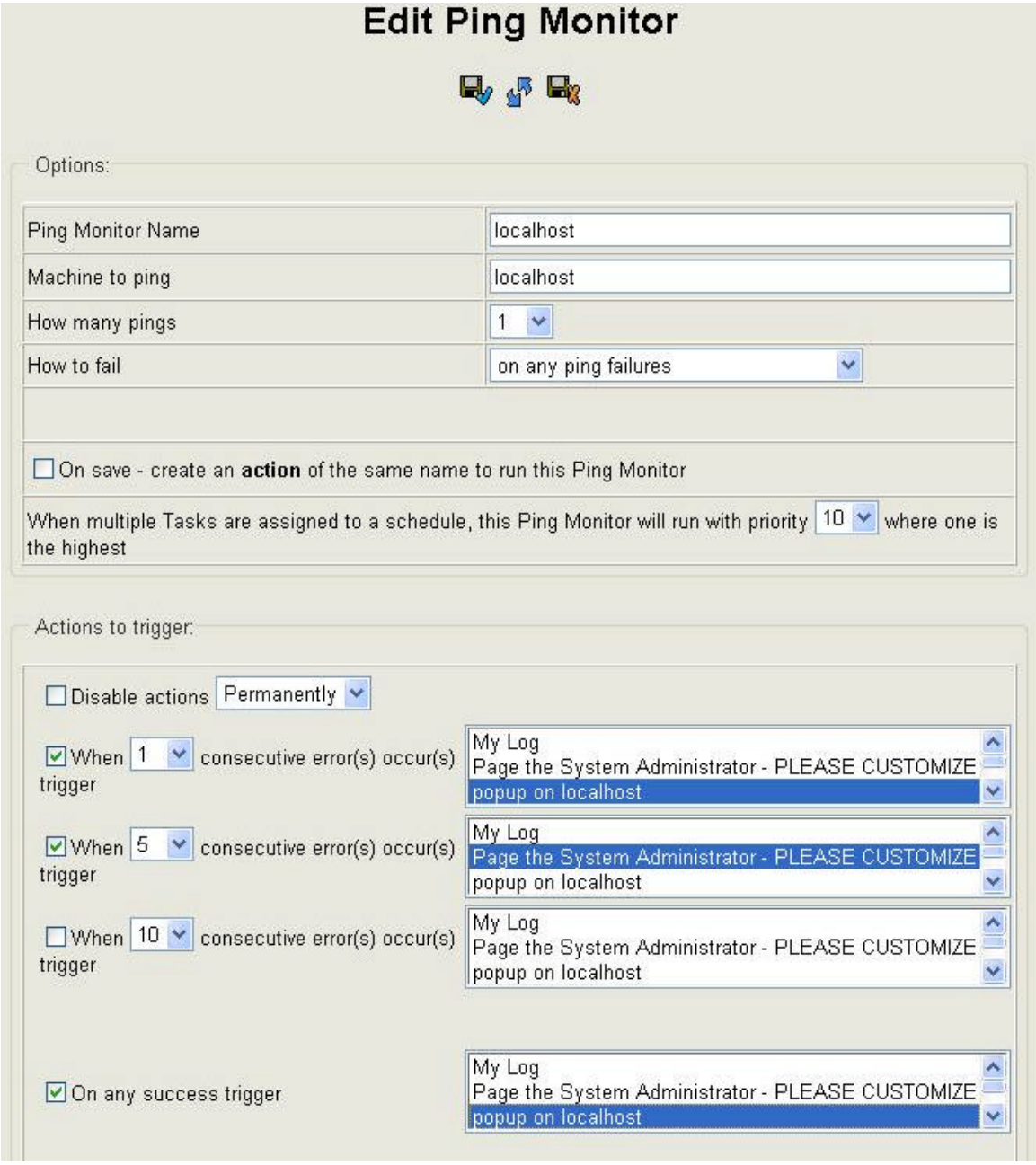
A monitor is a task that runs on a monitoring station and is responsible for monitoring the health of a physical or virtual IT resource such as a port, a URL, a disk drive or an application. The key elements of a monitor are an IT resource to be monitored (e.g., server, workstation, URL, disk, etc), a metric for evaluating the condition of that resource, a schedule on which to monitor that item, and actions to be taken based on the success or failure reported by the monitor.

AlertCentre predefines many kinds of monitors in three main categories: Network Connectivity, Resource Availability and Application Availability. You create a new instance of one of these monitors and customize it by specifying various parameters via

the AlertCentre Graphical User Interface. In the case of a predefined monitor, the task is predefined, such as a monitor for an HTTP server. You may also create your own new kinds of monitors called custom monitors to do whatever you like.

Network Connectivity Monitoring

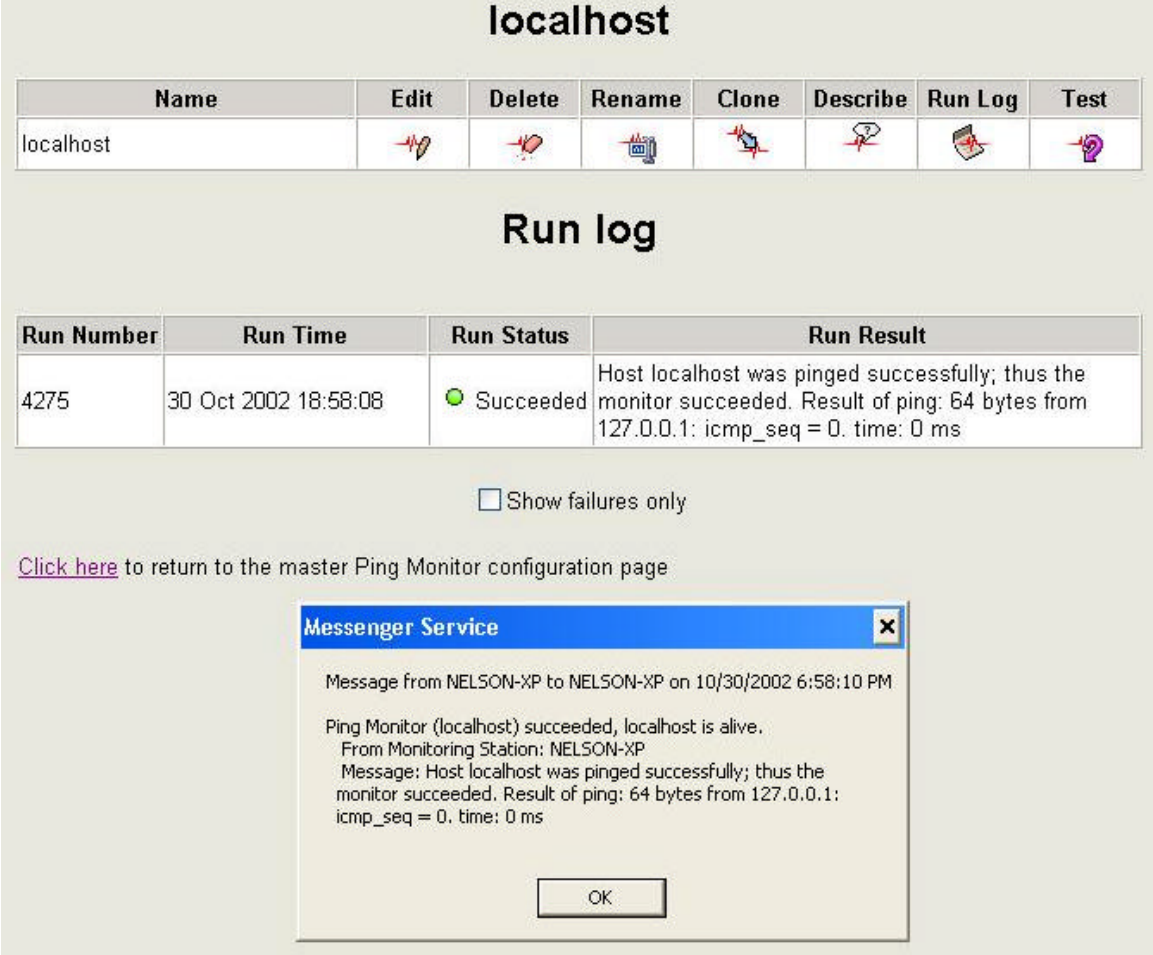
A Ping Monitor is one example of the many monitor types that are ready to be used for Network Connectivity Monitoring. Click on the *View a Ping Monitor* link and you will see the following screen:



