Installation and configuration guide

Version 1.1

Systemintegrasjon AS
www.sysint.no

END-USER LICENSE AGREEMENT FOR CPUGUARD
Important - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the author of this Software, Systemintegrasjon AS ("VENDOR"), for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by national copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE
Choose between license for Evaluation purposes or a purchased license:

a) Evaluation purpose
This EULA grants you the following rights: Installation and Use for Evaluation purposes. You may install and use a limited number of copies of the SOFTWARE PRODUCT for up to 30 days for Evaluation purposes only. It is strictly prohibited to use the SOFTWARE PRODUCT in a production environment, unless sanctioned in advance by the VENDOR. Any violation of this provision shall require a mandatory purchase license as well as expose the user to other legal recourse for collection and punitive damages.

b) Purchased license
After installing this SOFTWARE PRODUCT, the VENDOR grants to you a non-exclusive license to use the SOFTWARE PRODUCT. The purchased license is valid for a workstation, a server or both, and is valid for one version of the SOFTWARE PRODUCT, e.g. version 1.0. The license may be valid for one machine, for a set of machines or may be a site license. The SOFTWARE PRODUCT may only be used on at most the number of machines for which there is purchased licenses. Any violation of this provision shall require a mandatory purchase of missing licenses as well as expose the user to other legal recourse for collection and punitive damages.

2. REPRODUCTION AND DISTRIBUTION
You may reproduce and distribute an unlimited number of copies of the Evaluation version of this SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may only be distributed as a standalone product. The right to distribute copies does not apply to the fully functional product, which only can be distributed by the VENDOR or his representatives. License keys and serial-numbers may NOT be distributed.

3. REVERSE ENGINEERING
You agree not to reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the SOFTWARE PRODUCT.

4. COPYRIGHT.
All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by Systemintegrasjon AS. The SOFTWARE PRODUCT is protected by national copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material.

LIMITED WARRANTY

NO WARRANTIES
The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or noninfringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

UPDATES
The end-user may free of cost download service releases, bug-fixes, etc, for the version of the SOFTWARE PRODUCT for which the license is valid.

NO LIABILITY FOR DAMAGES
In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the VENDOR has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

The total responsibility of the VENDOR according to this EULA, is limited to at most the price of the SOFTWARE PRODUCT.

Trademarks
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Citrix, the Citrix logo, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, MultiWin and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc., and may be registered in certain jurisdictions.

Contents

1 General information about CPUGuard 2005

1.1 Purpose

CPUGuard protects client and server computers of excessive CPU usage, so that if a process or application goes beyond the configurable limits of CPU use, CPUGuard will lower its priorities so that other processes can continue to run without interruption.

CPUGuard makes it possible to run multiple applications on the same server, without the risk of interference between the applications when it comes to CPU usage. CPUGuard insures that all your applications get its share of CPU time.

When multiple users are sharing the same application servers it normally affect the servers response time. If a Terminal Server user starts an Excel sheet which uses 100% CPU time the whole server becomes unresponsive and other logged in users will experience a degraded session. CPUGuard prevents this by lowering the priority on the process which uses more than a configurable percentage of CPU in a configurable time slot.

CPUGuard also has capabilities for locking processes to one or more specific processors, and limiting the maximum working-set memory processes are allowed to consume.

Because of this CPUGuard gives your users a better Server Based Computing experience.

CPUGuard uses standard and documented Microsoft Windows API's.

1.2 System requirements

1.2.1 Windows installer

CPUGuard minimum requirements are Windows Installer 1.1

1.2.2 Supported operating systems

- Windows 2000 Professional and Server

- Windows XP Professional

- Windows Server 2003

- Terminal Services

- Citrix Metaframe

- CPUGuard also work on Windows NT 4.0 with SP6 and IE 5 or higher, but since no excessive testing has been performed on Windows NT 4.0 this configuration is unsupported at this time.

1.2.3 Hardware requirements

CPUGuard has no particular hardware requirements.

2 Installation

2.1 Overview

In this chapter we show you how to setup CPUGuard 2005 in your environment.

2.2 CPUGuard installation methods

Multiple methods are available to suit your specific needs.

2.2.1 Manual installation

Manual installation using the setup wizard is suitable when you have a few servers, or wish to test CPUGuard on a single computer for evaluation purposes.
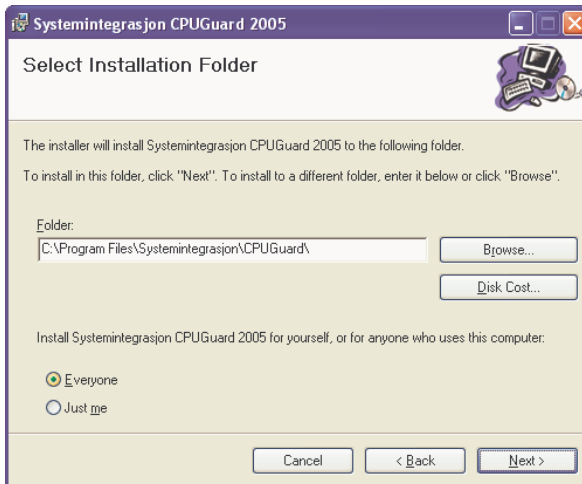
2.2.1.1 Installation

Start the installation of CPUGuard by double clicking on the setup package *SetupCPUGuard.msi* file. Then follow the simple installation wizard illustrated in the figure below:
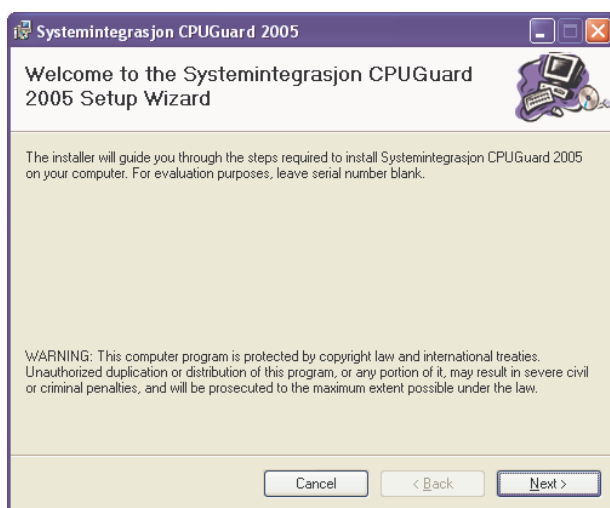
Next.
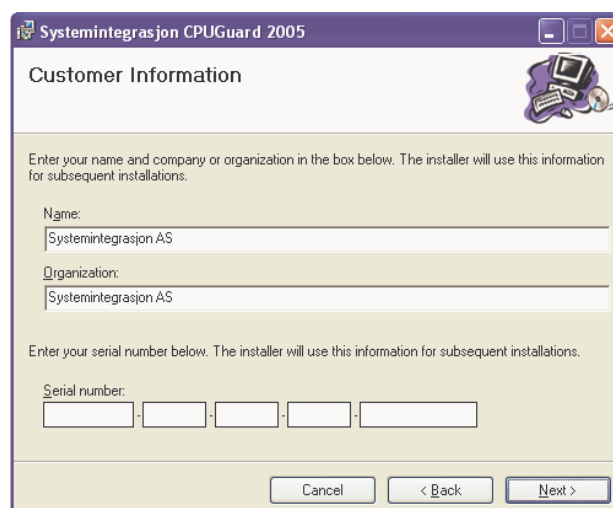
Enter company and license information. Without a serial number, CPUGuard will be fully functional in evaluation mode for 30 days. Next.
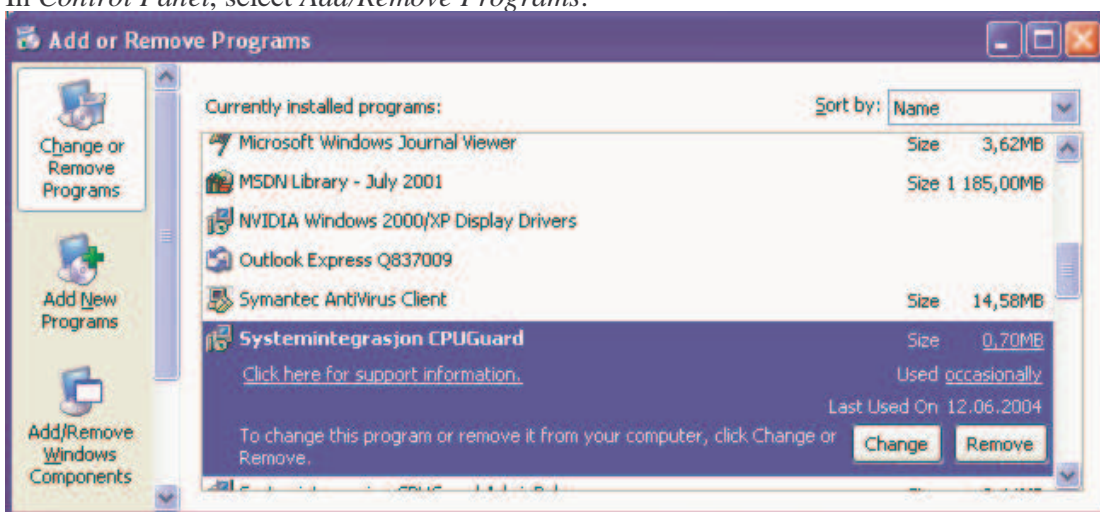
Verify installation path. Next.
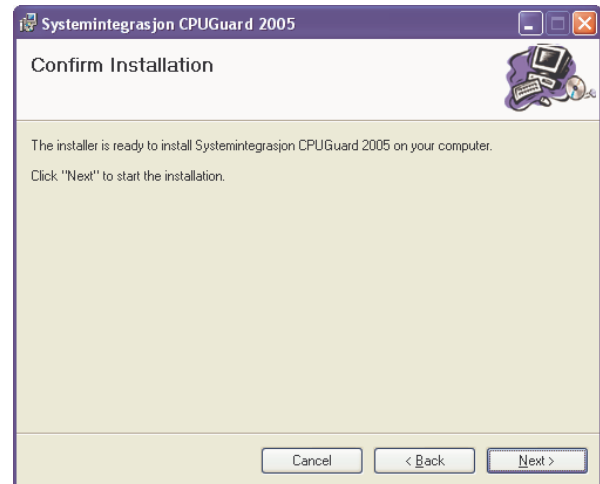
Next.
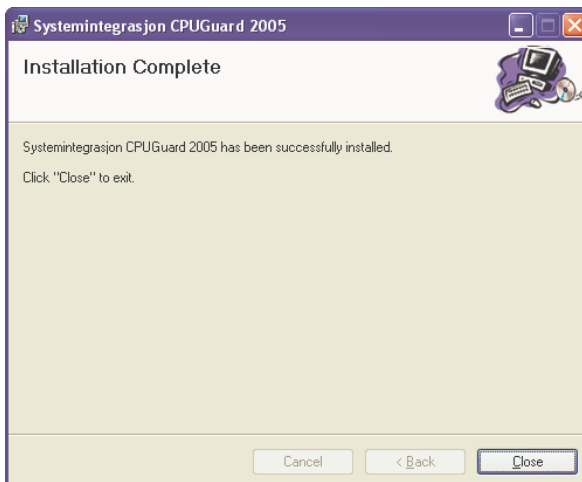
Installation is finished. Close.
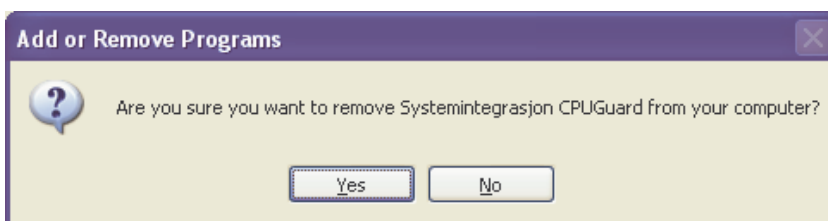
2.2.1.2 Uninstallation

Uninstallation can be performed locally from the installation wizard.

