

User Guide

Vexira Antivirus Central Management Solution





TABLE OF CONTENTS

VEXIRA ANTIVIRUS CENTRAL MANAGEMENT SOLUTION	4
Introducing the CMS System	4
Minimal System Requirements	5
Installation	6
Installation with Parameters.....	6
If the Installation Has Not Started... ..	6
Removal, Modification, Reparation	6
Starting from the Start Menu	7
MMC Console	8
Starting the Console	8
Handling Installed Products.....	8
Options, Setting Parameters.....	9
Discovering the CMS	12
Installation Template and Configuration Template	12
Groups.....	12
SubCMS	12
CMS – A Possible Structure	12
Automatic Monitoring Tasks	15
Browsing for Active Computers in the Network	15
Listing the Status of Protection on the Managed Computers	15
Installer/Uninstaller	15
Registration Status	15
Replication.....	16
Network Browser	16
Structure	17
CMS MANAGEMENT MODULES	18
Management	18
CMS System – Default Settings	19
Groups Folder.....	20
Templates.....	20
Subtree Folder.....	23
Timetable.....	24
Network	26
Handling Domains and Workgroups.....	26
Non-managed Computers	31
List of Assigned Computers.....	31
General Settings	33
Machine Management	33
Installation Management.....	33
License Management	33
Automatic Assignment of New Machines	34
Local Menu	35
Filter.....	37
Product Versions	39
Uninstallation	40
Install Copier	41
Source Settings	41
Tasks	41
Event Logs	43
Reporter	45
License Manager	48



LOCAL SETTINGS	49
General Settings	49
Security Context for Network Connections	49
General Settings	49
SMTP Client.....	49
Log Settings.....	50
Additional Scan Settings.....	50
Log	51
Central Alert.....	52
Task Manager	54
Tasks and Task Settings	54
Registration	57
Updater	58
Source Settings	58
Tasks	59
END USER SOFTWARE LICENSE AGREEMENT	60
CONTACT	62



VEXIRA ANTIVIRUS CENTRAL MANAGEMENT SOLUTION

Vexira Antivirus Central Management Solution (CMS) provides a real and comprehensive central controlling and monitoring option on Windows networks. With the help of CMS, corporate networks can have a suitable up-to-date protection that requires a minimal level of maintenance.

With the help of automatic central installations, updates, configuration and license management, protection of servers and workstations can be controlled effectively saving a lot of time. You can receive comprehensive reports in e-mail and the status of the virus protection on the whole network can be checked in a second any time. The MMC-based user interface helps in checking and handling all settings and functions in a matter of minutes.

Introducing the CMS System

One of the main advantages of CMS is that it can be applied to almost any network structure. It supports multi-level management systems if the physical or logical structure of the network requires it. Companies with several sites can manage their antivirus protection at all sites from their headquarters. The separate levels of the system communicate with each other according to the settings and are capable of replicating installation packages or templates automatically to centralize updates, installations configurations and registrations.

Some services provided by CMS:

- **Installation and configuration groups**
With the help of these groups, the elements and settings needed for the protection of a specific group of computers, which is automatically installed, updated and applied on all of the computers, which have been assigned to the group. The computers can be added to the group either manually or automatically. With the help of configuration management, the configuration of specific computers in the network can be managed; therefore the protection of computer groups operates according to the same settings.
- **LDAP support to create computer groups**
Selectable rules make sure that machines are added automatically to the protection system. The security product for the given operating system is installed without human intervention. The rules can be custom-made, machines can be assigned not only according to their operating systems, but rules can be created according to all the attributes available in LDAP (for example, machines inactive for a long period are not assigned).
- **Supervision of Windows workgroups and domains**
Centralized supervision of several, different workgroups and domains.
- **Central monitoring and logging**
Beside the versions of the installed products, you can obtain information about the configuration, the operating system of the machines available in the network and the possible active or deleted infections.
The product logs the events and incidents in set categories (for example, malware incidents, quarantine events, and so on). Custom-made filtering can also be applied to the event logs. The separate log of a managed machine is also available.
- **Central updates**
You can select the type of report to appear in the product or to be sent in pdf format as an e-mail attachment to the specified recipients. You can easily create reports about the status of the managed machines, the licences used, the possible errors, or the malware detected in the network with the help of predefined reports (for example, about the most infected machines, the most frequently detected malware, or the complete list of detections).
- **Easy-to-use interface, detailed reports**
The whole network's security updates can be performed from a single source automatically. The system updates the set installation kits and updates managed clients from these. Only modules



Vexira Antivirus Central Management Solution

set in the installation template are updated on each client so as to avoid performing useless actions and unnecessary network load.

