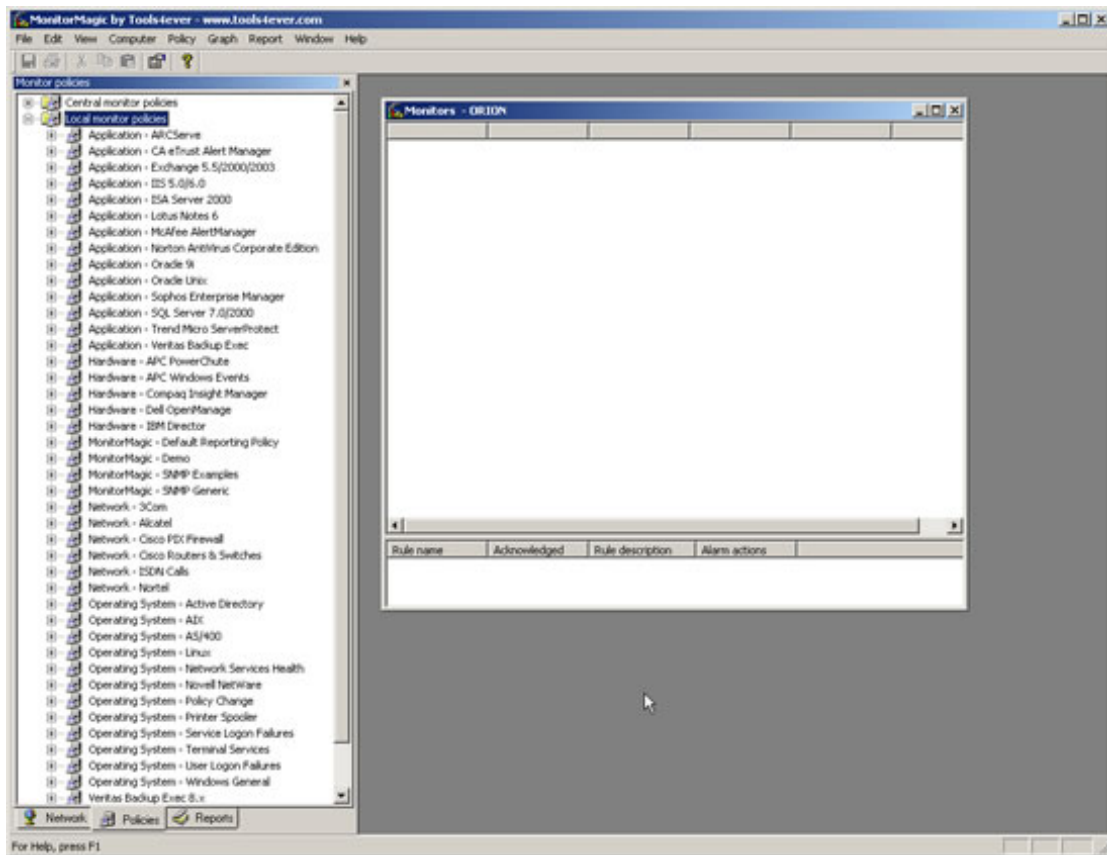


I. MonitorMagic policy basics

Note: this document is meant as an extension to the *MonitorMagic Implementation Guide* and certain parts assume that you have read and performed all operations in this document.

Always make sure you use the latest set of policies released by Tools4ever. The easiest way to obtain the latest policy bundle is to access our forum through <http://forum.tools4ever.com>. When you have downloaded the latest policy bundle, delete all existing policies under the **Local monitor policies** branch, as shown in the screenshot below. Do this by simply clicking on the first entry, hold shift and select the last entry, then right-click and select the **Delete** option. Now select the **Local monitor policies** branch, click on the **Policy** menu, select **Import policies...** and select the downloaded policy bundle. You will notice that the policy list has been rebuilt from the new policy bundle.