In *Control Panel*, select *Add/Remove Programs*.

Select *Systemintegrasjon CPUGuard*, and choose *Remove*.

Confirm removal.

2.2.2 Unattended installation using Windows Installer

Unattended installation can be performed using the Windows Installer executable **msiexec.exe**.

2.2.2.1 Installation

Installation can be performed from the command-line or in a script.
An example command-line can look like this:

```
msiexec /i SetupCpuGuard.msi /qn PIDKEY="00102-020302-0320002-000124"
COMPANYNAME="Your Company" USERNAME="John Smith"
```

Check the Windows Installer documentation for details on using msiexec.exe.

2.2.2.2 Uninstallation

Uninstallation can be performed from the command-line or in a script.
An example command-line can look like this:

```
msiexec /qn /x "<path to setup file>\SetupCpuGuard.msi"
```

Check the Windows Installer documentation for details on using msiexec.exe.

2.2.3 Distributing via Active Directory Group policy

If you have multiple servers we recommend using software distribution tools, and configuring
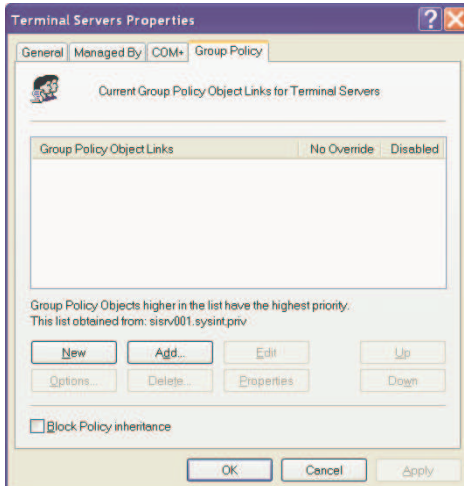CPUGuard with a Group Policy.

2.2.3.1 Installation

CPUGuard is delivered as a standard .MSI setup package. This package supports distribution
trough Active Directory Group policies without any modifications.
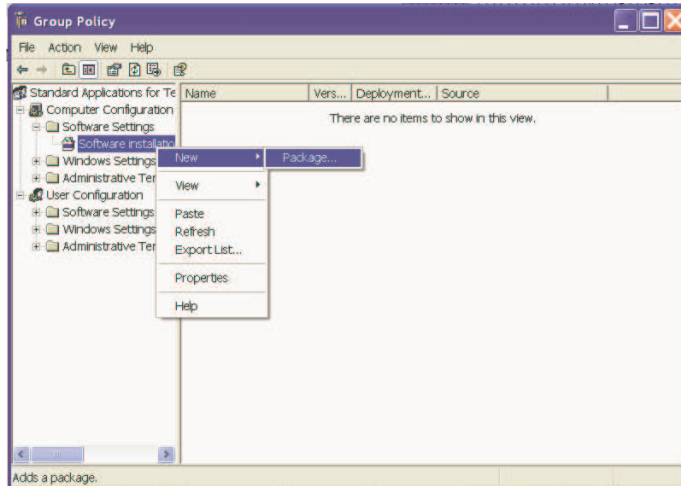
Start *Active Directory Users and Computers*.
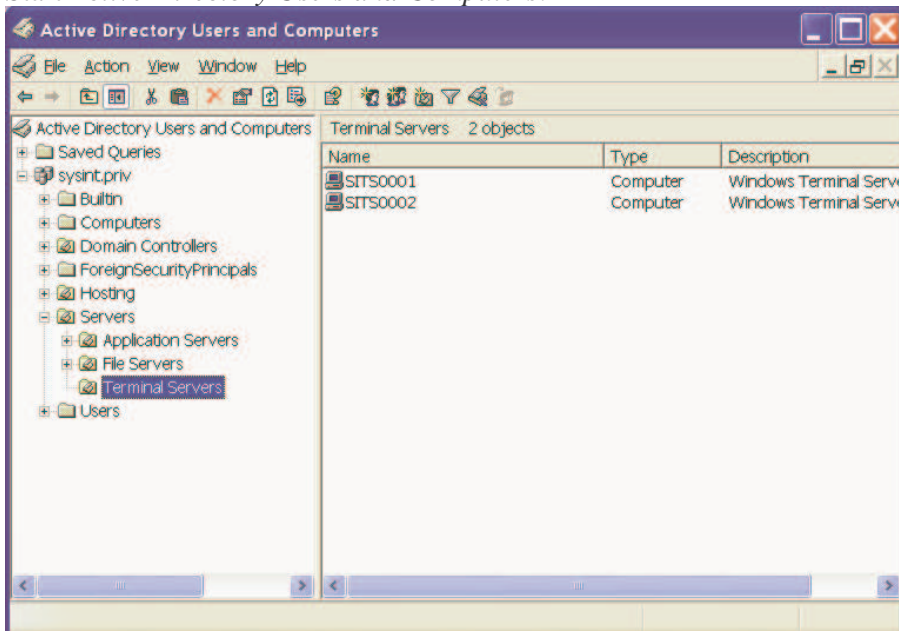
Right click on the OU where you want to place your Group Policy, and select *Properties*.
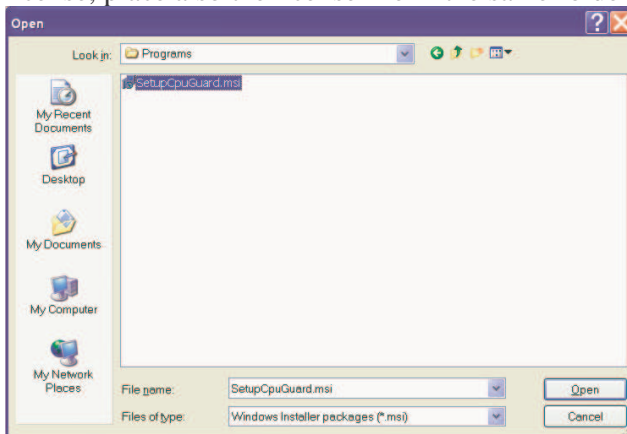
Create a new Group Policy Object, or modify an existing GPO.

Right click software installation in the GPO, and select *New -> Package*.
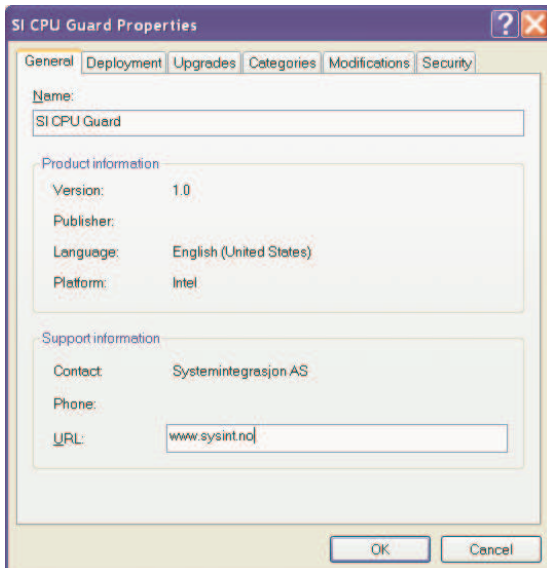
Place the installation package *SetupCPUGuard.msi* on a shared folder. For automatic installation of license, place also the license file in the same folder.
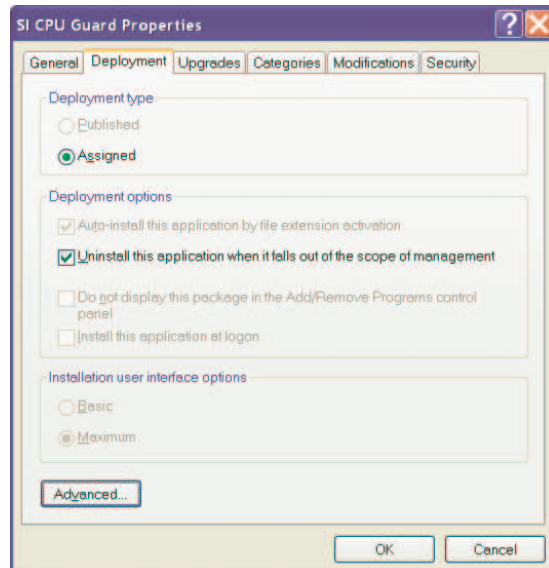