- Reliability, performance
To increase performance and to avoid unnecessary network load, the number of parallel installations and the date of the updates of the separate products or the virus database can be set. This guarantees that our solution does not use more resources than needed.
- Complete support
Central Command, Inc. provides complete technical support for the products with high quality. Our support services enable the creation, maintenance, and even the efficient troubleshooting of effective antivirus protection for the users. Customers can request professional assistance easily via e-mail, on the phone.

Main features of the product:

- The central management and monitoring of the protection of the network from a single computer
- Supports multi-level management systems
- MMC-based, clear and easy to use user interface
- Installation groups for easy installations and updates
- Central configuration and registration
- Pre-defined and custom-made reporting that appears on the GUI of the product or can be sent as an e-mail attachment in pdf format
- Automatic updates on the network from a single source
- Task-oriented operation
- Central logging
- Supports multi-language installations in the same network

Minimal System Requirements

The following system requirements must be available to execute the program:

Processor	400 MHz (x86/x64)
Supported operating system - memory	Windows 2000 Server* - 256 MB Windows Server 2003/2008* - 512 MB <i>*The product can work on NT based workstations as well. It is recommended to install the latest Service Pack and use at least 1024 MB memory depending on other applications running on the system.)</i>
Free hard disk space	100 MB + ~600 MB working disk space (it can take even more disk space (depending on the size of the managed system))
Browser	Internet Explorer 6
Other	If you need more information, check the readme.txt file – it is in the installation kit. <i>Vexira Antivirus Remote Admin Client</i> must be installed on client computers running Windows 98se/Me operating system so that CMS can manage them.



Installation

Note!

Make sure that your computer is virus free before installing the software.

The antivirus software can only operate properly if it was installed on a virus free computer. Perform a virus scan on the computer with the help of Vexira Antivirus Scanner's latest version, which can scan the whole system for viruses in a fast and easy way. You can download information about the product from Central Command, Inc.'s website.

The product can be installed from a self-extracting archive ([wincms.exe](#)). After executing the file, the installation package will be decompressed and installation will be started.

To be able to install the product, read the *CMS – Installation Guide*. The document can be downloaded from Central Command, Inc.'s website.

Installation with Parameters

By specifying parameters after the installation file, other installation modes can be enabled that are not available during regular installation. You can find information about these parameters and installation modes in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product.

If the Installation Has Not Started...

Check that your computer fits all minimal system requirements. Check if your system has all the needed system and program components. Without these, installation cannot be performed and an error message informs you about the needed system component that is required in your computer before installing the antivirus software. You can find detailed information about this topic in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product.

Removal, Modification, Reparation

If you want to remove Vexira Antivirus from you computer or modify the installed components or reinstall installed components, perform the following:

1. Click on the *Add/remove program* icon on the *Control panel*.
2. Search for the product to be removed from the list and select it.
3. Click on the **Modify/remove** button.

You can select the needed operation in the window that is displayed:

- *Modify*
If you select this option, a component list appears after clicking on the **Next >** button. By selecting or deselecting components in the list, you can add new components or remove installed ones. The needed operations (installation/removal) are performed after clicking on the next button.
- *Repair*
Reinstalls installed components.
- *Remove*
Uninstalls all installed components from the computer.



Starting from the Start Menu

The Vexira Antivirus Central Management Solution is available under Start / Programs / Vexira Antivirus CMS after installation. All the shortcuts related to the product are placed here, the software can be started here and product-related documentation can also be opened from this menu.



MMC Console

The advantage of Microsoft Management Console (MMC) is that experienced users can perform tasks in the hierarchical system in a matter of minutes and modifying settings and configuration is much easier.