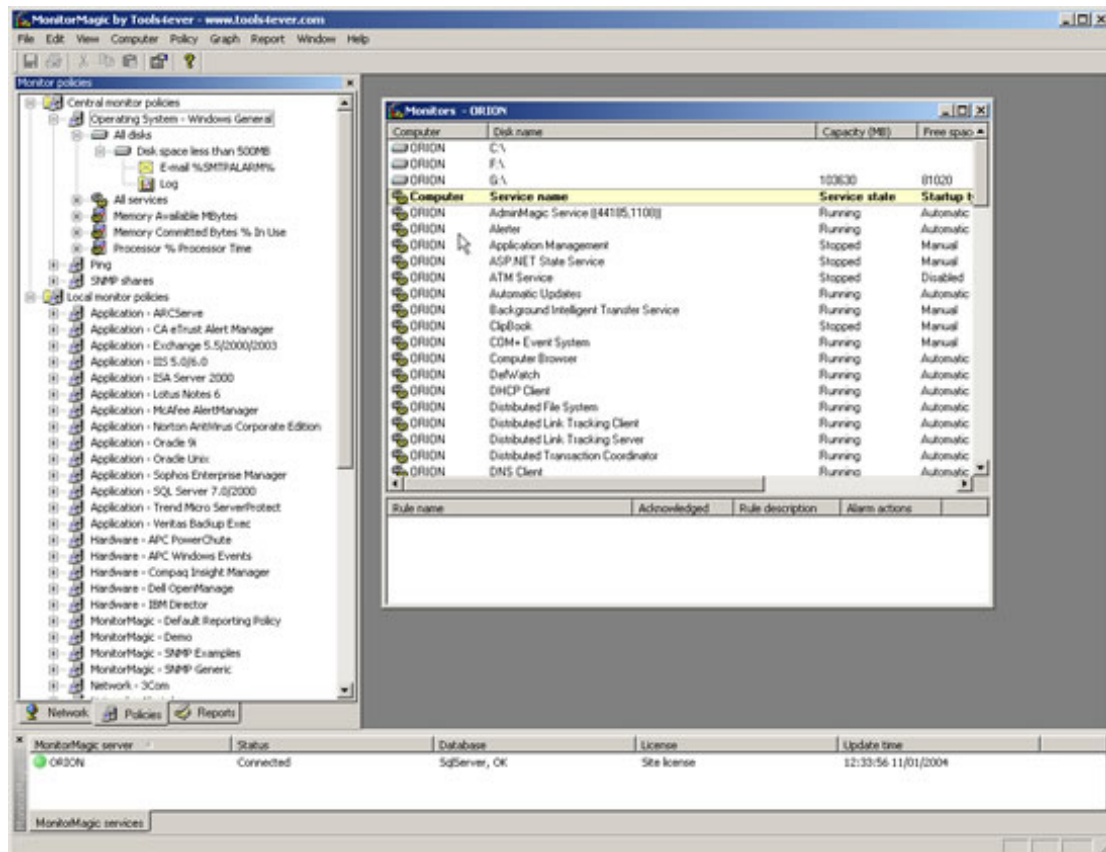


A policy represents a group of "monitors". In MonitorMagic, a monitor represents a single identity capable of monitoring one or more resources. In the screenshot below, you can see subset of all policies that are pre-configured and ship with MonitorMagic.

When looking at a policy and expanding the first level, you will see the monitors appearing. Each monitor can have one or more "rules", which in turn can have one or more "alarm actions". An example is show in the screenshot below, where the Operating System – Windows General policy has been expanded. Inside, there is 1 disk monitor, 1 service monitor and 3 performance counter monitors. When expanding the disk monitor, you will see the rule, which in this case is named "Disk space less than 500MB". This is just a caption for the real rule, which can be revealed by double clicking on the rule. In the dialog that appears, you will see several rule criteria which decide of the value that the monitor has found is reason enough to execute an alarm action. If you go back and expand the rule, you will notice one or more alarm actions, in this case an email alert and an event log alert.

Monitor auto-sensing:

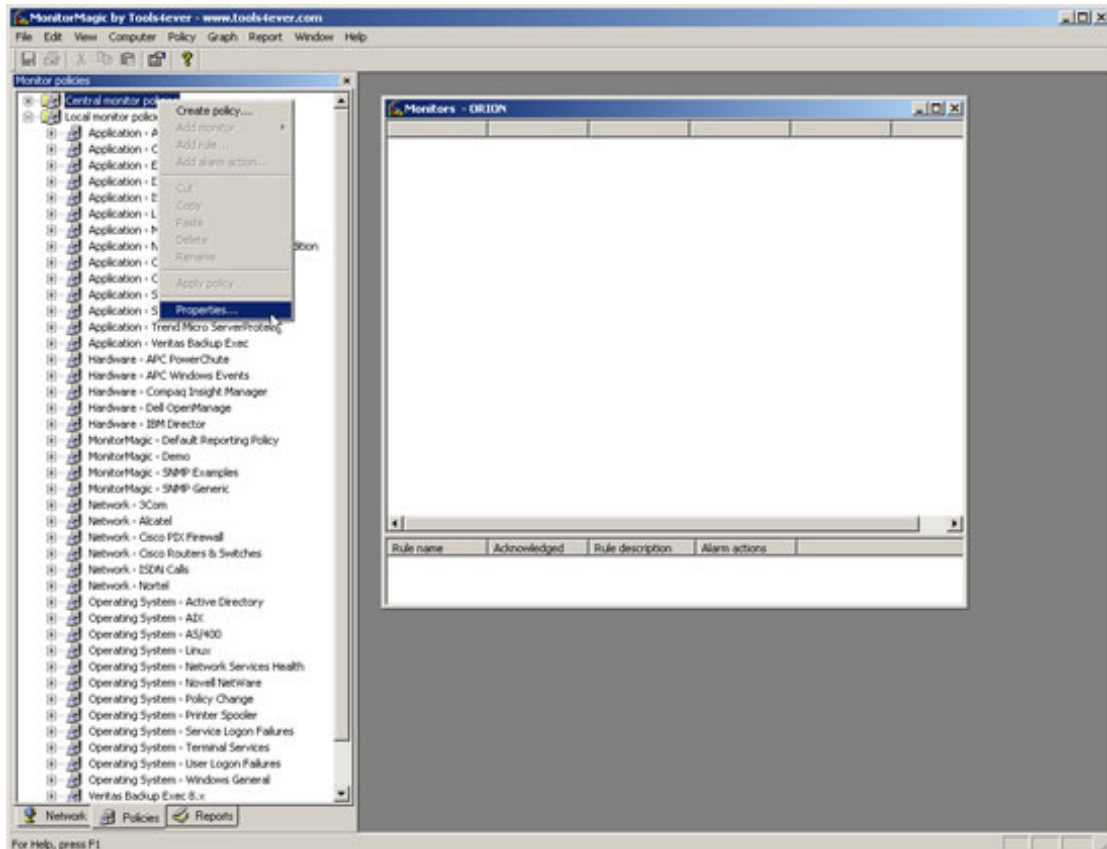
A very important concept in MonitorMagic is that certain monitor types have auto-sensing capabilities. Imagine configuring disk monitoring for your servers, and that SERVERA has drive C, D and E, while SERVERB has drive C, P and U. Without auto-sensing this would require the specification and configuration of 6 monitors, one for each logical drive. Not only will this take a lot time to do, you no longer have the ability to define a generic policy for all servers. To solve this issue, MonitorMagic introduces the concept of auto-sensing monitors. As you can see in the screenshot below, there is only a single disk monitor which has been configured to monitor "All Disks". So when you apply this policy on a target system, monitors for drive C, F and G are automatically generated and inherit the configuration of the master monitor you already defined.



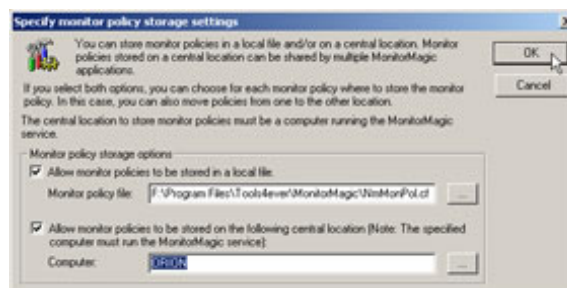
2. Setup central monitoring policies

Local monitoring policies are saved on the client, whereas central monitoring policies are saved on a MonitorMagic service. This means: **Central monitor policies can be shared by multiple MonitorMagic applications installed on different computers. Local monitor policies cannot be shared.**

To setup central monitoring policies, right-click on the Central monitor policies branch and select Properties.