Browse to the folder where *SetupCPUGuard.msi* is located. Select the software package, and click *Open*.
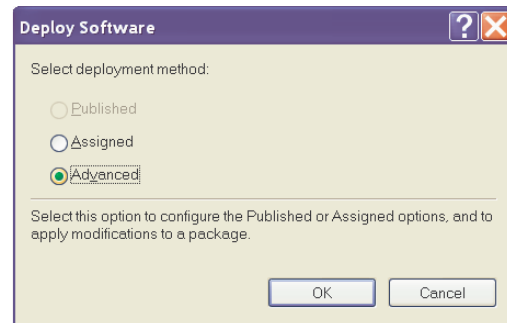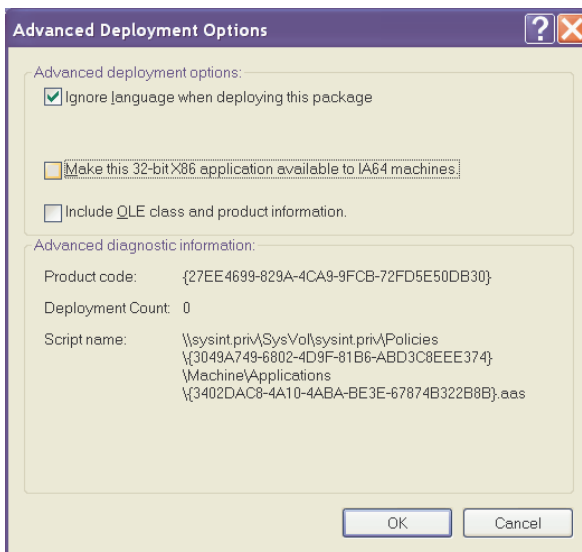
Select *Advanced*, and click *OK*.
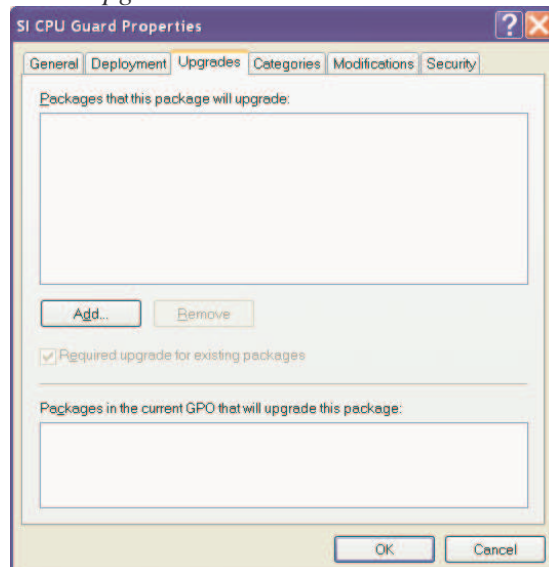
Name the package, and click *Deployment*.

Check that the settings look like this, and click *Advanced*.
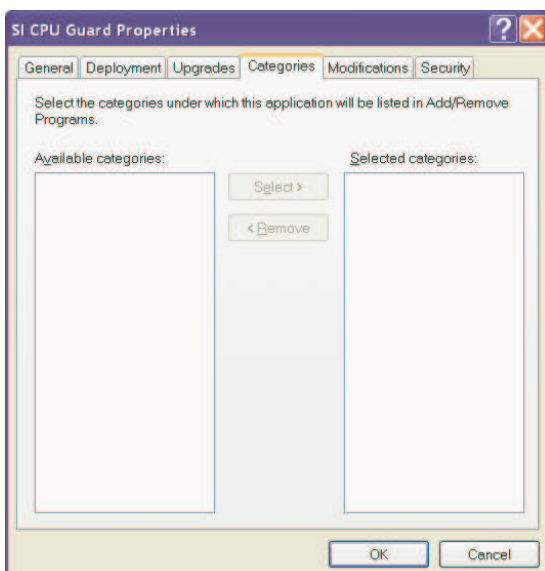

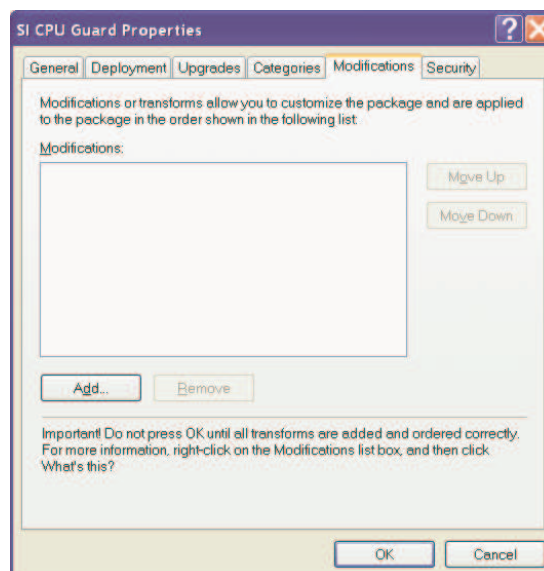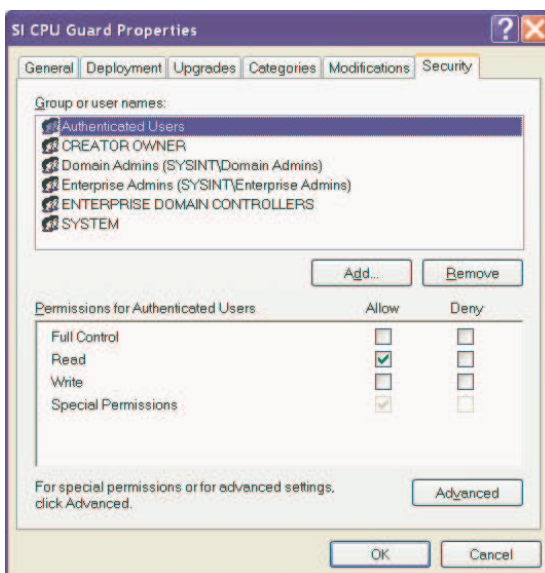Check that the settings look like this, and click *OK*.

Click *Upgrades*.

Leave the settings like this, and click *Categories*.

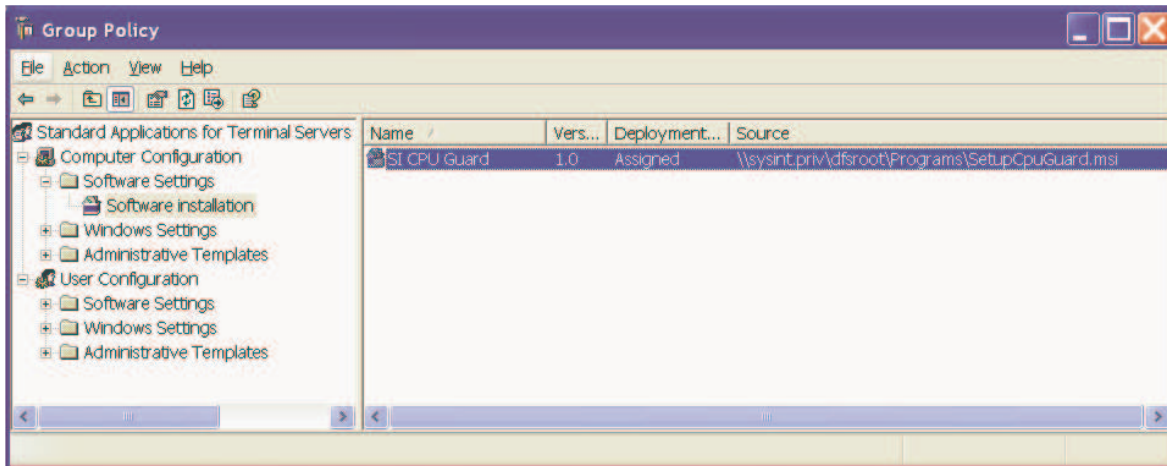**SI CPU Guard Properties**

General | Deployment | Upgrades | Categories | Modifications | Security

Select the categories under which this application will be listed in Add/Remove Programs.

Available categories:

Selected categories:

Select >

< Remove

OK   Cancel

Leave the settings as the dialog shows, and click *Security*.

SI CPU Guard Properties

General | Deployment | Upgrades | Categories | Modifications | Security

Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list.

Modifications:

Move Up

Move Down

Add...   Remove

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

OK   Cancel

Leave the settings as the dialog shows, and click *Security*.

SI CPU Guard Properties

General | Deployment | Upgrades | Categories | Modifications | Security

Group or user names:

Authenticated Users
CREATOR OWNER
Domain Admins (SYSINT\Domain Admins)
Enterprise Admins (SYSINT\Enterprise Admins)
ENTERPRISE DOMAIN CONTROLLERS
SYSTEM

Add...   Remove

Permissions for Authenticated Users   Allow   Deny

Full Control
Read
Write
Special Permissions

For special permissions or for advanced settings, click Advanced.   Advanced
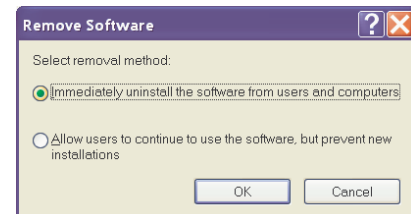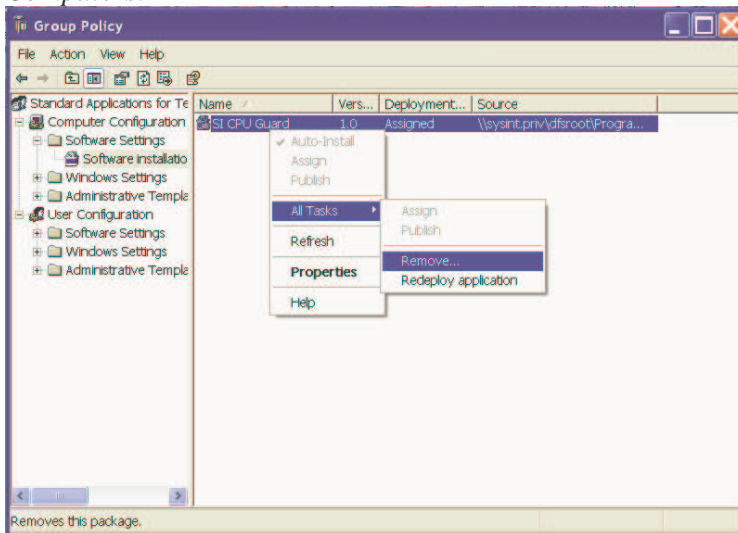
OK   Cancel

Change the security to follow your standards, or leave unchanged. Click *OK*.

CPUGuard will now be distributed via Group Policies, and installed during the next reboot on the computers which are in scope of this Group Policy.
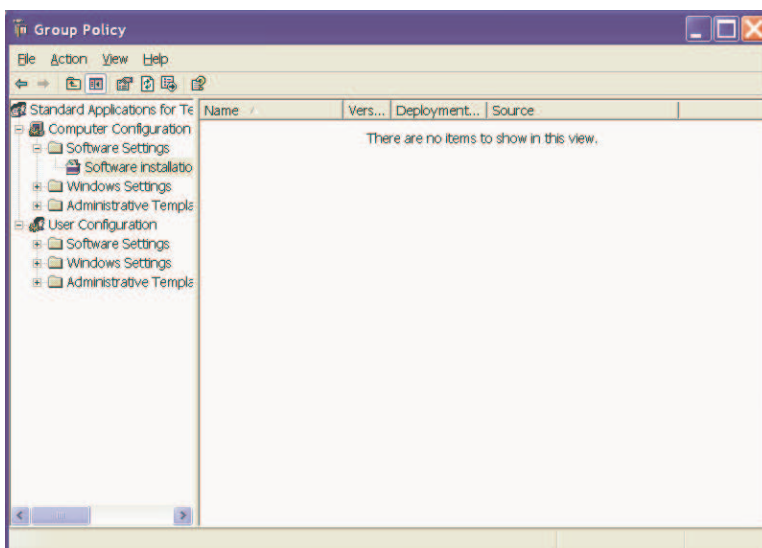
2.2.3.2 Uninstallation

Open the Group Policy via *Active Directory Users and Computers*.