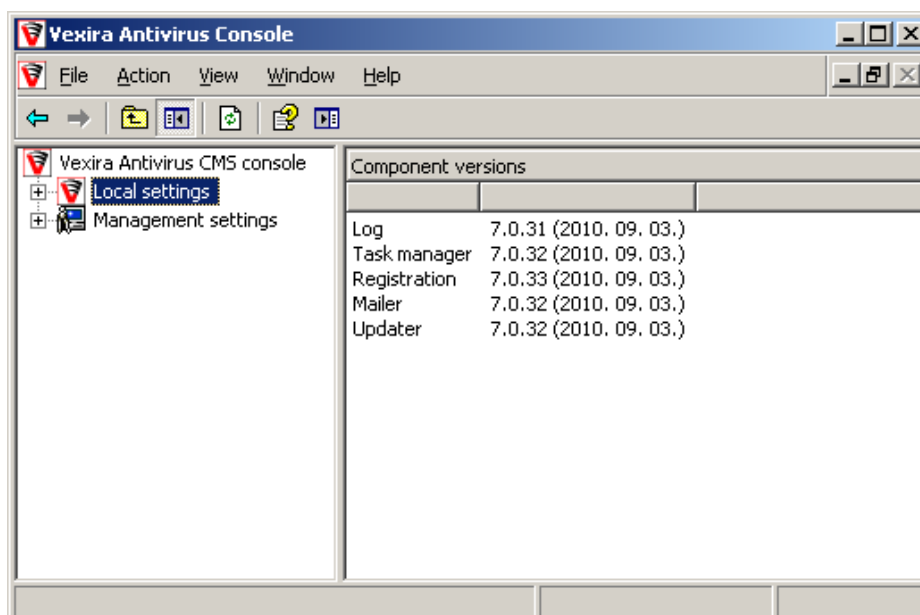
Starting the Console

To start the MMC user interface, start the 'Vexira Antivirus CMS Console' program from the *Start menu* (Start menu / Programs / Vexira Antivirus CMS / Vexira Antivirus MMC Console (CMS)), and the MMC console elements are displayed in a parent window (Vexira Antivirus CMS Console). This window contains the menu and the toolbar with commands to open or create additional consoles and to save them. When launching the product, the parent window already contains the Vexira Antivirus CMS console window where you can access the product settings.

Handling Installed Products

The settings of the products are shown in the console tree. General modules of the product are located in the *Local settings* node. Click on the *Management settings* node to display the following in the right-hand (details) window:

- [Product version](#)
It displays the version number of the installed product.
- *Discovered computers*
It displays the number of computers discovered by the CMS in the network.
- *Managed computers*
It displays the number of machines that are managed by the CMS in the network.
- *SubCMS*
It displays the number of machines that function as SubCMSs in the system.
- *Free licenses*
It displays the number of purchased licences that are not used for installing antivirus products on the machines in the network.

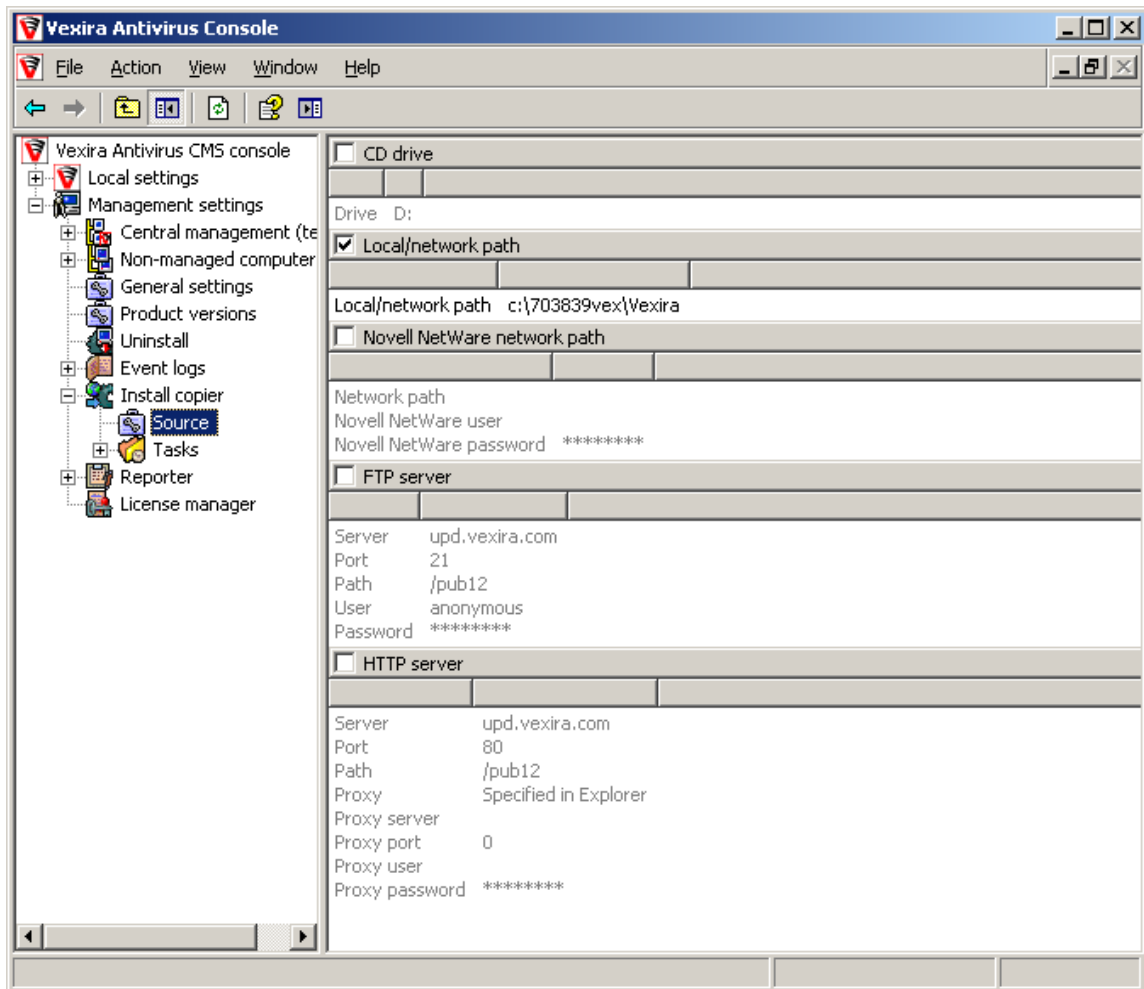


An Installed Product and Its Module Versions



Vexira Antivirus Central Management Solution

To access module settings, click on the plus (+) sign in front of the name of the module, and the settings groups are displayed under the module.