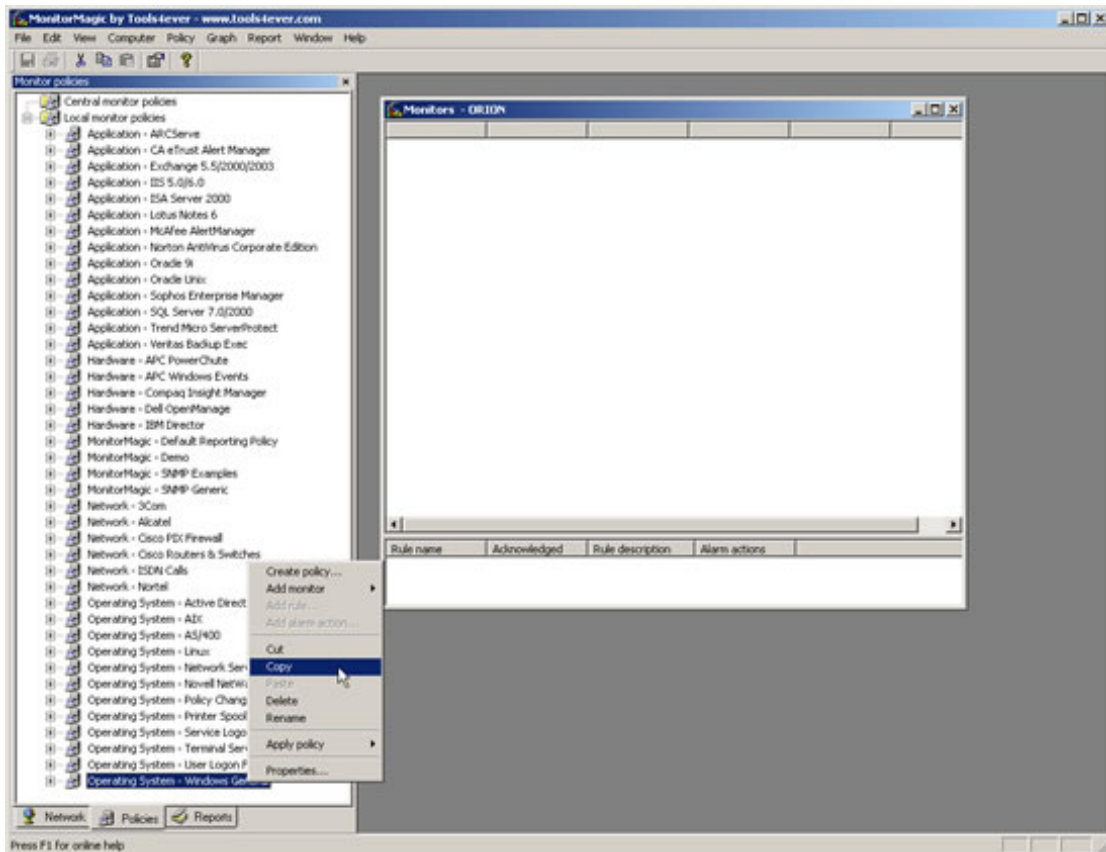


In the next dialog, shown in the screenshot below, enter the name of the computer running the MonitorMagic service. Note that the local policies are stored in the file listed also in this window. When migrating a client to another computer, be sure to make a backup copy of this file.



3. Using central monitoring policies

Now that central monitoring policies have been configured, let's start using it by copying the policies that we actively use in our implementation into the central monitor policies branch. To do this, select the most widely used policy – "**Operating System – Windows General**", right-click and select **Copy**.