Note that the monitor will ping the Monitoring Station (i.e., localhost) and on the first success and the first failure it will popup a dialog on the Monitoring Station console. Every monitor defines what actions will be taken upon success or failure and the escalation rules for those actions. Note also that it is possible to temporarily disable the

actions for a monitor – for example during routine maintenance. Also, note that there are currently no schedules designated to trigger the localhost ping monitor.

Now click *Test Ping Monitor* to see the monitor in action. For either success or failure you should expect to see a popup dialog indicating the state of the monitor. You will also see the monitor run log for this monitor so that you have a history of the state of this monitor at discrete intervals over time.



KEY POINTS

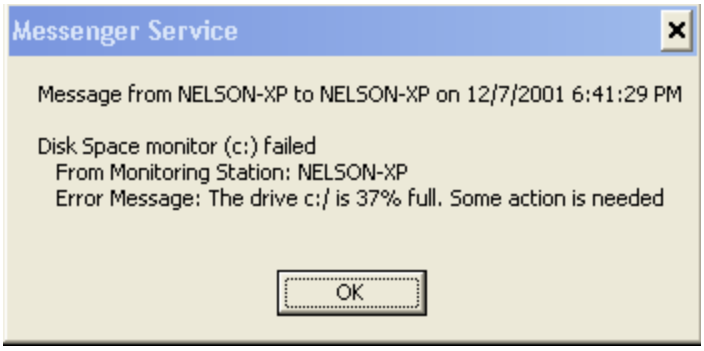
Network Connectivity Monitoring

1. Can be used to test connectivity across a broad array of computers, operating systems and devices that support TCP/IP network protocols.
2. Monitor types include: HTTP, FTP, SMTP, IP (TCP or UDP) Port, NetBIOS Share, DNS, Remote Access, Ping, Machine Share and Incoming Mail..

Resource Availability Monitoring

A Disk Space Monitor is one example of the many monitor types that are ready to be used for Resource Availability Monitoring. Click the *View a Disk Space Monitor* link and observe that the monitor will likely fail because it is set to fail if the C: drive is more than 2% full. Normally such a monitor would be set to 80% or 90% for failure. You can set this to monitor any valid file name either by drive letter or Universal Naming Convention (UNC) such as \\server\share.

Click *Test a Disk Space Monitor* and you should see a failure dialog and a single failure in the monitor run log.



When you configure monitors for your own network, likely you will trigger automatic corrective actions such as removing temporary files from disk drives that are over capacity, in addition to alerting the people responsible for the health of the network.

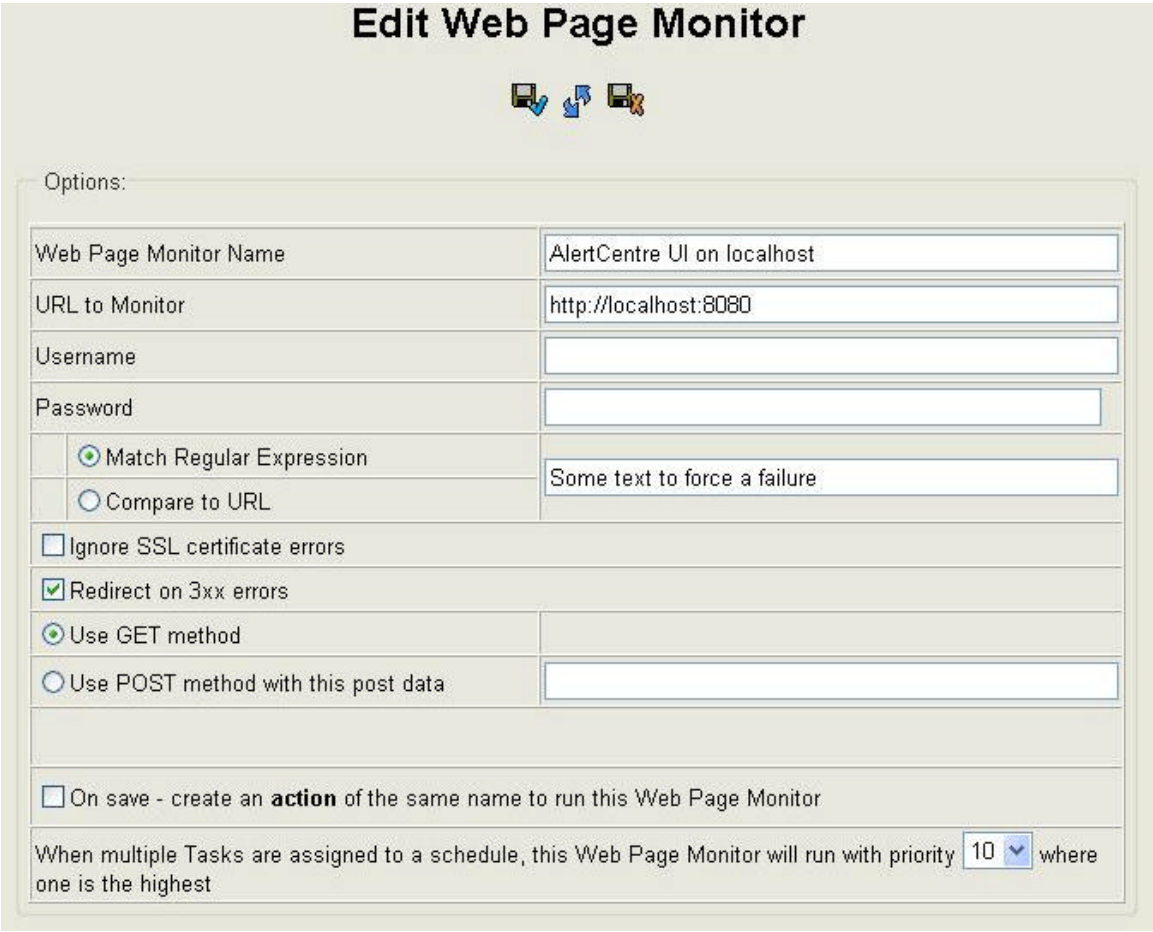
KEY POINTS

Resource Availability Monitoring

1. Can be used to test resource availability primarily for Windows-based devices, however, custom monitors can be created readily to test these same resources on UNIX machines.
2. Monitor types include: Disk Utilization, CPU Utilization, Memory Utilization, Windows Performance Counters, Directory, File, SSL, Print, News and SNMP.
3. The type of Windows Performance Counter Monitors can vary widely based on the range of applications running on the machine(s) being monitored. The AlertCentre Graphical User Interface enumerates Performance Counters automatically.