Select *Immediately uninstall*, and click *OK*.

Right click CPUGuard software installation package, and select *All Tasks -> Remove*.

CPUGuard is removed from the policy, and will be removed from target computers on next reboot.

.

2.2.4 Installation from CPUGuard Administration console

CPUGuard can be pushed out to remote computers from the *CPUGuard Administation* console.
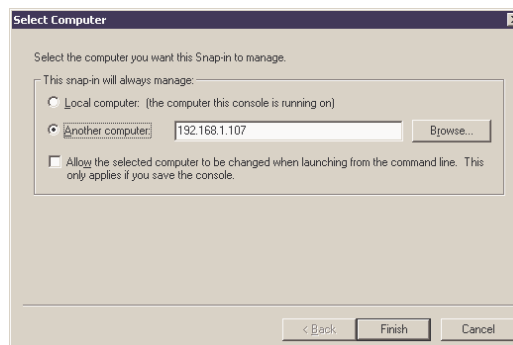
NB! To be able to perform installations from the admin console, the installation package SetupCPUGuard.msi must be placed in the program-folder where CPUGuard is installed on the computer where the admin console is run from!
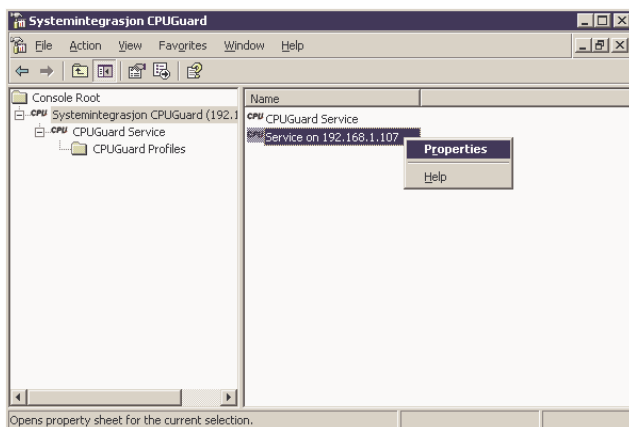
2.2.4.1 Installation
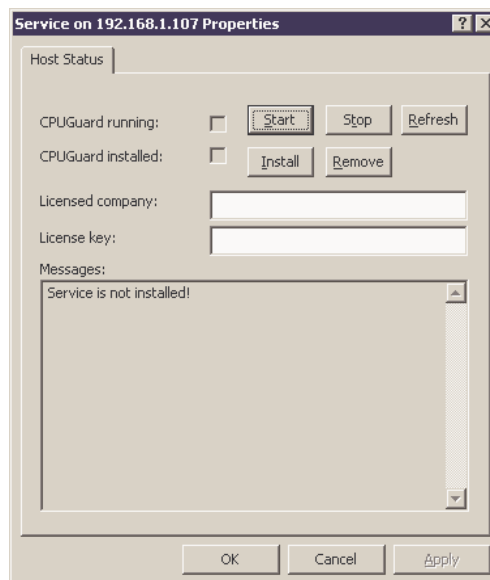
Open the *CPUGuard Administration* console
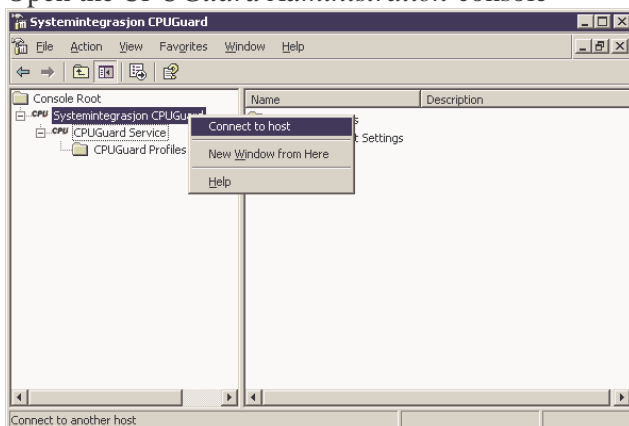
Right-click *Systemintegrasjon CPUGuard* and select *Connect to host*.
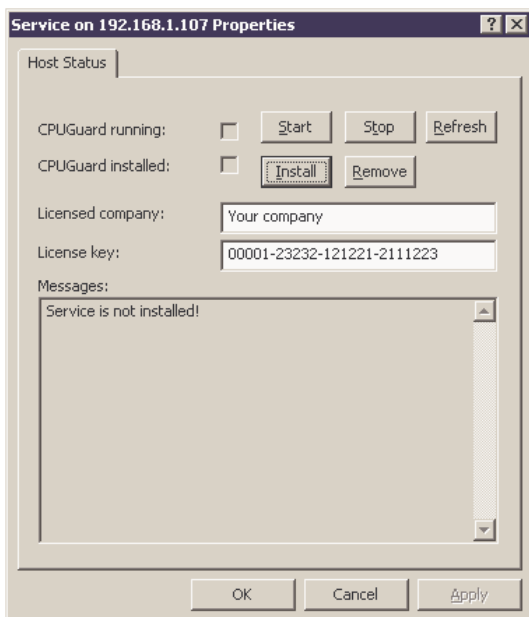

Enter hostname or IP-address of the computer to be administered, and click *Finish*.
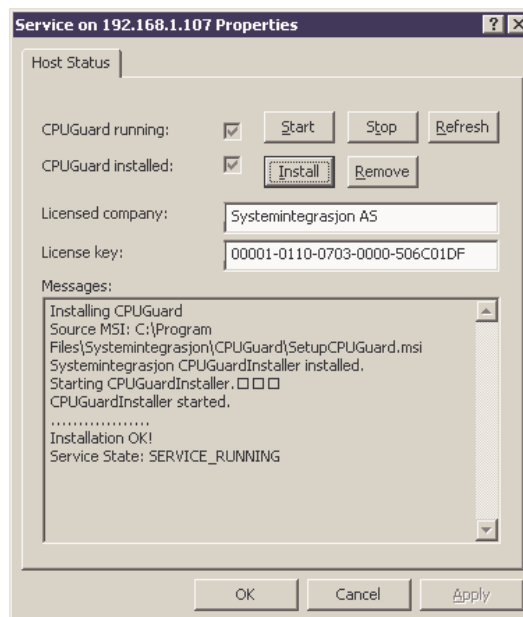
Right-click *Service on <host>* and select *Properties.*

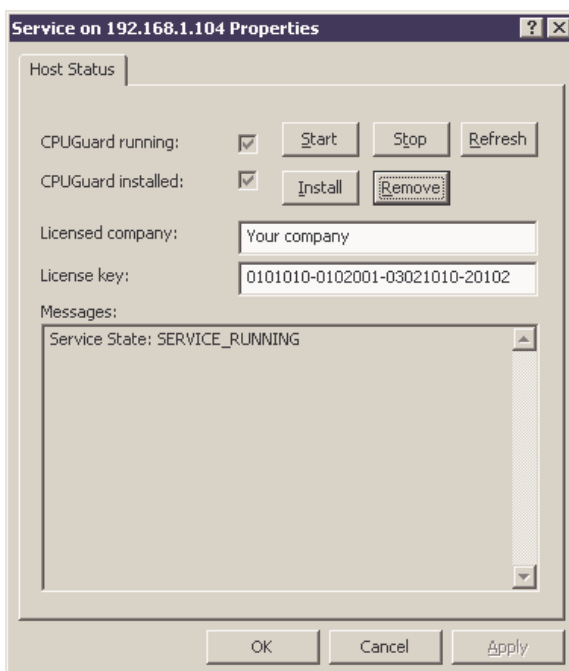Properties on target host are displayed.

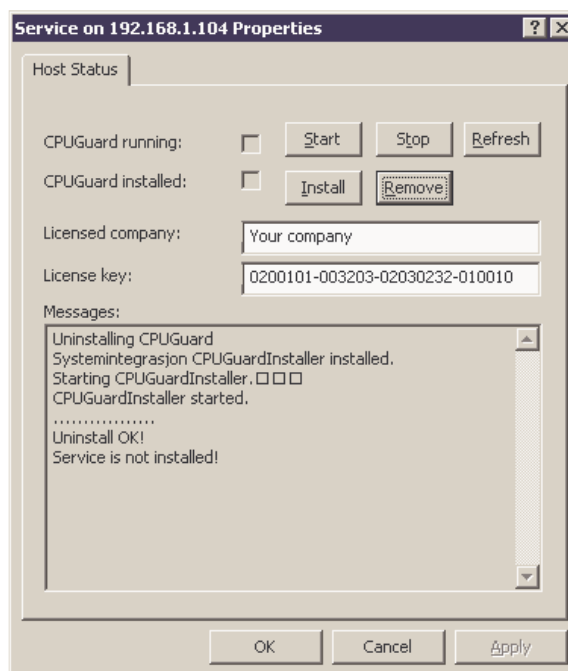Enter company and license information and click *Install.*

Verify that you get the status messages *Installation OK!* and *Service State: SERVICE_RUNNING.*

2.2.4.2 Uninstallation

Uninstallation can be performed from the admin console in the same dialog as installation.

Connect to the computer to administer, select *Remove*.

Check for the status messages *Uninstall OK!* and *Service is not installed!*.

2.2.5 Installation from CPUGuard command line utility

CPUGuard can be pushed out to remote computers via the CPUGuard command line utility *CGInstaller.exe*.