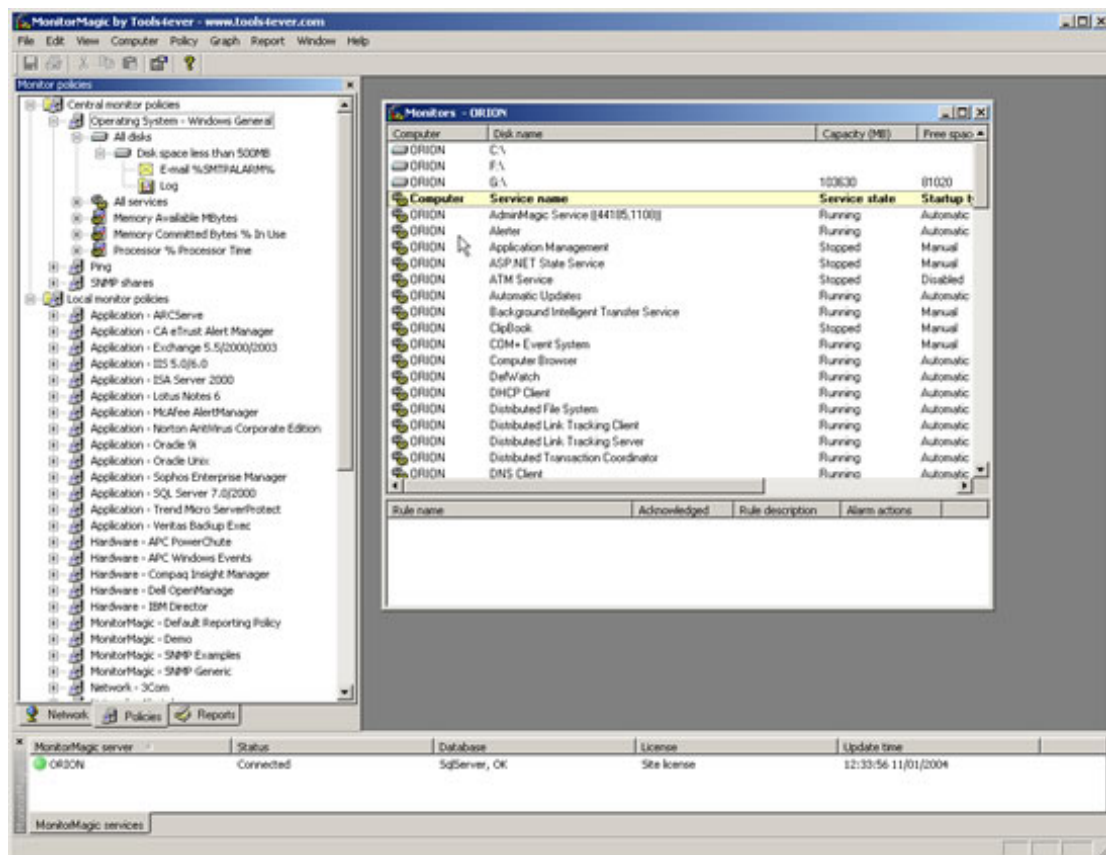
Now, select the **Central monitor policies** branch, right-click and click **Paste**. A copy of the original policy is now available as a central monitor policy. All clients connecting to the MonitorMagic service that we have setup can access the same policy.

4. Applying policies

The process of activating a policy on a machine is when you “apply” a policy. In MonitorMagic, the preferred method of doing this is to use drag-and-drop. In the screenshot below, the policy “Operating System – Windows General” has been applied by dragging it to the window Monitors – ORION. This window represents an active MonitorMagic service running in ORION.

Important: when you drag and drop a policy on a target, all monitors inside the policy will be activated to monitor the target. It does not indicate which service will actually perform the monitoring. Since MonitorMagic supports both agentless and agent-oriented scenarios, you can control this using another method.

In the screenshot below, you can see that the disks and services on computer ORION are being monitored, and that the service on ORION is doing the work.