Application Availability Monitoring

A Web Page Monitor is one example of the many monitor types that are ready to be used for Application Availability Monitoring. Click on View a Web Page Monitor. You will see this screen:



A web page monitor establishes a connection to a URL, retrieves the page stored at that URL and them matches this output to a regular expression (sophisticated pattern matching) or matches to text in a file. This gives you the power to look for errors at the connection level, as well as errors in the page content (e.g., CGI errors) using a single monitor. The page being monitored in the example, which you will view momentarily (http://localhost:8080), may require you to enter a username (i.e., domainname\username) and password of an AlertCentre Administrator before the monitor will succeed.

Click on *Test a Web Page Monitor* to watch it fail – since the regular expression "Some text to force a failure" will not be found at the URL being monitored (i.e., AlertCentre UI). If the monitor fails with a 401 error, then you need to supply a username (i.e., domainname\username) and password of an AlertCentre Administrator and test again. The monitor should fail, because the text supplied as a regular expression to look for on the page does not exist on the page. Feel free to go back and change the comparison text to "MKS", and test again to see it succeed.

KEY POINTS

Application Availability Monitoring

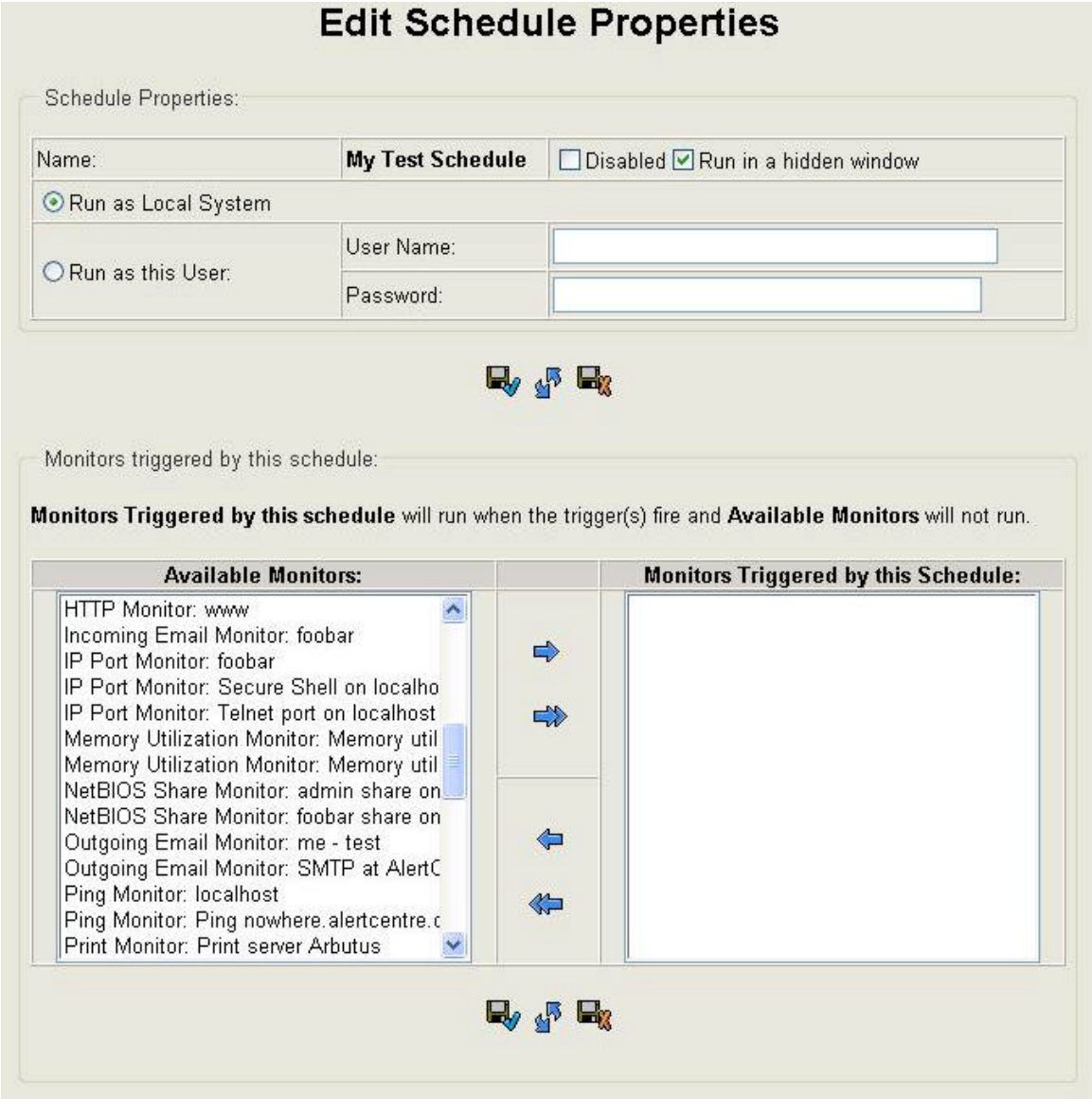
1. Compare current state of an application to a well known state
2. Take action on match or failure to match a well-known state.
3. Monitor types include: Windows Service, Web Page, ODBC Database, Generic Query, Windows Event Log, Application Event Log, Website Link Integrity and E-Mail.
4. The AlertCentre UI will automatically enumerate the Windows Services that can be monitored on any machine on your network as well as the Windows Event Logs that can be monitored. These are very useful monitor types that can keep you informed about everything from the health of Exchange Message Transfer Agents (via Windows Service Monitors) to the identification of unauthorized logon attempts (via Windows Event Log Monitors).

Schedules

Schedules are the driving force behind monitors and automated batch jobs, defining when and how often these tasks run. It helps to think of a schedule as a process that runs at specified times. And when the schedule runs, it then runs any associated monitors and batch jobs as its children. A schedule has three key components: a security context, a set of triggers, and a set of associations with monitors.

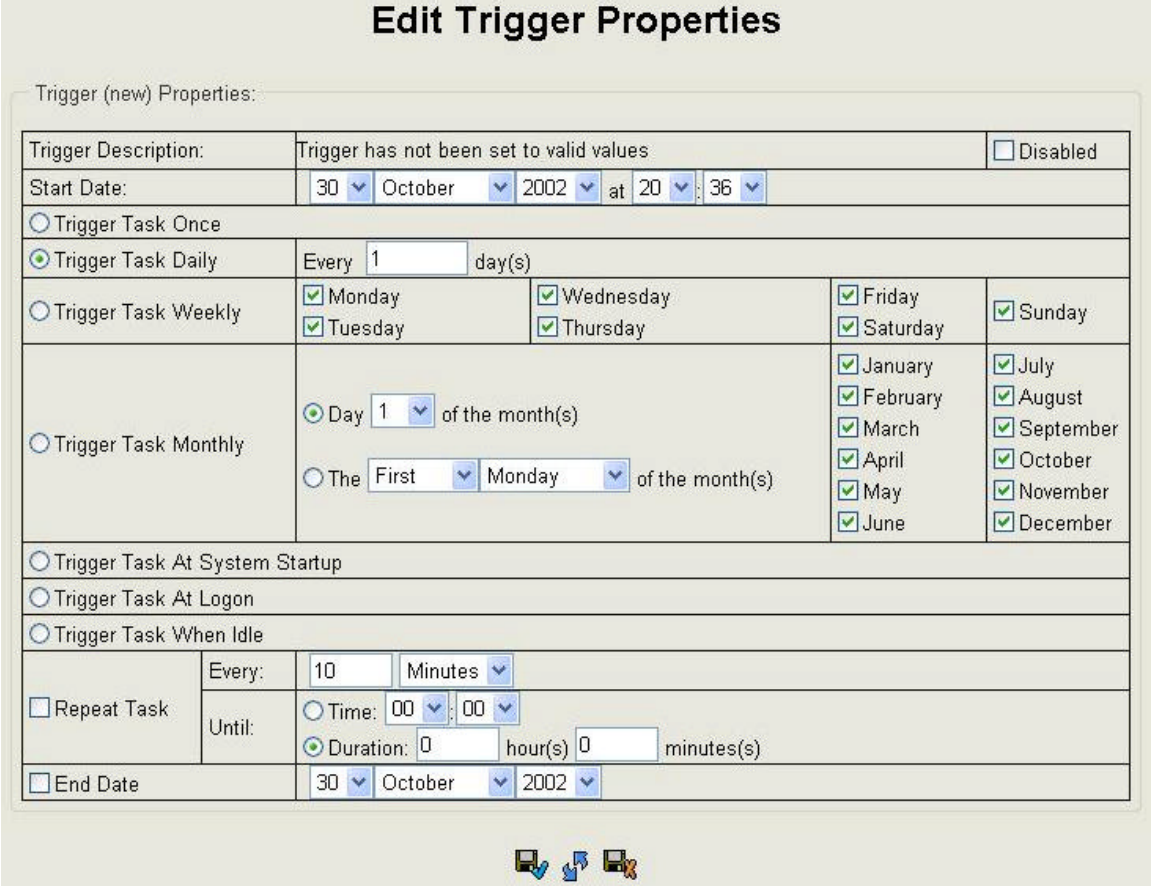
Because monitors and jobs run on the monitoring station as child processes of the schedule process, they inherit the security context from the parent, the schedule. You must ensure that the schedule runs with sufficient permissions to let all of its associated monitors and batch jobs run. We typically recommend that you run all schedules under the account of a domain administrator. By default, schedules run under the LocalSystem account. Most monitors will try to access other machines or devices on your network, and running under the LocalSystem security context, they are almost certainly guaranteed to fail for insufficient permission to access the remote machine.