2.2.5.1 Installation

To perform a push installation of CPUGuard to a remote host, open a Windows command prompt an change directory to the folder where CPUGuard is installed. The command-line for pushing CPUGuard to remote computers will then be:

```
cginstaller -cmd push <target host> installmsi <path to setup file> <path to license file>
```

Example:
```
C:\Program Files\Systemintegrasjon\CPUGuard>cginstaller -cmd push 192.168.1.107
installmsi SetupCpuGuard.msi License.txt
```

2.2.5.2 Uninstallation

Remote uninstallation can be performed using *CGInstaller.exe*. The command-line for pushing removal of CPUGuard to remote computers will then be:

```
cginstaller -cmd push <target host> uninstall "Systemintegrasjon CPUGuard"
```

Example:
```
C:\Program Files\Systemintegrasjon\CPUGuard>cginstaller -cmd push 192.168.1.107
uninstall "Systemintegrasjon CPUGuard"
```

2.3 Verifying CPUGuard installation

To verify the installation of CPUGuard, you can check the event logs on your computers. All CPUGuard events are logged in the Application log.
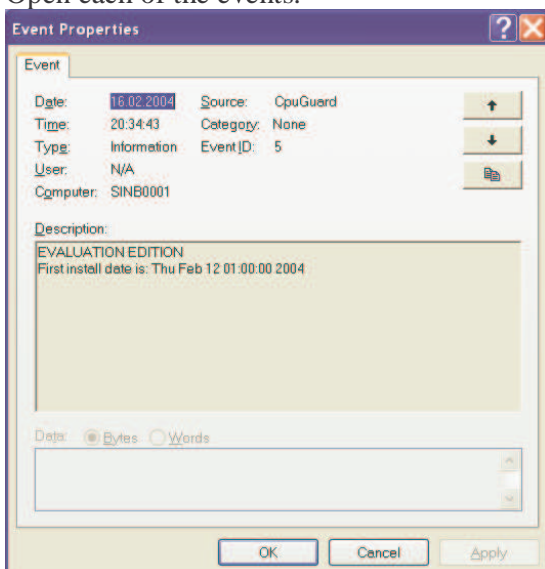
2.3.1 Verifying installation

Open the Event Viewer on the target machine where installation is to be checked:
Control Panel -> Administrative tools -> Event viewer.
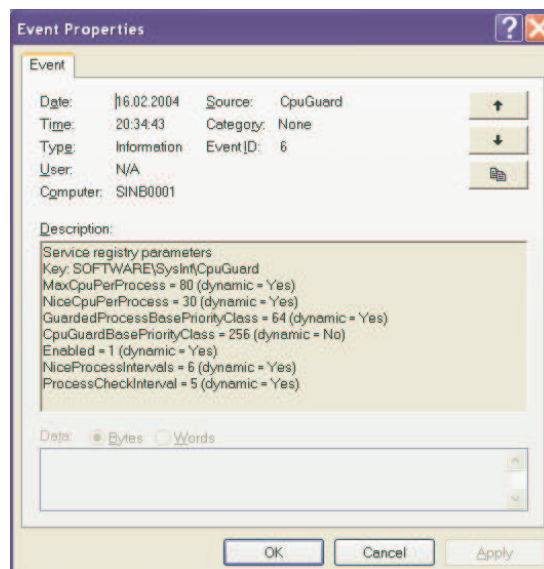
In your application log you should now find the following entries:
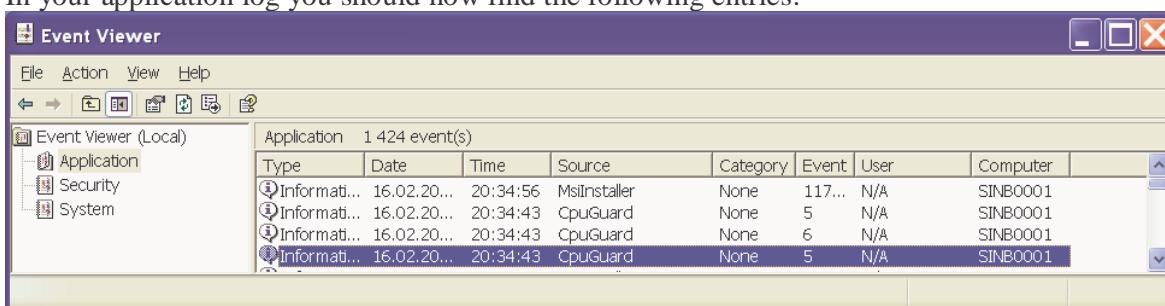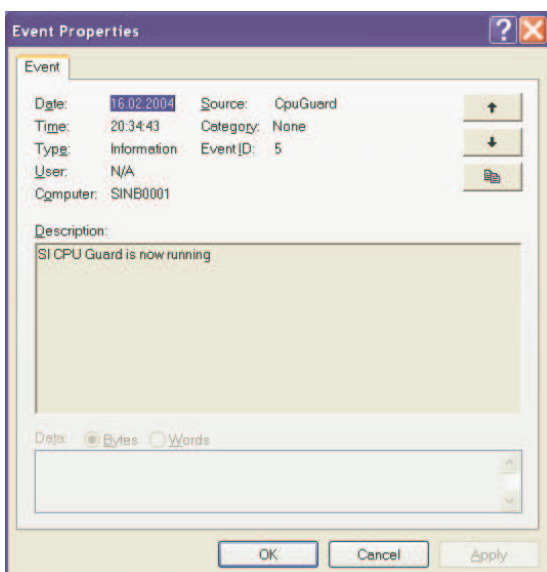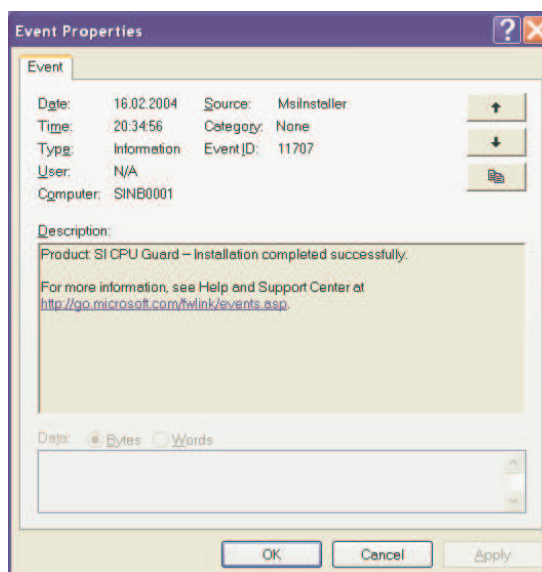

Open each of the events.

The first entry shows the type of license CPUGuard is installed with.

The next entry shows the default configuration CPUGuard is running under. Read the chapter *CPUGuard Configuration* for further explanation of the configuration parameters.
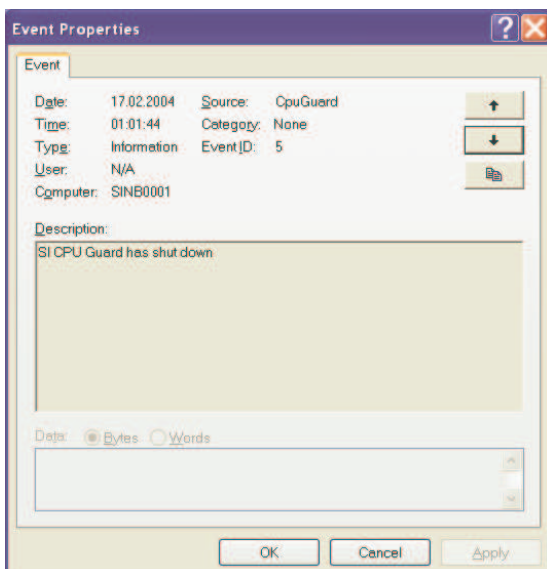
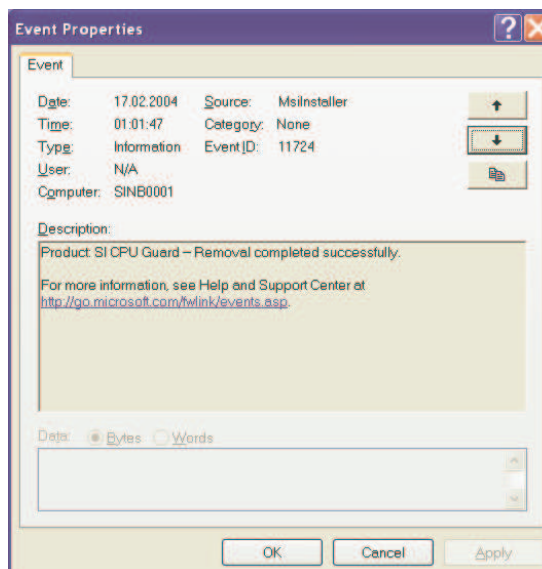This entry confirms that CPUGuard is running on the system.

The last event is from Windows Installer, and shows that CPUGuard is successfully installed.

2.3.2 Verifying uninstallation

Open the application log in the event viewer, and check for the following events:
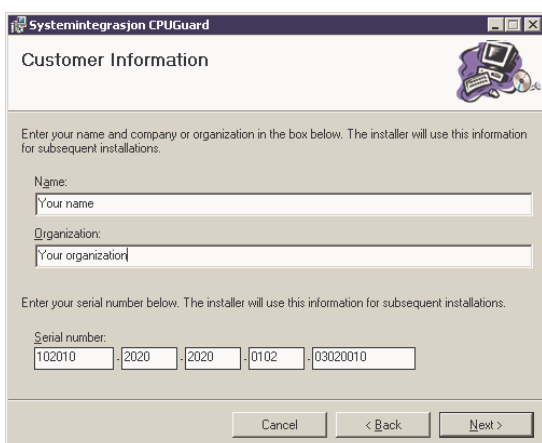

The service shuts down.

Product is removed.

2.4 Applying Licenses

Licenses can be applied to CPUGuard services in several ways. If changes are done to license information after installation, the CPUGuard service must be restarted after the change.
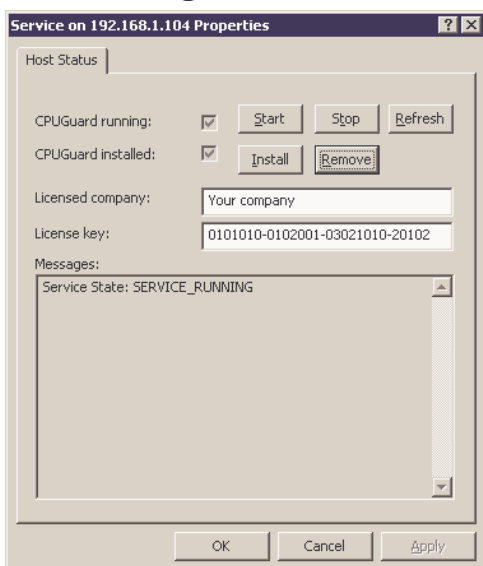
2.4.1 Installation wizard

The license key can be entered during installation.