Module Settings

By clicking on the settings groups under the module, the module settings are displayed in the details window. You can modify these by double-clicking on the selected option or by right-clicking on the option and choosing Modify from the local menu. Other functions in the local menu are detailed in the description of each module.

Important!

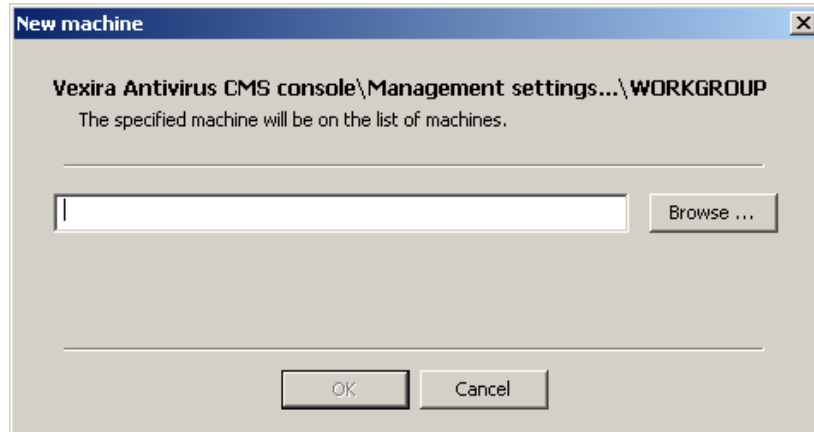
Some of the settings or options above general options can only be accessed in the local menus.

Options, Setting Parameters

You can access the settings of each module by specifying the needed options in the details window. The options can be modified in two ways:

- Double-clicking on the name of the setting
- Right-clicking on the name of the setting and selecting the Modify option

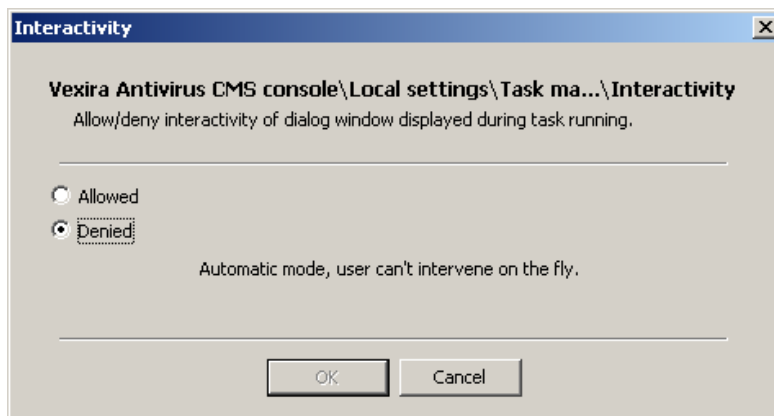
The values of the options can be set in the input dialogs. The simplest setting is when the user must specify the value in an input field.



Simple Input Dialog

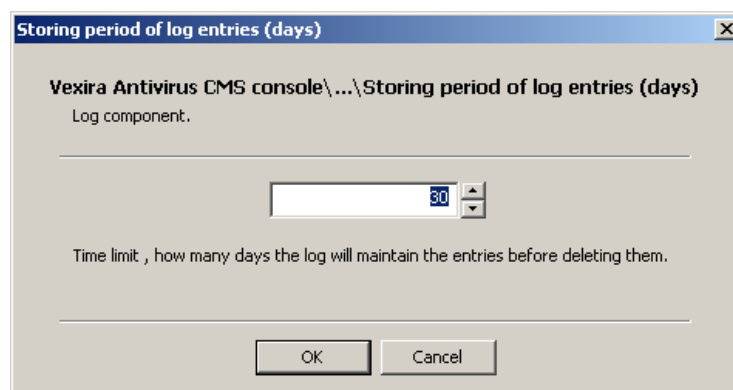
In some cases, the needed value can be specified by clicking on the **|Browse ...|** button. After having specified or selected the needed value, the window can be closed with the **|OK|** button and the value of the setting is the parameter specified in the input field. If you do not want to specify a value or you do not want to modify the value, use the **|Cancel|** button. This applies to all dialog windows.