Since schedules should be run as a local domain administrator, you will be asked to create your own schedule – rather than relying upon a schedule created by MKS. Please click on the Create a schedule link and you will see the following page:



Enter the username of a domain administrator and if you do not have JavaScript enabled, you will need to manually check the “Run as this user” option, and the corresponding password. Then push the >> button to add all the monitors to the schedule and then press save. Normally you associate monitors with a small set of well-defined schedules as you create the monitor, but you may also create a new schedule and associate monitors with it.

Once you have defined the name of the schedule, what monitors it triggers and whom it runs as, you should click *Save* and then specify when it runs using one or more triggers. Upon saving the schedule, you will automatically be taken to the first trigger page:



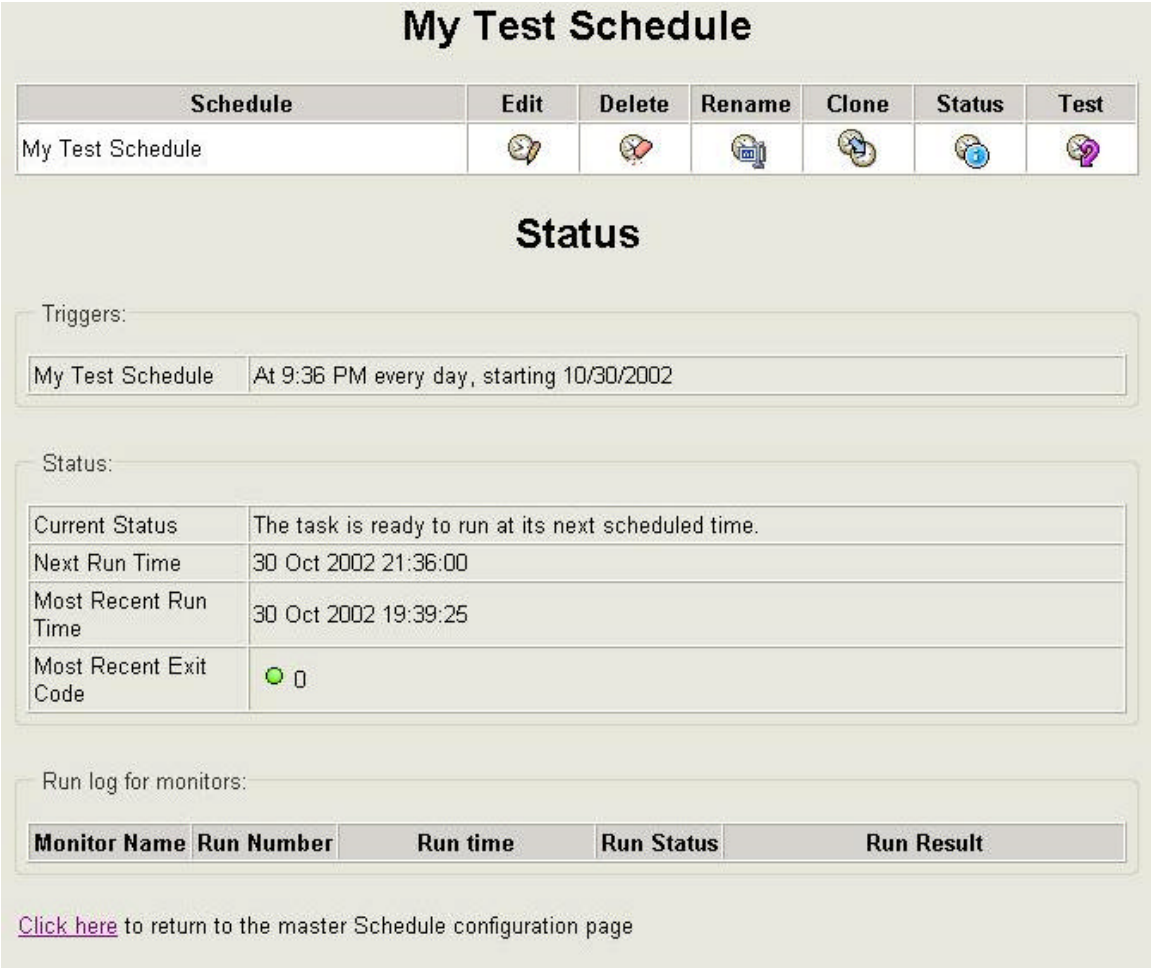
Select a start date and time for the trigger (nothing will happen until this date/time is passed), select the trigger type (once, daily, weekly, monthly, system startup, a user logon, or on idle). And fill in any parameters needed for that type (e.g. weekly on Monday and Wednesday). If you wish the trigger to fire more than once in a day, then select the "repeat task" check box and specify the repeat frequency and duration. If you wish the trigger to expire at some future date, select an end date.

E.g. an "Every 5 Minutes for the remainder of the decade" schedule would trigger daily, with a repeat interval of 5 minutes and a duration of 24 hours with an end date of 31 December 2010.

Then press "save" and you will be returned to the schedule editing page – but you will be able to edit, clone or delete the trigger you just created.

Click on the *Test a schedule* link to simulate the firing of a trigger and run the monitors – and any associated success or failure actions (several popup dialog boxes one after the other). Unlike the previous tests, which were run in the security context of the user logged into AlertCentre, this test actually runs the schedule in its own security context just as if the trigger had fired. You are now starting to see AlertCentre in action.

You will be taken to the schedule status page. Likely it will show something like the following:



My Test Schedule

Schedule	Edit	Delete	Rename	Clone	Status	Test
My Test Schedule						

Status

Triggers:

My Test Schedule	At 9:36 PM every day, starting 10/30/2002

Status:

Current Status	The task is ready to run at its next scheduled time.
Next Run Time	30 Oct 2002 21:36:00
Most Recent Run Time	30 Oct 2002 19:39:25
Most Recent Exit Code	0

Run log for monitors:

Monitor Name	Run Number	Run time	Run Status	Run Result

Click here to return to the master Schedule configuration page

A non-zero exit code would indicate that there were problems running the schedule.