2.4.2 Management Console

License key can be installed from the service properties dialog which can be opened from the CPUGuard management console.

2.4.3 License File

A valid license file can be put in either the folder where CPUGuard is installed from, or in the program folder where CPUGuard is installed.

3 CPUGuard Configuration

3.1 Overview

CPUGuard monitors CPU activity and memory usage on Windows systems.

3.1.1 CPU resources

If a process (a "CPU-hog") uses more than a set limit of CPU resources for more than a set number of seconds, CPUGuard lowers the processes base priority class for the CPU-hog to IDLE. In this way a CPU-hog will only consume CPU resources when no other process is demanding the same resources. If the CPU-hog reduces its demand for CPU to less than the set low-mark limit for a set number of seconds, the process will be restored to its original priority class.

The limits for how much CPU in percentage a process may consume, which base priority it is lowered to when the limit is exceeded, and how little CPU it must consume to be restored, are all configurable parameters.

3.1.2 Memory resources

The amount of working-set memory processes are allowed to consume, is configurable via CPUGuard. The default behavior is such that processes may consume more than the set maximum limit of memory, if free memory resources are available. This is controlled by the operating system. For Windows Server 2003, an option for strict enforcement of memory limits is available.

3.1.3 Locking processes to specific CPUs

CPUGuard may also be used to lock certain processes to one or more CPU's. This may be very advantageous for applications which are licensed according to the number of CPU's in the server.

By locking the processes of the application to for example one CPU, the application runs on only one CPU, and one should be eligible for a cheaper license. This is of course dependant upon approval by the software vendor. Some applications may check the number of CPU's in the machine on startup instead of checking the number of CPU's actually in use. This problem should be addressed to the vendor in question.
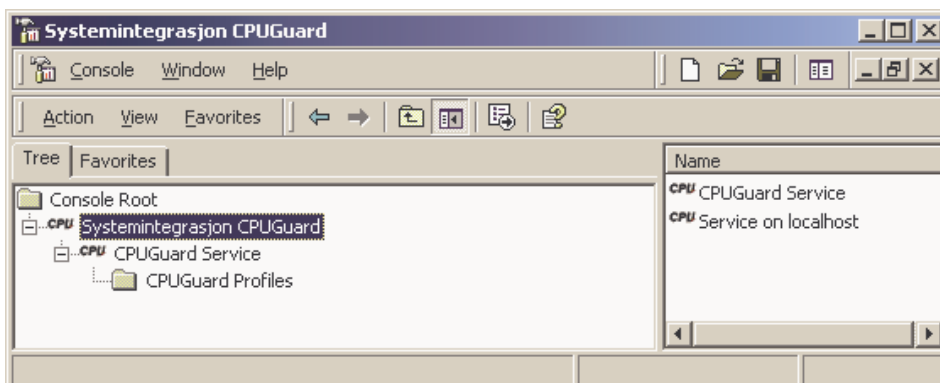
Another use for this feature is for processes which are very eager to use all the CPU it gets it hands on. By locking it to one or a few CPU's, one in effect throttles the process down.

This mechanism both works for multi-CPU machines and for Pentium 4's with Hyper-threading capability.

3.2 Ways to configure

There are three ways to configure CPUGuard:

- Using the Systemintegrasjon CPUGuard MMC (Microsoft Management Console) snapin
  - o Manages Local Settings
  - o Both remote and local configurations

With the CPUGuard MMC you can configure the local service, or connect to and manage CPUGuard services on remote computers.

- Using the Group Policy Editor
  - o Manages Policy Settings
  - o Both in Active Directory GPO's and local policies
  - o Not for Windows NT 4
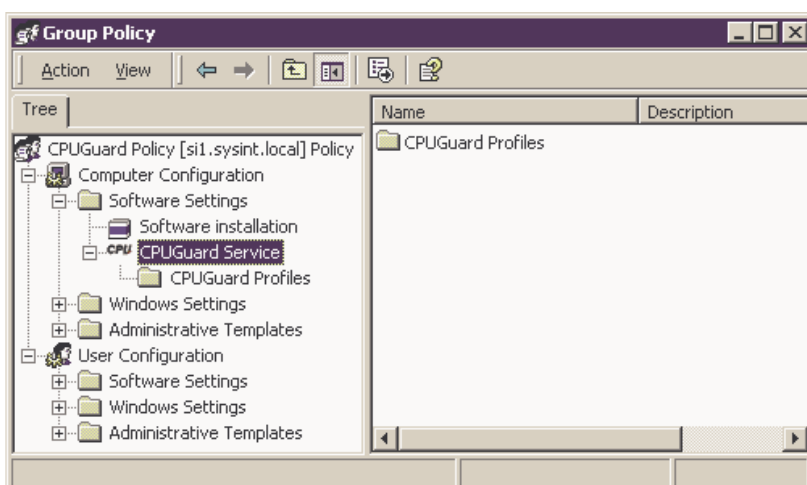
CPUGuard registers itself automatically as an integrated part of Active Directory Group Policies.

- Using the Computer Management MMC snap-in
  - Manages Local Settings
  - Both remote and local configurations

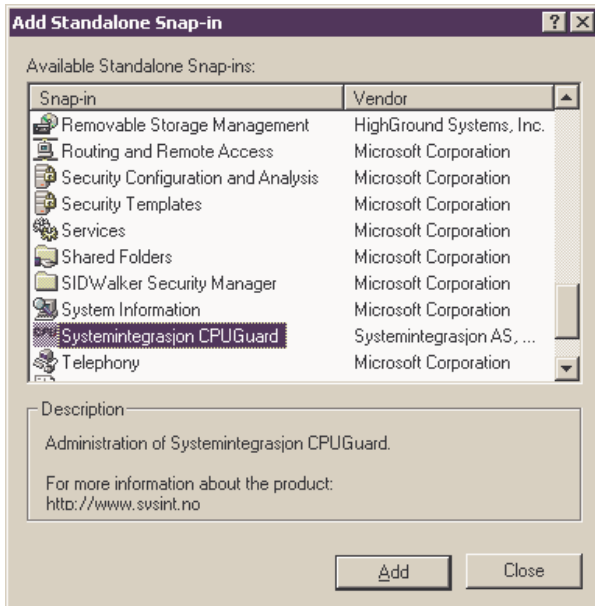A standard MMC can be updated with one or more instances of the CPUGuard snap-in.
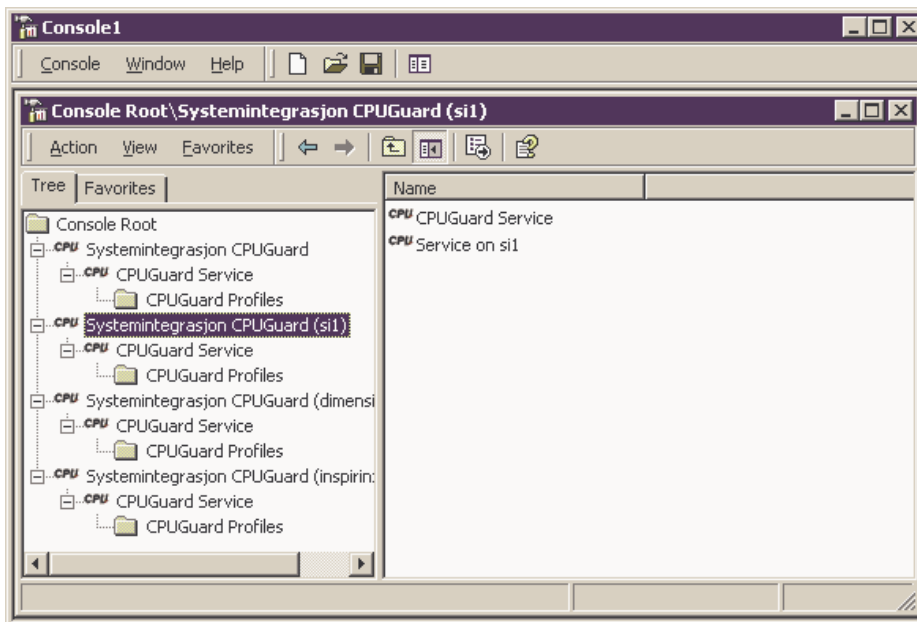
If several CPUGuard snap-ins are added, services on several different computers can be easily managed without having to reconnect to each computer every time you need to switch from one computer to another.

3.3 Application of Configuration Settings

As all well-behaving software, CPUGuard may be configured both with Local Settings and with Policy Settings. CPUGuard also has a model where you may define Profiles which may apply to certain processes (more of this later in the document). The different configurations are read in this order: Local Settings is read first and then Policy Settings. This means that Policy Settings will take precedence over Local Settings, whenever defined.

Regarding Profiles
Profiles from Policy Settings take precedence over Profiles with the same name from Local Settings. Local Profiles without name-collision will be read and applied, even if Policy Settings is used.

If the Policy Settings, either Local Policies or Group Policy Objects, goes out of scope, the program will revert to using Local Settings, or using program-builtin settings, if no settings is defined.

Application of configuration settings changes is almost instantaneous for Local Settings, and Policy Settings are applied as soon as the operating system applies the policy on the computer.