In some cases, the option can only be enabled or disabled. In this case, the program offers these two options in a dialog window, and you can select the one needed.



Enable/Disable Option

The values can be set with arrows to increase or decrease the value of the parameter. In this case, you can only specify values between the allowed values. The needed value can be set by typing it as well.

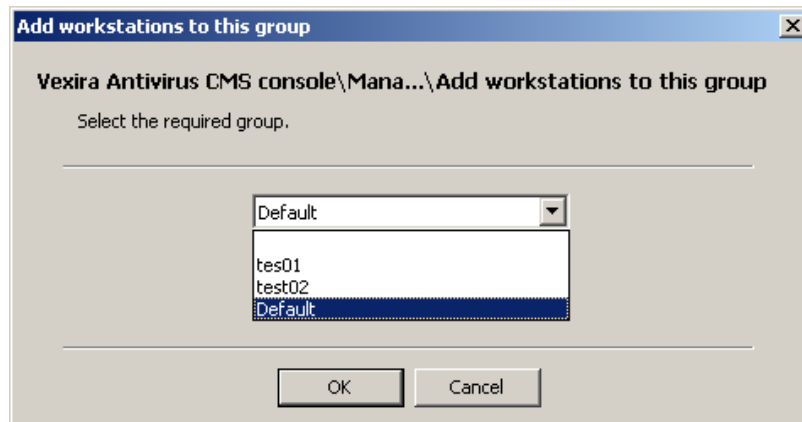


Parameter Settings Window



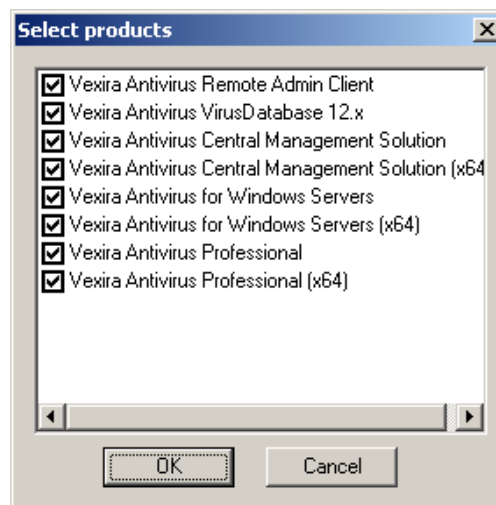
Vexira Antivirus Central Management Solution

In the following window, the value of the settings can only be a pre-defined parameter; in this case, these can be selected from a drop-down list:



Selecting a Value from a Drop-down List

The settings group may only be modified in a comprehensive dialog window (like selecting products for an update task). In this case, the comprehensive window is displayed if any of the options is modified, and you can specify the value of all the settings in the group in this window.



Comprehensive Settings Window



Discovering the CMS

A central computer manages the virus protection of the computers assigned to it in the CMS system and updates Vexira Antivirus products and their modules on these computers according to the settings. The following sections describe some of the definitions required to understand the operation and structure of CMS.

Installation Template and Configuration Template

The parameters and the products to be installed by the CMS server on the managed workstations can be specified in the [Installation template](#) and the [Configuration template](#) settings. The software stores information about the configuration of the antivirus software to be installed on the computers in these templates.

Groups

The system administrator may install and operate different types of virus protection or products with different settings on some computers in the network. This is possible with the help of CMS, because settings *Groups* can be created for the installation of the products (*Installation template*) and their settings (*Configuration template*) can be specified individually. Groups can be used globally in the system and after having created them, workstations can be assigned to the most suitable group and the server can manage these workstations according to the settings of the group. One group is always needed; therefore the *Default group* cannot be deleted from the system.