KEY POINTS

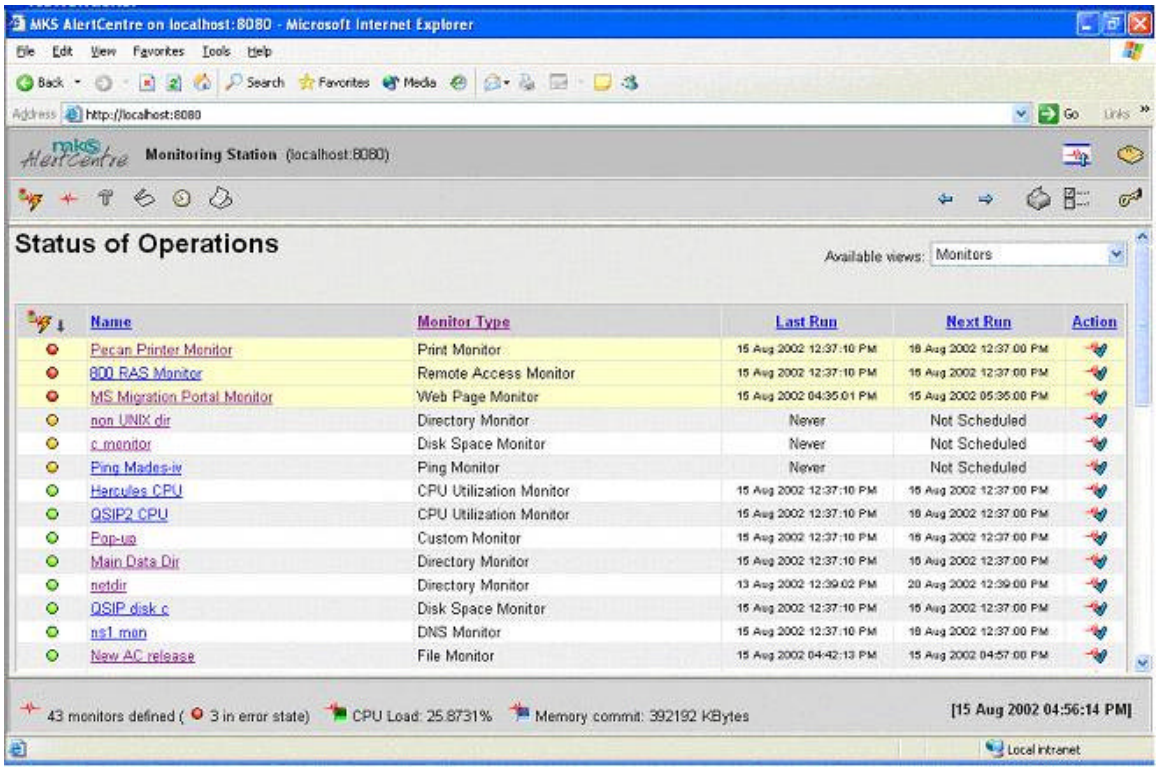
Schedules and Triggers

1. Schedules and corresponding triggers are the traffic cops in AlertCentre that control when Monitors and Jobs are executed. A single schedule can be used to trigger one or many Monitors or Jobs.
2. Triggers can be fired: Once, Daily, Weekly, Monthly, at Startup, at Logon and when Idle.
3. Triggers can also be repeated on regular intervals defined in hours or minutes.
4. AlertCentre supports complex scheduling through the use of multiple triggers per schedule.

Status of Operations

AlertCentre includes a classic-style console that makes use of Red, Amber and Green indicators, status pop-ups, and customizable views to let you know instantly the status of all network connections, system resources and applications that are being monitored by AlertCentre.

- The console view can be tailored to show Monitors, Jobs, Monitors by Group, and monitors with actions disabled.
- Within each view, you may sort the columns by Name, Monitor type, Last run, Next run or Action state.
- Hovering over a Red or Amber indicator will produce a popup containing the reason the indicator is not Green.
- Clicking an action icon will toggle the state of an action from enabled to permanently disabled, this gives you a chance to quickly disable actions on several monitors so that you can correct the issue without further interruption.



KEY POINTS

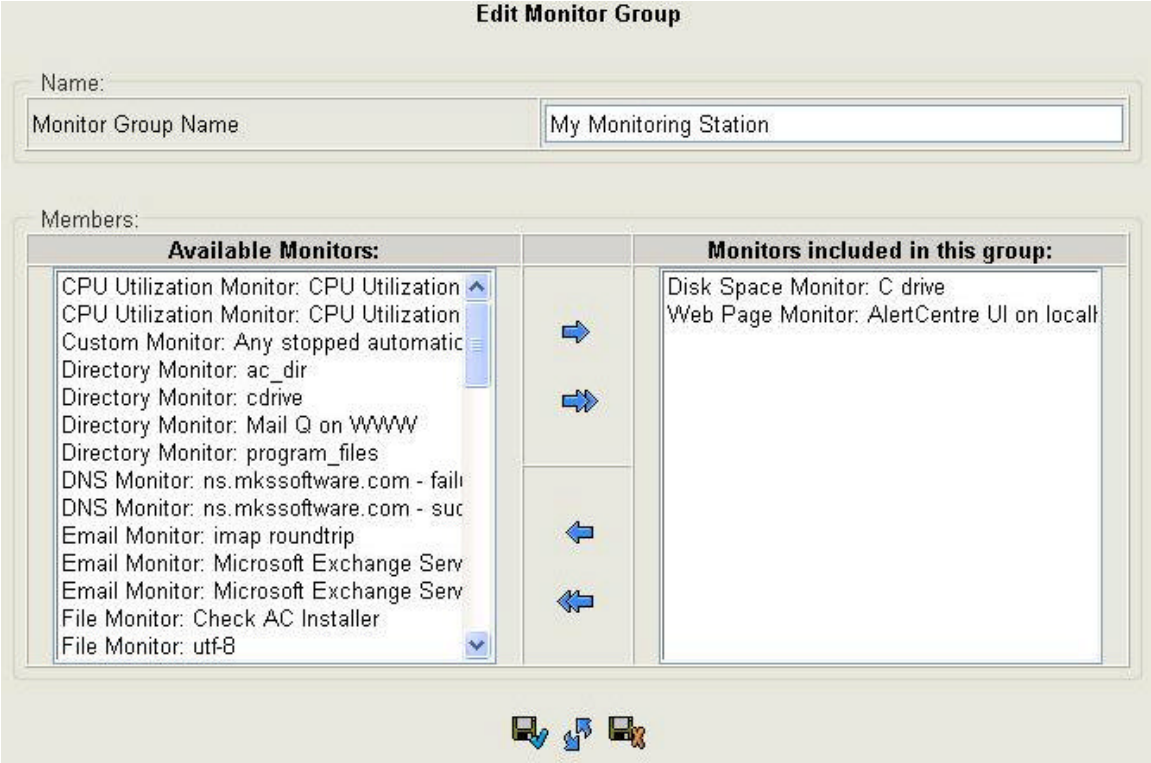
Status of Operations

1. Red, Amber and Green lights give use status at a *single glance*.
2. Customizable views to limit the information on the screen, perhaps by operational area.
3. Hover over a status icon the lean more about Alerts and Warnings.
4. Disable monitor actions to give you time to repair the problem.