All matching of processes to Profiles or default settings is done again whenever there is a configuration change. CPUGuard is fully dynamic regarding configuration settings, without need to restart the service or even less the computer.
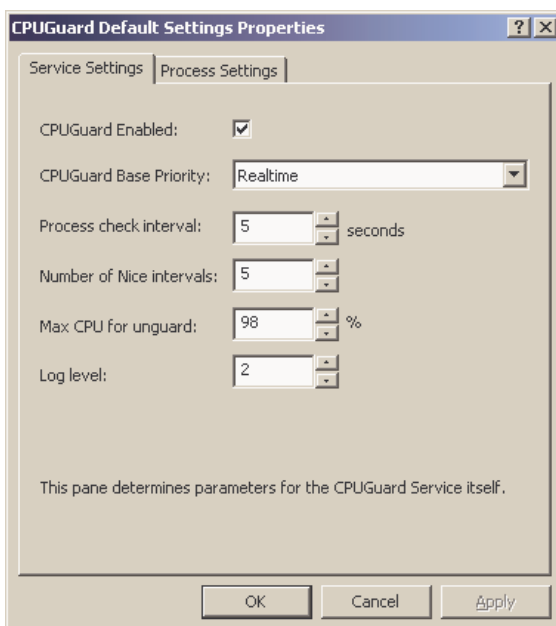
3.4 CPUGuard Settings

CPUGuard settings can be configured through the default settings. These settings will be valid if they are not overridden by policy settings.
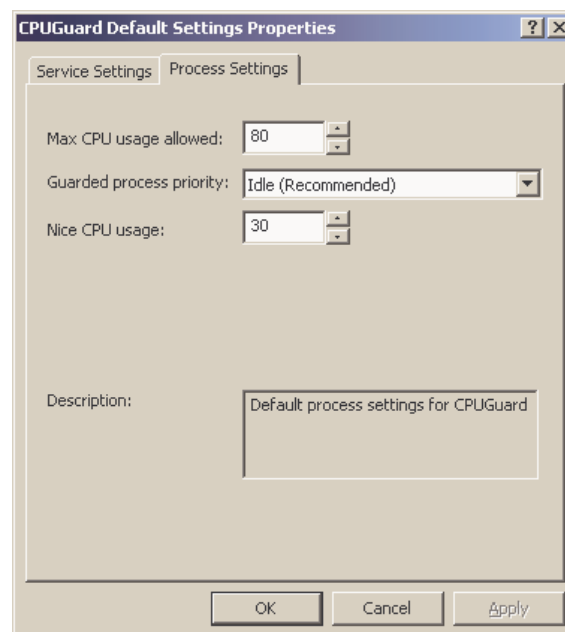
To configure CPUGuard default settings, start the CPUGuard Administration console.
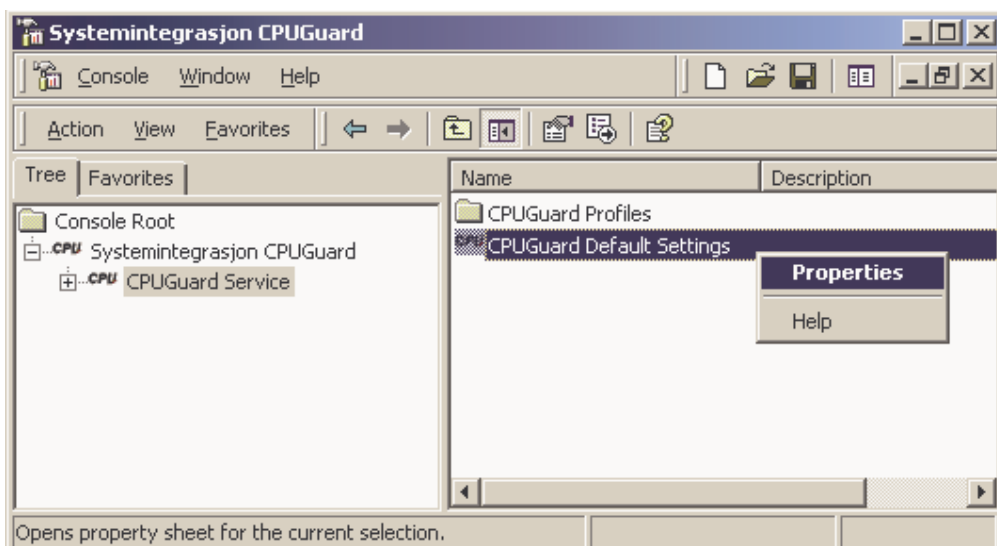
Browse to *CPUGuard Service*, right-click *CPUGuard Default Settings*, and select *Properties*.

The options on the pane *Service Settings* define the behavior of CPUGuard. For details, read the section **Settings** in this document.

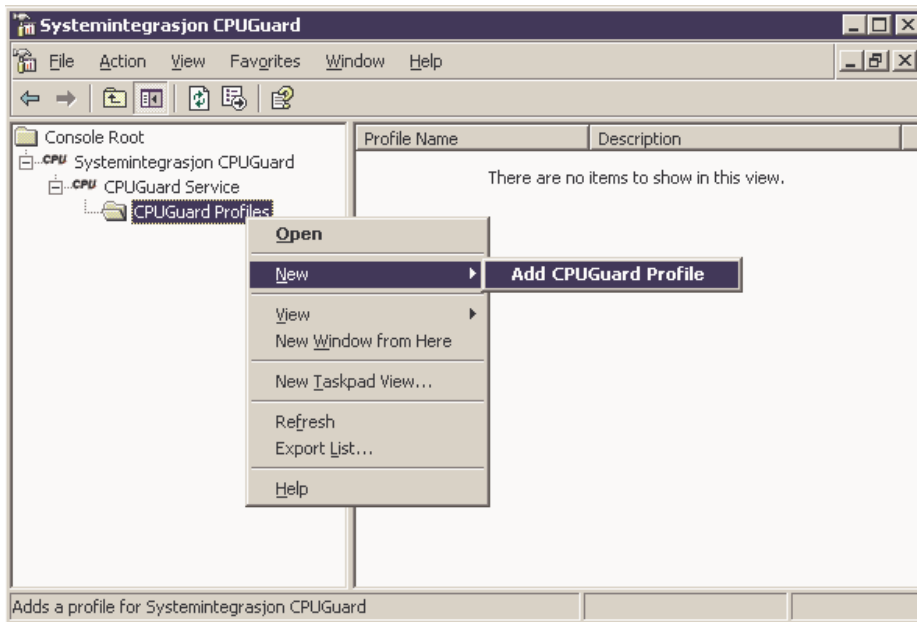Options on pane *Process Settings* define CPUGuard behavior on processes.

3.5 Advanced settings with profiles

Advanced configuration of CPUGuard is done via profiles.

To configure CPUGuard profiles, start the CPUGuard Administration console, and browse to CPUGuard Profiles.

Right-click **CPUGuard Profiles**, select **New** -> **Add CPUGuard Profile**.
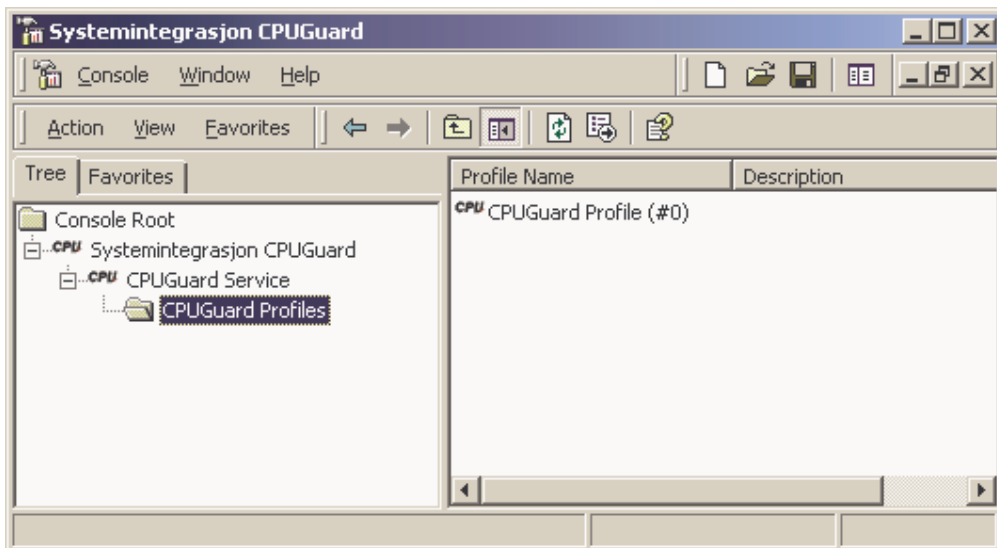
A new CPUGuard profile is created.
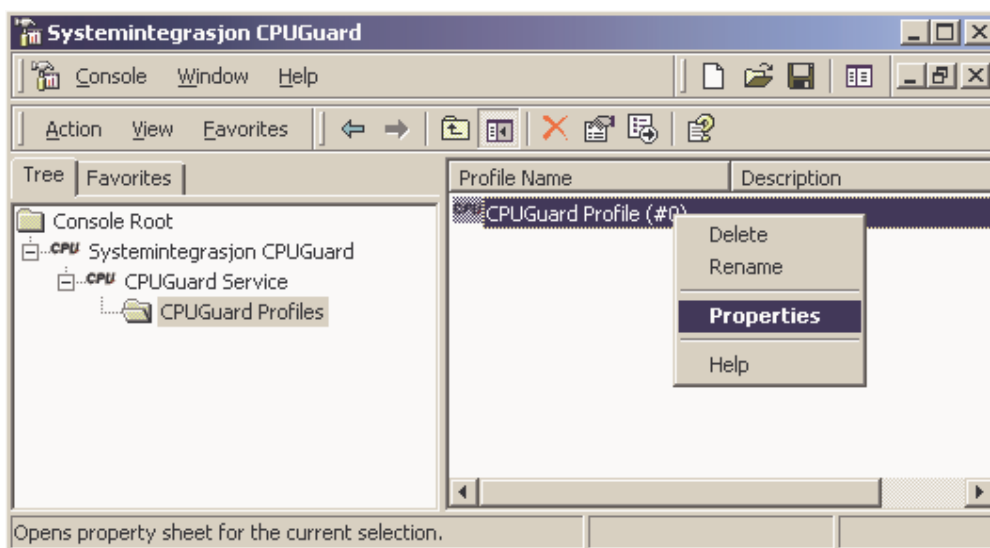
Right-click the new CPUGuard profile and select *Properties*.
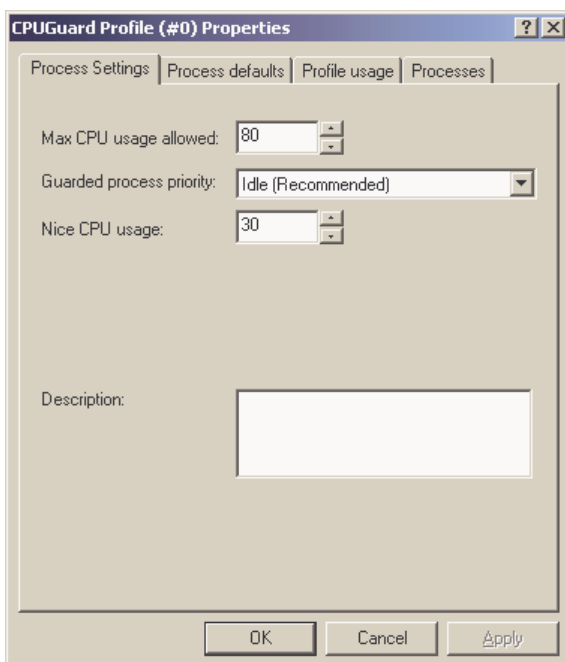
Options on pane *Process Settings* define CPUGuard behavior on processes. For details, read the section **Settings** in this document.

Options on pane *Process Defaults* define default settings for guarded processes.

CPUGuard Profile (#0) Properties

Process Settings | Process defaults | Profile usage | Processes

Name   Add...