SubCMS

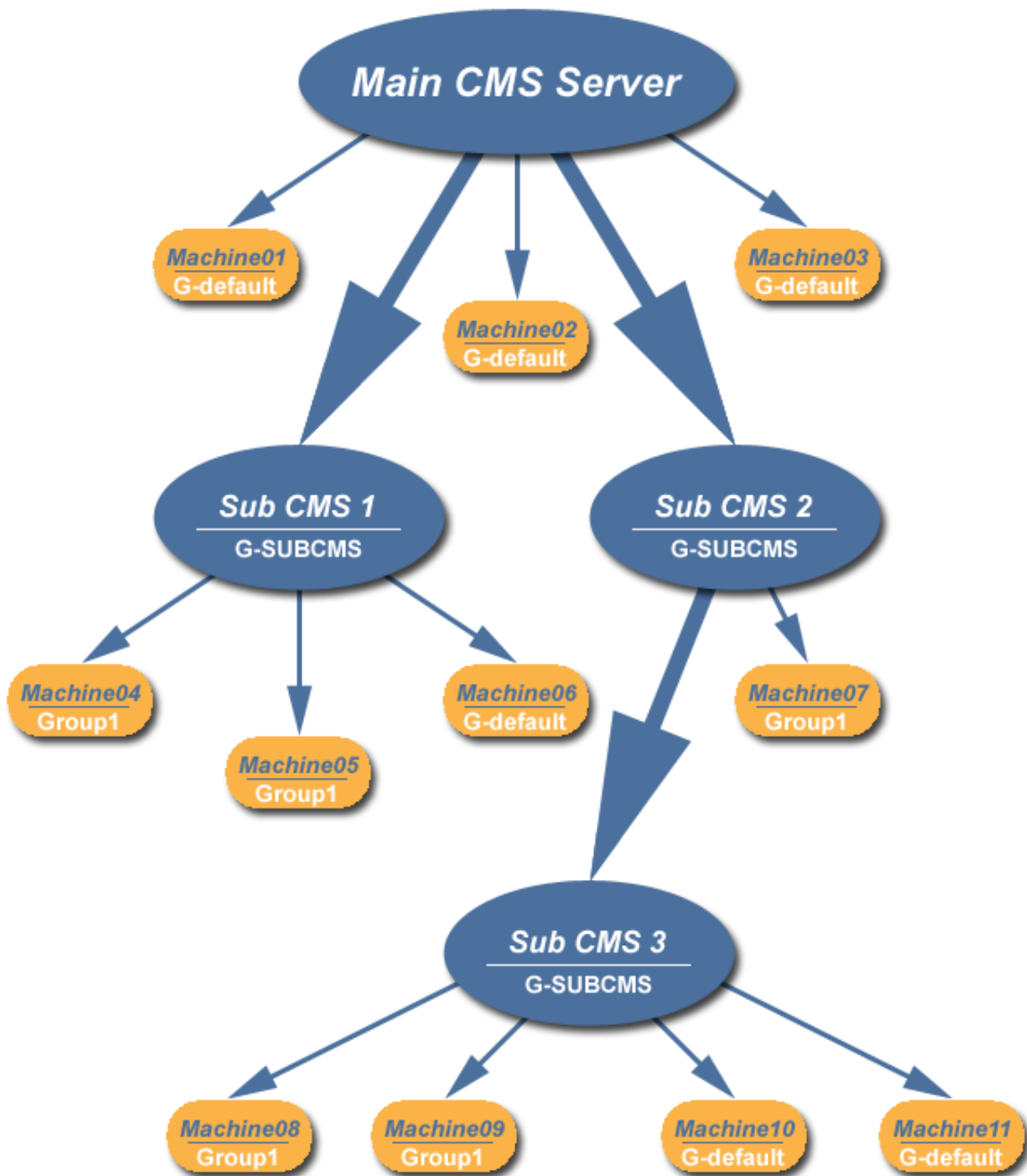
In a network of several computers, subCMS servers may be needed, which take over copying and management tasks from the main CMS server to reduce network load and optimize network traffic. These subCMS servers manage the computer assigned to them – and to the above mentioned groups – like the main CMS. The antivirus protection and its settings for these subCMS servers can be configured in a separate settings template, which is applied to all subCMS computers in the system.

Promoted SubCMS

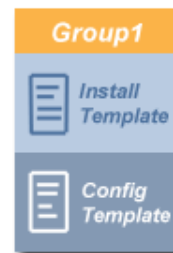
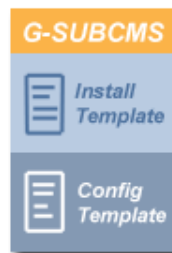
The promoted subCMS is a means to manage separated networks. For more details, click [here](#).

CMS – A Possible Structure

The following CMS system is a structured network of several subCMS servers. The main CMS manages three computers directly (*Computer01-03*), the rest of the computers are managed by the subCMSs (*Computer04-11*). Basically there are two types of groups in the system for the protection and its settings of the managed computers (*C-default*, *Group1*); the third – special – “group” contains the configuration of the subCMS computers (*C-SUBCMS*). The applications, which should be installed on the computers and their settings (Installation template, Configuration template) can be specified in each group. The templates for the subCMS servers can be found at a special location and not in the *Groups* folder, where the other groups and their settings are stored.