Monitor Groups

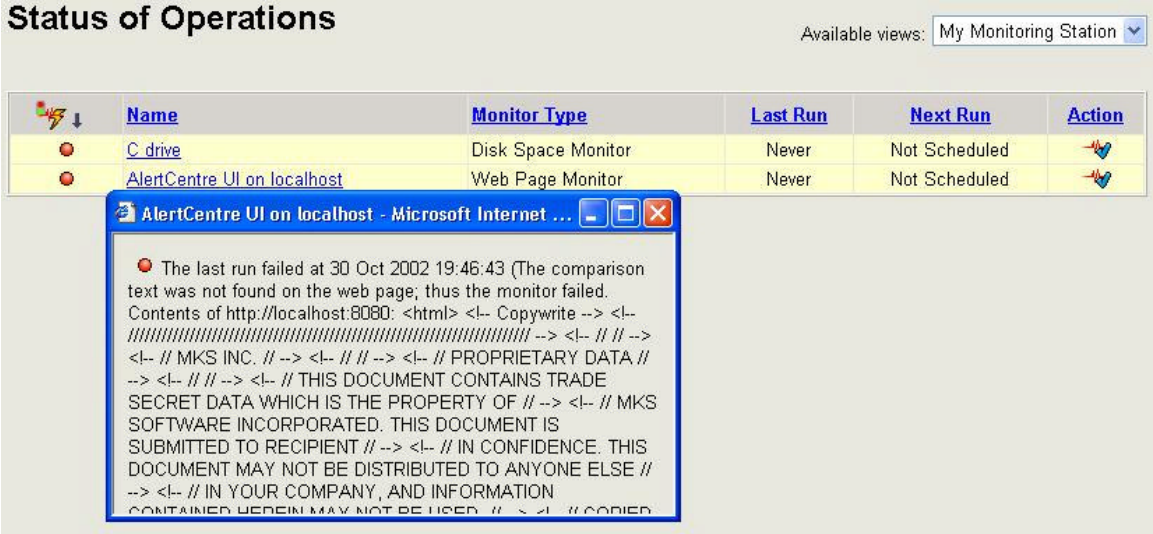
A monitor group is a container with links to monitors. Deleting a monitor group has no effect on the contained monitors; it merely deletes the grouping. Cloning a monitor group builds a new monitor group containing the same monitors as the parent. Monitor groups are useful for viewing status of and testing multiple monitors. For example if you are responsible for a given area, say Microsoft Exchange administration, you might want create a group of all the monitors necessary to monitor a single Exchange server, which may include 4 or more Windows Service Monitors, plus an SMTP port monitor, along with several Disk Space Monitors, a CPU Utilization Monitor and a Memory Utilization Monitor. Such a group can help you to find, test and review the status of all the important health metrics of given Exchange Server quickly and easily.

Click on *View a Monitor Group* to see how a Monitor Group is defined.



The Monitor Group *My Monitoring Station* contains two monitors, the Disk Space Monitor *"C drive"* and the Web Page Monitor *"AlertCentre UI on localhost"*. Feel free to make changes and save.

Click *View status by Monitor Group*.You will see output something like the following:



The Status of Operations page is typically the page you see when you first connect to AlertCentre and when you click on the SOO icon in the titlebar window. This screen shows you the current state of the AlertCentre Monitoring Station and in this case filtered by the Monitor Group. Since there are two monitors contained in the group (unless you changed it), you see failures for each member of the group. This screen will allow you to look at the overall state of the monitored objects or allow you to filter by group.

KEY POINTS

Monitor Groups allow you to:

1. Sort, filter and view manageable subsets of your configuration.
2. Manage virtual resources such as Web Stores that can be made up of multiple servers, ports, system services and applications, such as Microsoft SQL Server-based and Microsoft IIS-based applications.
3. Find, Test and View Status of groups of associated monitors all at one time.

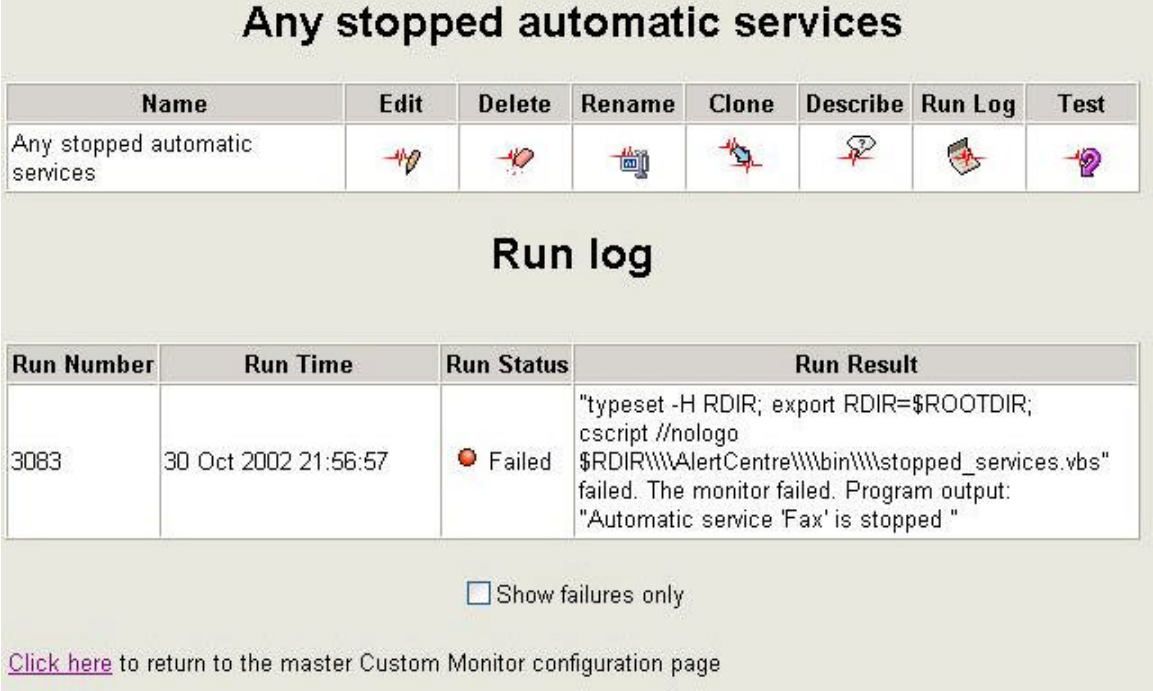
Custom Monitors

A key strength of AlertCentre is the flexibility of its architecture and its openness to customization to meet real world business needs. At MKS, we are constantly extending our own internal implementation of AlertCentre as we find new things that we need to monitor. Two key ways of extending AlertCentre are via custom monitors and via jobs. A custom monitors allows for almost infinite flexibility. Anything that you can imagine, you can implement as a custom monitor. A custom monitor is an executable program or

script that is integrated with AlertCentre, such that it has the same attributes as other monitors: a schedule, actions and alerts, and escalation rules.

Two examples are provided. The first executes a VBScript which communicates through the Windows Management Interface (WMI) to find all services marked as *Automatic* (run at system startup) which are currently stopped. To view this configuration, click on *View a Custom Monitor*.

And click *Test a Custom Monitor* to see it in action.



The second example requires that you have a Linux machine configured to accept remote shell (rsh) connections from your Monitoring Station.