Everyone   Remove

Permissions: Allow   Deny

Apply Profile   ☑   ☐
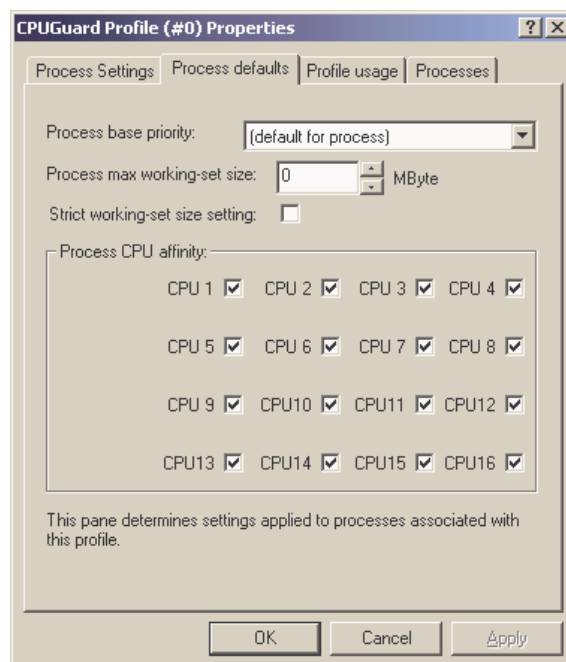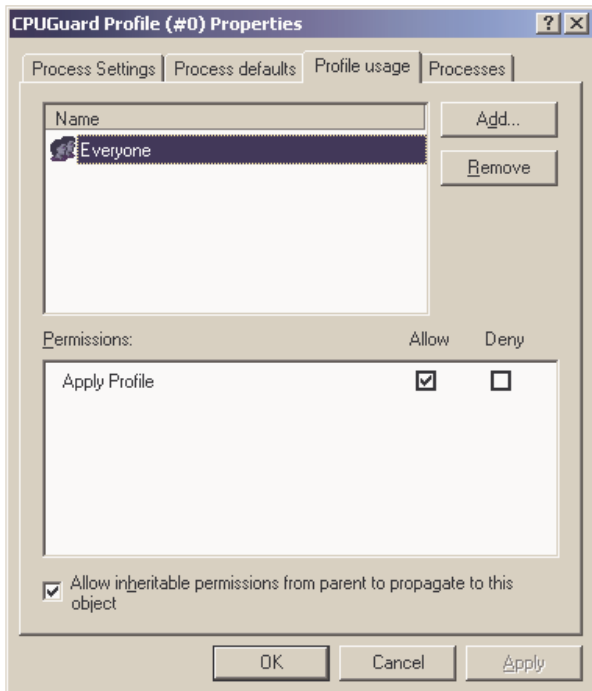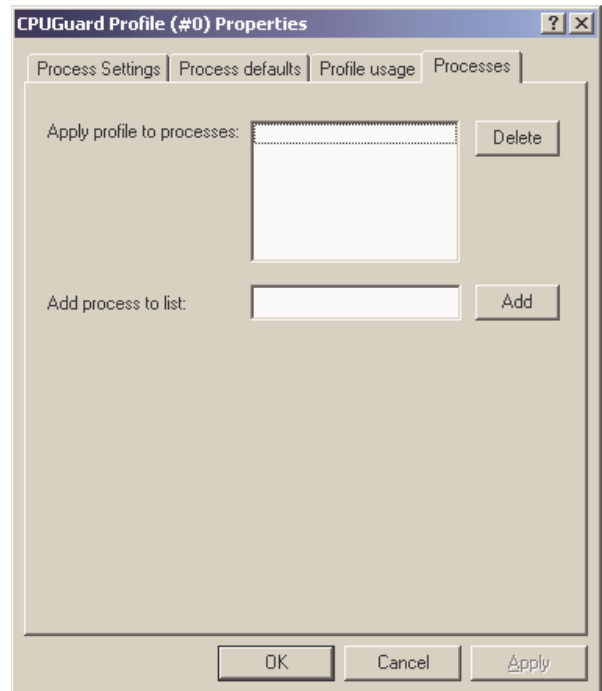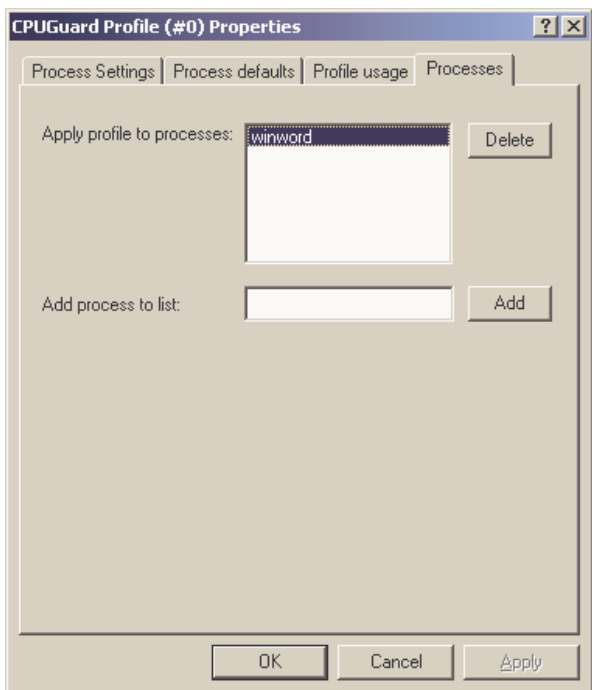
☑ Allow inheritable permissions from parent to propagate to this
   object

OK   Cancel   Apply

CPUGuard Profile (#0) Properties

Process Settings | Process defaults | Profile usage | Processes

Apply profile to processes: Delete

Add process to list: Add

OK   Cancel   Apply

Profiles can be limited to specific users or groups, or applied to everyone.

By default a profile is applied to all processes for the users or groups it is defined for.

CPUGuard Profile (#0) Properties

Process Settings | Process defaults | Profile usage | Processes

Apply profile to processes: winword   Delete

Add process to list: Add
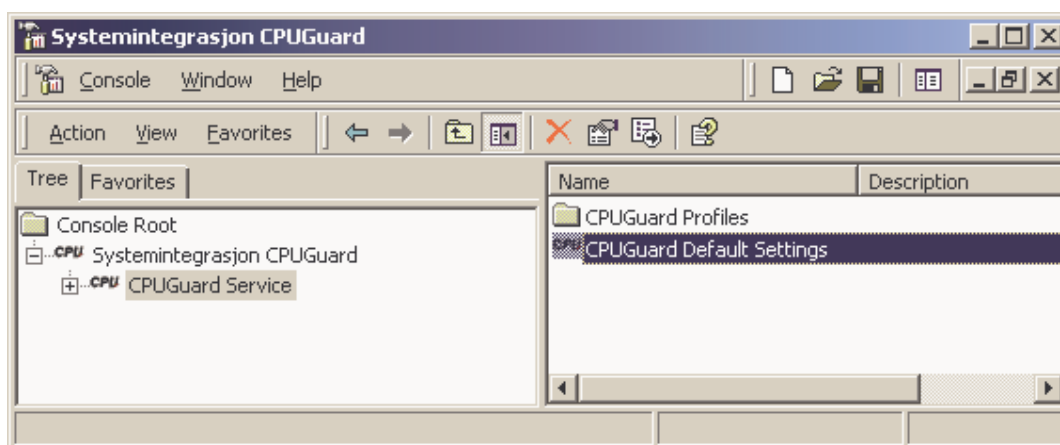
OK   Cancel   Apply

Profiles can be defined to apply only to specific processes. If both users and processes are defined for a profile, both criteria must match for the profile to be applied.

3.6 Validation of profiles

Multiple CPUGuard profiles may be defined.
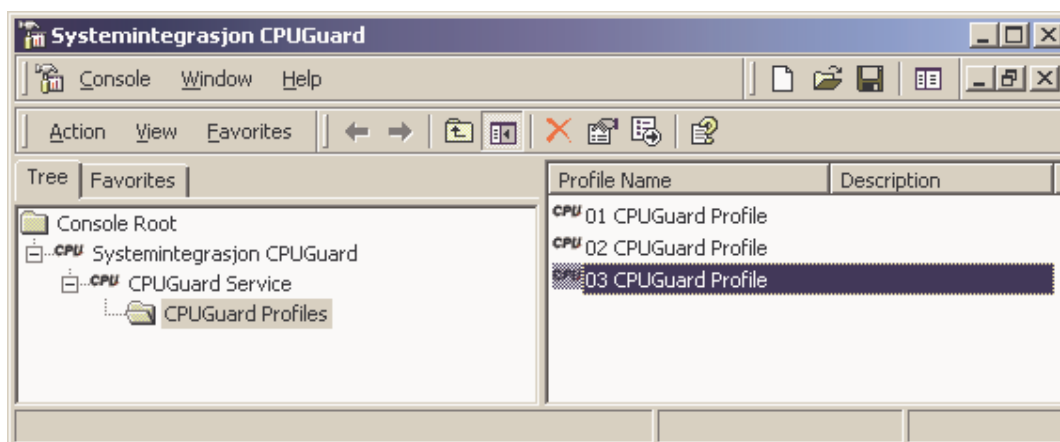
- CPUGuard profiles will be validated in alphabetical order.
- Profiles defined in Group Policies will be validated before local policies.
- The first profile that is matched to a process will be applied, and no more profiles will be validated for the process.
- If no profile is matched to a process, the **CPUGuard Default Settings** will be applied.

3.7 Settings

This section explains the options found in CPUGuard configuration dialogs.

CPUGuard Enabled	Enables or disables the CPUGuard service.
CPUGuard Base Priority	Sets the priority for the CPUGuard service.
Process Check Interval:	The interval between each check of process resource usage.
Number of Nice intervals	The number of intervals a process must consume less than the set "Nice CPU usage"-limit.
Max CPU for unguard	The maximum percentage CPU usage that can be consumed when unguard of processes will be performed.
Log level	Sets log level for logging to the Windows Application Log
Max CPU usage allowed	The percentage limit where CPUGuard takes action and reduces the base priority of a process.
Guarded process priority	The base priority a process will receive if it exceeds the set limit.
Nice CPU usage	If a guarded process uses less than this percentage limit, CPUGuard restores the process to its original priority class.
Process base priority	The base priority for guarded processes.
Process CPU affinity	Defines which processors guarded processes may run on.
Process max working-set size setting	The number of MB of working-set guarded processes may consume.
Strict working-set size	This setting enforces strictly the set limits for max working set size, even if free memory working-set resources are available. This setting is only supported on Windows Server 2003.