GROUPS



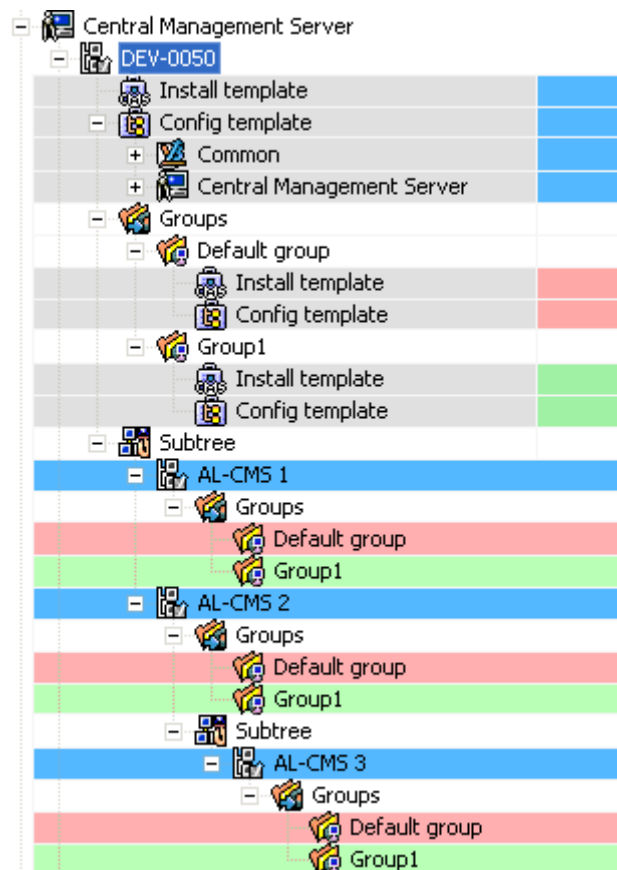
Structure of a Possible CMS System (1)



Vexira Antivirus Central Management Solution

The elements and the settings of the CMS system above are displayed on the main CMS server as described in the following figure. The meaning of the color codes is the following:

- SubCMS servers are blue.
- The default group is red.
- Group 1 (*Group1*) is green.
- The gray folders contain settings, and are applied to the item (subCMS or group), which has its color displayed at the end of the gray row.



Structure of a Possible CMS System (2)

The picture clearly indicates, that the template settings for the subCMS servers can be found directly under the *Central management ()* and it is applied to all subCMS servers.

In the *Groups* folder, the created groups and their settings can be found (which are also displayed under the subCMS computers). The managed computers can be assigned to the needed item (main CMS, subCMS) in these folders (*Default group*, *Group1*) and the system executes installations and updates on them according the settings in the needed group. The settings of the groups are specified in the *Install template* and *Config template* folders; these can only be modified in the *Groups* folder under the *Central management ()*.

The subCMS computers created in the system can be found in one folder (*Subtree*). Additional subCMS servers created under another subCMS can also be found in a folder named *Subtree*.

For setting up a CMS system, read the CMS – Installation Guide document that can be downloaded from Vexira Antivirus's website.



Automatic Monitoring Tasks

Basic operation of the CMS is ensured by scheduled tasks, which run automatically in regular periods to monitor any changes in settings. These monitoring tasks schedule tasks to be executed in order to optimize network load.

Because the CMS may manage a system of hundreds of workstations, servers, various networks and subCMSs:

- Tasks are executed in the system (spooling, installation, configuration changes) with a little delay.
- The status of supervised clients appears in the main CMS with a little delay.

Remember the previously-described rules when administrating CMS. The main tasks running in the CMS are described below.

Browsing for Active Computers in the Network

Default schedule: every 10 minutes

It lists the active computers in the managed network(s) with the help of Master Browser.

If the *Add new machines to database automatically* option is enabled and if a new active computer is found, it is added to the list of computers.

The description of the above settings can be found in the [Machine Management](#) section.

This task also checks if the machine is online or not, so the display of the online/offline status is performed according to this. When a machine is not active, CMS cannot perform installations or updates on it. It can be checked in the following two ways if a machine is active or not:

- When clicking on the name of a group under *Management settings > Central Management > Groups*, in the window on the right hand side, the status of the machines assigned to the group are displayed in the Current operation/status column.
- Under *Management settings > Non-managed computers*, when right-clicking on the name of a computer from a selected network, click Machine details in the local menu for the status of a machine.

Listing the Status of Protection on the Managed Computers

Default schedule: every 30 minutes

The task automatically checks the status of the managed computers (the installed products, the version of the products and the virus database, the necessity of an update). This task can be started on demand as well by clicking on the [Check managed product](#) local menu item.

Installer/Uninstaller

Default schedule: every minute

This default task analyzes the results of the above task and if an installation (an update) or an uninstallation is needed on one of the managed computers, it initiates the needed operation and returns the actual status of the installation/uninstallation processes.

Registration Status

Default schedule: once a day

The task checks and optimizes the distribution of license keys so as to cover different managed products and platforms as much as possible. The task monitors and removes expired license keys from the



database.

Replication

Default schedule: every 5 minutes

The main CMS updates the configuration of the subCMS with its actual settings. Modifications of the machine list and configuration/installation templates are replicated to the affected subCMS.

Network Browser

Default schedule: once a day

This task runs on promoted subCMSs and checks the networks known by the promoted subCMS.