1. Ensure that your Linux machine will accept inbound connections from your Monitoring Station. One way to accomplish this is to set up a .rhosts file in the home directory of the user you wish to use.
2. Ensure that Perl is installed on the Linux machine.
3. Copy the cpuload custom perl script from the local Demonstrations directory to the Linux machine r*cp $ROOTDIR/Demonstrations/cpuload.pl username@linux_machine:~/cpuload.pl*. (You can use scp instead of rcp if OpenSSH is installed on your Linux machine. Passwordless authentication is required – setup is described below).
    a. ssh-keygen –t rsa1 –f c:\tmp\.ssh\identity
        i. use an empty key password
    b. scp c:\tmp\.ssh\identity* user@host:~/.ssh.
    c. ssh host –l user
        i. cd .ssh
        ii. cat ./identity.pub >> authorized_keys
        iii. exit
    d. mv c:\tmp\.ssh\identity* c:\documents and settings\<NT username>\.ssh
4. Log into the Linux machine and ensure that Perl is in /usr/bin (and if not update the #! Line in the cpuload.pl file accordingly). Also mark cpuload.pl as executable *chmod +x cpuload.pl*
5. Test a remote shell connection from the command line. Rsh/ssh *–l <linux_machine> -l <username> ~/cpuload.pl.* See documentation for rshd/sshd and rsh/ssh is this command does not work immediately. Do not proceed to the next step until this works. Note that secure shell can be set up for password-less authentication and can be used instead of remote shell if you prefer.

6. Now return to the Evaluation Guide browser window and click *Create a Custom Monitor*. You will see this screen:

7. In the *Command line* type: *rsh <linux_machine> -l <username> '~/cpuload.pl'*. The single quotes are needed as the ~ will be expanded by the local shell if not escaped.
8. The *Success exit code* will remain unchanged at zero
9. Please leave the *Match To* blank.
10. Press Save

Now click the *Test your Custom Monitor* link to see a Custom Monitor in action.

KEY POINTS

Extensibility

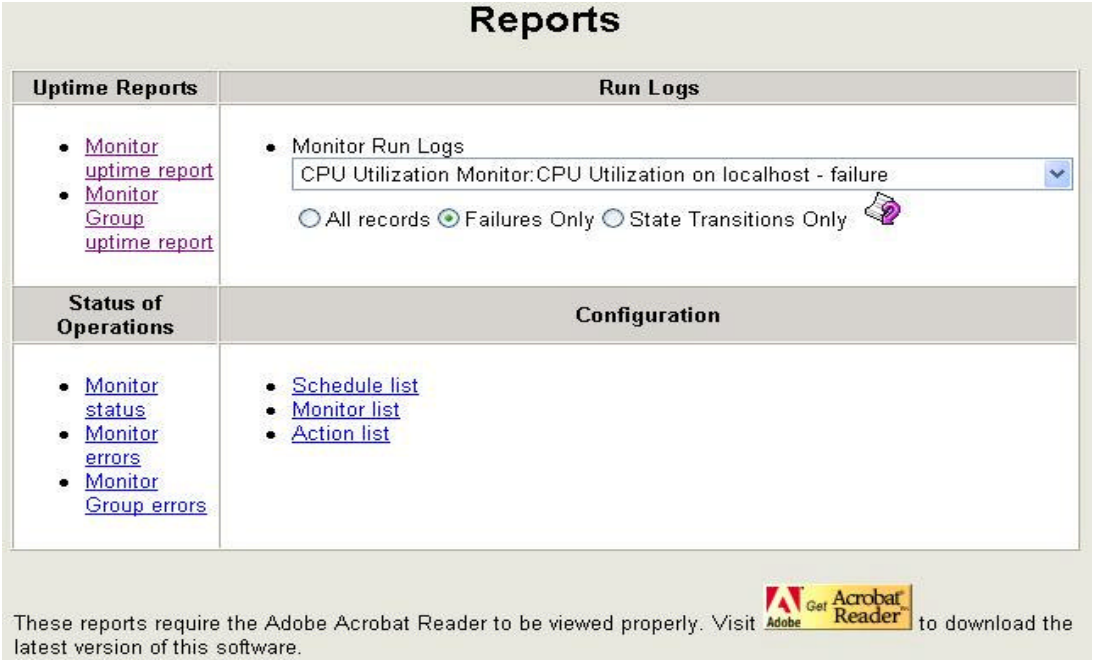
1. Custom Monitors allow you to extend the capabilities of AlertCentre to satisfy your unique monitoring needs.
2. MKS Toolkit, which comes bundled with AlertCentre, provides valuable tools such as Perl, rsh and secsh for extending the functionality of AlertCentre.
3. You can use built-in Windows tools such as Windows Scripting Host to run VBScript custom monitors.
4. You can run programs on local or remote machines.
5. You can monitor UNIX and Linux machines.
6. You can monitor your own custom applications and objects.

Reports

AlertCentre maintains an SQL database table containing information from each polling operation. This information is used to create some Adobe Acrobat files on the fly. These reports include:

- Monitor and Monitor Group uptime
- Various monitor run logs
- Various Monitor status reports
- Configuration reports for schedules, monitors and actions

The SQL table also stores (as appropriate) the counter value for each monitor. This gives you the ability to write custom queries to (e.g. chart CPU utilization over time).



AlertCentre Features and Benefits Summary

MKS AlertCentre is a cost-effective, availability monitoring solution with a killer combination of features and benefits. There are many valuable features of AlertCentre, which are not covered in the preceding evaluation demonstration, that need to be understood in order to grasp the overall value of this simple yet powerful availability monitoring solution.

Remote-ability

You don't have to be physically located at a Monitoring Station in order to use AlertCentre. The user interface provides the ability to configure and use AlertCentre from any location on a network through the use of a Web browser. This includes wireless, remote access over the Internet via VPN provided you have the appropriate administrator privileges. It is best to install AlertCentre on a server for performance reasons and because this remote use functionality enables you to access your Monitoring Stations from almost any location at any time.

Built-in Redundancy

AlertCentre is designed around the concept of a monitoring station, a machine that runs monitors and jobs that automate repetitive tasks and keep you informed of any problems in your system. A product that monitors for problems is not very useful if it does not run continually. What happens if the machine monitoring your network suddenly loses a network card, or the motherboard dies, or a faulty network hub or switch isolates it from the majority of the network? There must be a monitor-monitor to ensure that the monitoring continues even in such a disastrous situation.

Therefore AlertCentre has adopted the concept of a primary monitoring station, the one that normally performs monitoring, and a backup (a partner) monitoring station, whose job it is to ensure that the primary stays alive and to take over monitoring should the primary fail to respond. When the primary comes back on line, the backup will revert to its usual role. Should the primary ever go down, the backup will alert you in the manner that you choose. Although use of backup monitoring stations is optional, we highly recommend that you use them.

Every AlertCentre license lets you install AlertCentre twice: once on the primary monitoring station and once again on the backup monitoring station. During installation, you must choose the role of the monitoring station: primary or backup. After installing the software, you will establish the partnering relationship. Until you have established the specific partnering relationship between two monitoring stations, you can change a monitoring station's role from primary to backup and vice-versa.

Once you establish the partnering relationship between the primary and its backup, all configuration information from the primary is replicated to the backup, so that the backup is ready to take over monitoring should the need arise. Periodically from that point on,

the primary signals the backup that it is still alive and the partners synchronize any configuration information that has changed since the previous synchronization point. You can force a manual synchronization at any time and you can sever the primary-backup relationship.

Security

To ensure sufficient privileges, all users of AlertCentre must be members of the Administrators and AlertCentre Administrators groups. The AlertCentre Administrators group is created locally during installation. By default, all local Administrators and Domain Admins (if the machine belongs to a domain) are added to this group to facilitate use of AlertCentre. All AlertCentre files including the HTML tree, components, and configuration files are secured such that AlertCentre Administrators have full control.

At any time, you can change membership in this group by selecting **Manage AlertCentre Administrators** on the Housekeeping page. Note that adding users to the AlertCentre Administrators group will permit access to the Graphical User Interface, but will not provide any rights to access the network or network resources. We recommend that you only add domain administrators to this group.

Other security issues are covered in the AlertCentre Users Guide.