5. Agentless monitoring

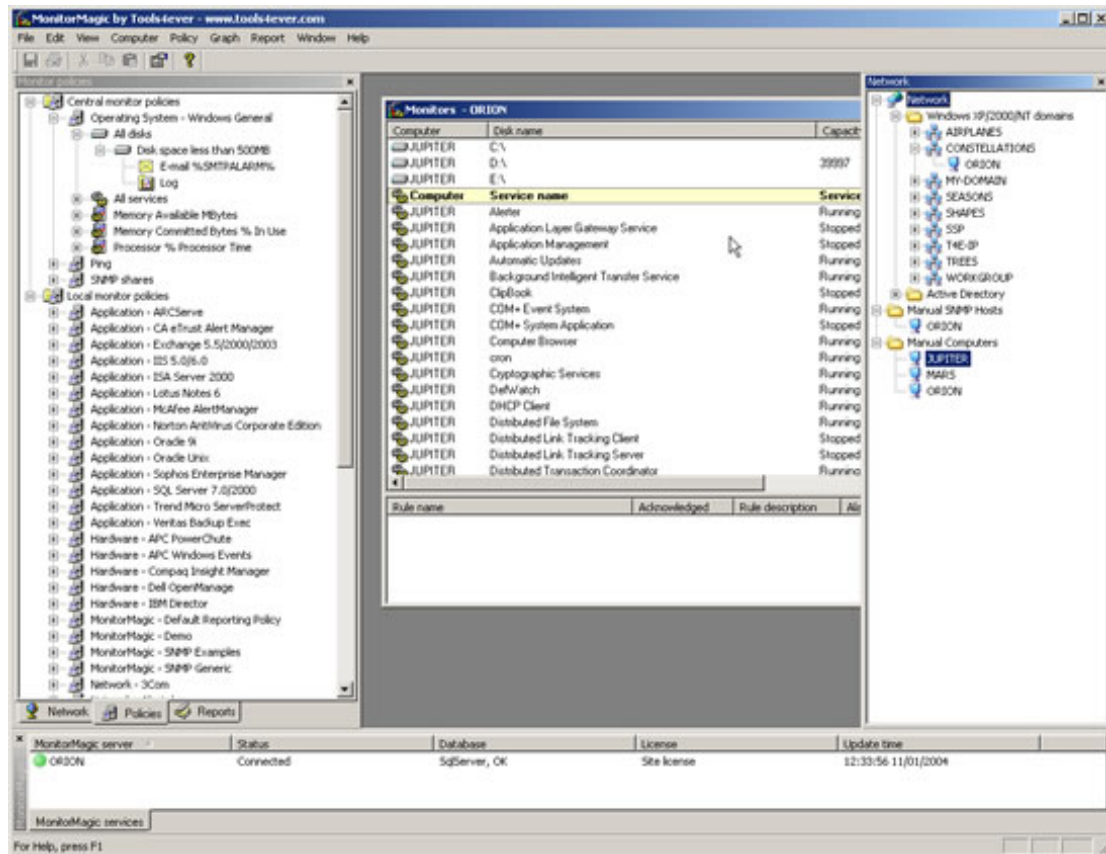
The strength of MonitorMagic lies in the architecture to support agentless monitoring. This means that to monitor a target, that target does not need a service to be installed. The monitoring can be performed from a remote location at the cost of minimal impact on network resources.

To understand the way MonitorMagic works when it comes to applying policies, take a look at the properties of the "**Operating System – Windows General**" policy by using right-click and properties. When looking at the "**Service selection**" tab, you will notice that the default setting is "**Ask the User**". Ok, so when you apply a policy on a target system MonitorMagic should ask you which service is going to operate the monitors. But, the exception to this rule is when there is only 1 monitor window open. In that case, MonitorMagic assumes that you want to use the service associated with the open window to operate the monitors. As we have seen in the previous chapter, MonitorMagic did not prompt to specify the service when we applied a policy onto the monitor window of ORION. This was because only one monitor window was open at the time.



To take advantage of the concept that we just introduced, open up a new network browse tree by using the "View" menu and then "Browse network". Drag-and-drop the "Operating System – Windows General" policy onto a computer in the network tree, while leaving the monitor window to ORION open.

The result is that the MonitorMagic service on ORION is now remotely monitoring disks and services on JUPITER. You can check this by verifying that the computer names in the monitor window are not the same as the name of the monitor window itself.



6. Maintaining policies

While it is possible to create monitors, rules and alarm actions directly in a monitor window using the right-click and "**Add monitor**" feature, Tools4ever strongly recommends using policies only. Using policies is the only way to save and replicate your configuration; monitors that have been created directly on a monitor window cannot be modified, except for scheduling and database options.

Important: when working with policies it is important to know that policies are not automatically propagated. When you have applied a policy to a number of servers and modify it afterwards, you will have to re-apply the modified policy again. Before you do this, best practice is to remove all existing monitors belonging to the policy. This can be time-consuming process since there is no way of linking monitors directly to a policy. The reason for this is that monitors inside a policy and active monitors do not have a 1:1 relationship. Remember the auto-sensing disk monitor, which was configured as a single monitor in the policy, but when applied automatically created 3 monitors? The best way to save as much time on re-applying policies as possible is to test your most complicated policy on several targets before applying them. Removing monitors for simple policies is very easy since you can spot them easily.