Agent-less Architecture

MKS AlertCentre was designed to function without requiring agents on monitored servers and other devices. This architecture has multiple benefits in terms of reduced maintenance and improved security. Since there are no agents to install on monitored machines, there is no need to install or maintain monitoring software on those machines for monitoring purposes. In some cases, you may want to install MKS Toolkit for System Administrators on monitored machines to enable secure, remote access to such machines for corrective action via secshd.

Extensibility

AlertCentre is built almost entirely from scripts. The back end monitors, event handlers and alerting engines are written in Perl. A very small amount of "C" and C++ code is encapsulated in about four COM components. To learn more about scripting and to learn more about the AlertCentre implementation, please read the Evaluation Guide for MKS Toolkit for System Administrators Start→Programs→MKS Toolkit→Evaluation Guide→For System Administrators→MKS TKSA Evaluator's Guide.

All of the scripts used to build AlertCentre are available on your Monitoring Stations as examples for you to use in building custom monitors, jobs and actions. In addition, every copy of AlertCentre requires MKS Toolkit so you also have at you disposal all the tools and scripting engines that MKS used to build AlertCentre. You are encouraged to copy a few of AlertCentre's scripts and modify them to fit your needs better. Then you can implement them as Custom scripts without affecting the rest of AlertCentre. Once you experience the power of scripting, you'll have more freedom to satisfy the needs of your organization. The back end scripts can be found in $ROOTDIR/AlertCentre/Scripts and it.

Application Wizards

AlertCentre makes it easy for you to define monitors for popular applications through Application Monitoring Wizards. The wizards automate discovery of an applications configuration and then generate the detailed monitors necessary to ensure high availability and maximize performance for the application's specific configuration. A wizard can potentially generate hundreds of monitors for a complex application such as IIS on a large web server, saving considerable time and ensuring comprehensive monitoring. The wizard also creates a monitor group to make it easier to manage the monitors associated with an application on a specific server or workstation. Wizards currently exist for the following applications:

- Microsoft Exchange
- Microsoft IIS
- Microsoft SQL Server

The AlertCentre Resource Kit

Please be sure you have updated it to the latest version by visiting the AlertCentre Resource Kit Home Page.

The AlertCentre Resource Kit contains some valuable additions to AlertCentre and serves as an example of how to extend the AlertCentre User Interface. At the time of writing, the Resource Kit contains:

- The ability to bulk change AlertCentre passwords. With all the schedules, monitors, and other insundry secrets, it can be hard to deal with a routine password aging policy. With this Resource Kit script (and corresponding User Interface) you can change all passwords associated with a particular account.
- Display the currently selected backup password. Since in general the AlertCentre UI never retrieves an LSA secret, it can be hard to remember what you set the automated backup password to. This option will display in clear text the current password. Caution is recommended to be sure others are not looking over your shoulder.
- The AlertCentre Initialization Wizard allows you to create a standard set of schedules. If you deleted them or simply did not create them when presented with the opportunity and wished you had - here is your pointer back to that page.
- You might have a set of monitors for a particular machine and wish to clone them all for a different machine The cloning capability within AlertCentre will allow you to do this manually, but it can be a lengthy and user intensive operation. The resource kit cloning tool makes this job a snap

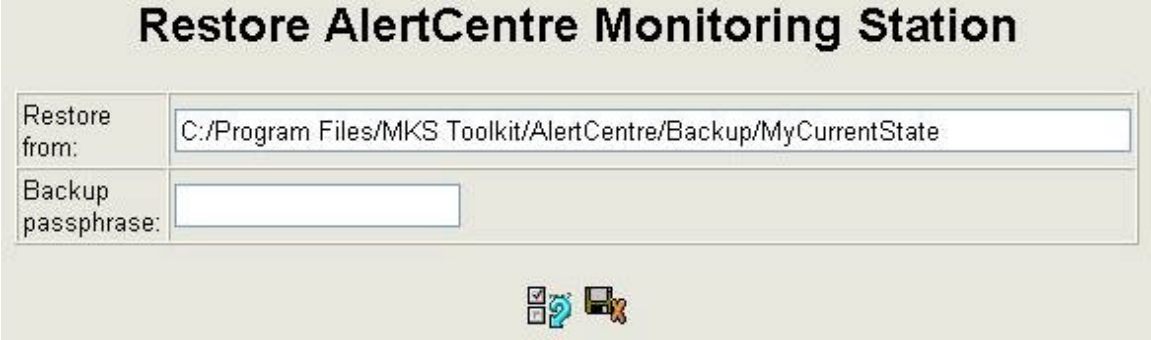
Check back often, since the Resource Kit is often updated between product releases.

Wrapping up the evaluation

Thank you for evaluating the MKS AlertCentre. AlertCentre is built on the scripting power of MKS Toolkit for System Administrators. Please see its Evaluation Guide for more detailed information about the underlying implementation and the power of scripting.

The Evaluation Guide sample configuration is full of useful examples and we encourage you to stray beyond the boundaries of this evaluation and experiment with this example configuration. When you are ready to remove this configuration, click on the *Wrapping up* link. You will have two options:

1. Restore the state you saved at the beginning of the evaluation. Use the same password you used for the backup.



2. Restore an empty configuration. Use the password *Empty* to restore this configuration.

Once you have restored one of these configurations, you are ready to build or improve your own configuration. Enjoy! In the unlikely event that we have left you with questions, please feel free to contact your MKS Software Sales Manager or Customer Support Representative.

Customer Support

MKS offers extensive customer support to ensure your success with our products. At any time during your evaluation of our products, please feel free to contact us concerning any issues that may arise.

The evaluation versions of any MKS Toolkit products include free support from the time of installation. In order to continue support beyond the evaluation period you must purchase a fully licensed version of the product along with a Preferred Customer Support

(PCS) contract. PCS is renewable annually for a small fee and entitles you to unlimited customer support, patches, bug fixes, and product upgrades. All of our sales channels offer MKS Toolkit products with bundled PCS for your convenience. You may also purchase unbundled PCS contracts by contacting MKS directly

To receive support, you must register. You will have the chance to register with our support organization during installation of your product, or you may do so at any time over the web at http://www.mkssoftware.com/register.

To request customer support, please contact us by one of the means listed below and in your request, include the name and version number of the product that you are using, your serial number, and the operating system and version/patch level that you are using. Contact MKS customer support at:

Web: http://www.mkssoftware.com/support
E-mail: mailto:tk_support@mkssoftware.com
Telephone: +1-703-803-7660 (9:00am to 7:00pm Eastern, Mon-Fri)
Fax: +1-703-803-3344

Additional MKS Toolkit Resources

There are several other sources for additional information about our MKS Toolkit products. We have general product information, including technical specifications, detailed utility listings, and datasheets at:

MKS Toolkit Product Information: http://www.mkssoftware.com/products

We offer a resource kit including example scripts, additional utilities, more tutorials, and a wide variety of other useful information at:

MKS Toolkit Resource Kit Page: http://www.mkssoftware.com/reskit

The MKS Toolkit product family also offers a number of Add-On components for download from out Web site:

MKS Toolkit Add-On Page: http://www.mkssoftware.com/support/add_ons.asp

Through the years, we have accumulated a lot of technical details about the MKS Toolkit products and have put this information in a searchable database at:

MKS Toolkit Knowledge Base: http://www.mkssoftware.com/support/kb

Our customers commonly ask certain questions. These questions and their answers are in our Frequently Asked Questions pages at:

MKS Toolkit FAQs: http://www.mkssoftware.com/support/faqs

Ordering Information

MKS Toolkit can be purchased from the MKS Web Store, from MKS Software Sales, from our resellers, or by calling +1-703-803-3343 or 1-800-637-8034.