Structure

The management modules of the product can be found under the *Management Settings* group in the MMC interface. The following list contains components that belong to this product. For their detailed description, select one of the components:

- [Central Management](#)
- [Non-managed Computers](#)
- [General Settings](#)
- [Product Versions](#)
- [Uninstallation](#)
- [Event Logs](#)
- [Install Copier](#)
- [Reporter](#)
- [License Manager](#)

Other components of the product can be found in the MMC tree in the *Local settings* group and are described in the [Local Settings components](#) section.

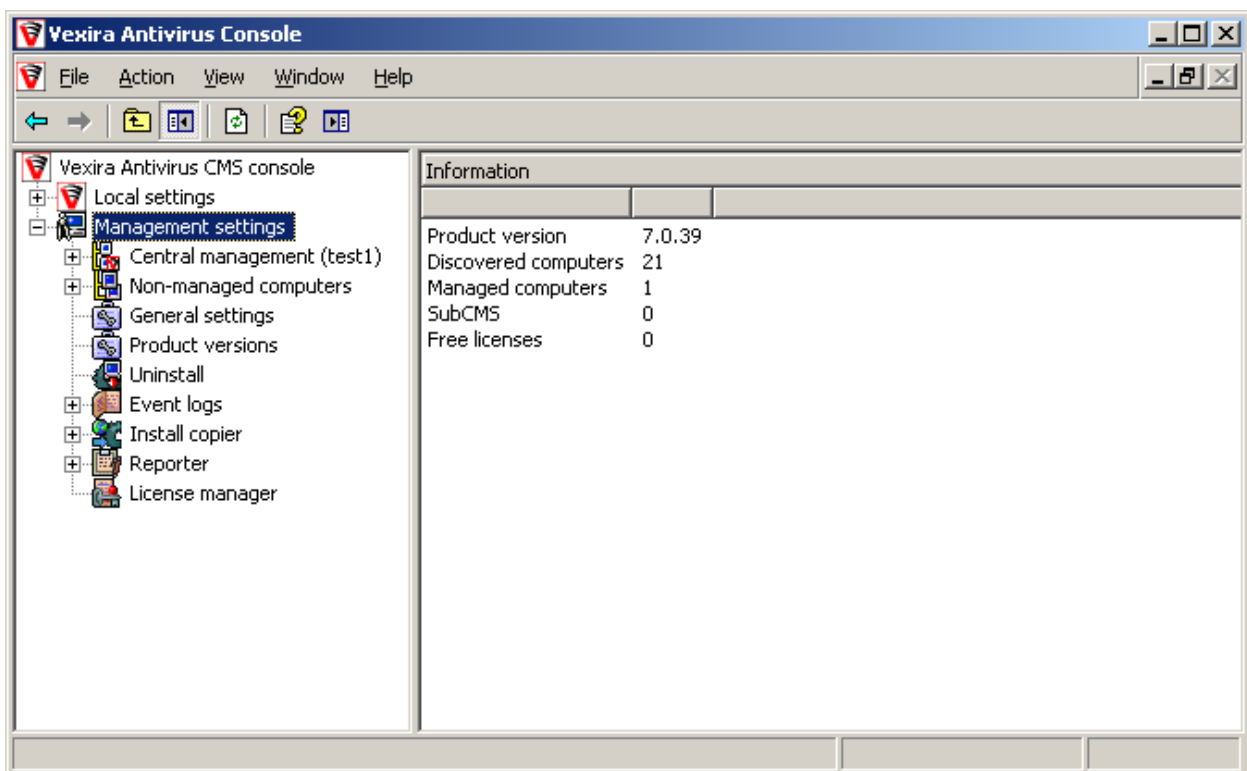


CMS MANAGEMENT MODULES

The management modules can be found in the *Management Settings* folder. This folder contains the modules needed for the management operation of CMS. Other settings of CMS are in the *Local settings* group.

Management

The central – main – CMS is on top of the management network, and all managed machines and subCMS servers are assigned to it. In the left side tree, the CMS structure (groups, levels, and templates) can be found under the *Central management (<name of the main CMS>)* folder that runs the main CMS. The name of the machine selected as the main CMS appears in *<name of the main CMS>*.



Main CMS and Folder

If you click on the *Central management ()* folder, a statistic overview is displayed in the right side window:

- *Machines to check*
The number of computers checked by CMS (only directly assigned computers).
- *Number of all remote actions*
Total number of computers under remote installation preparation or remote installation.
- *Preparation of installations on remote machines*
Total number of computers on which remote installation (or uninstallation) initialization processes are being performed.
- *Remote installations in progress currently*
Total number of computers on which installation or uninstallation processes have been started and are still in progress (or the automatic checking – [installation](#) or [uninstallation](#) – tasks have not finished yet).
- *Status*



Vexira Antivirus Central Management Solution

The installation/update procedure that reached the percentage is displayed here.

- *Currently processing*
The name of the computer being installed or updated.

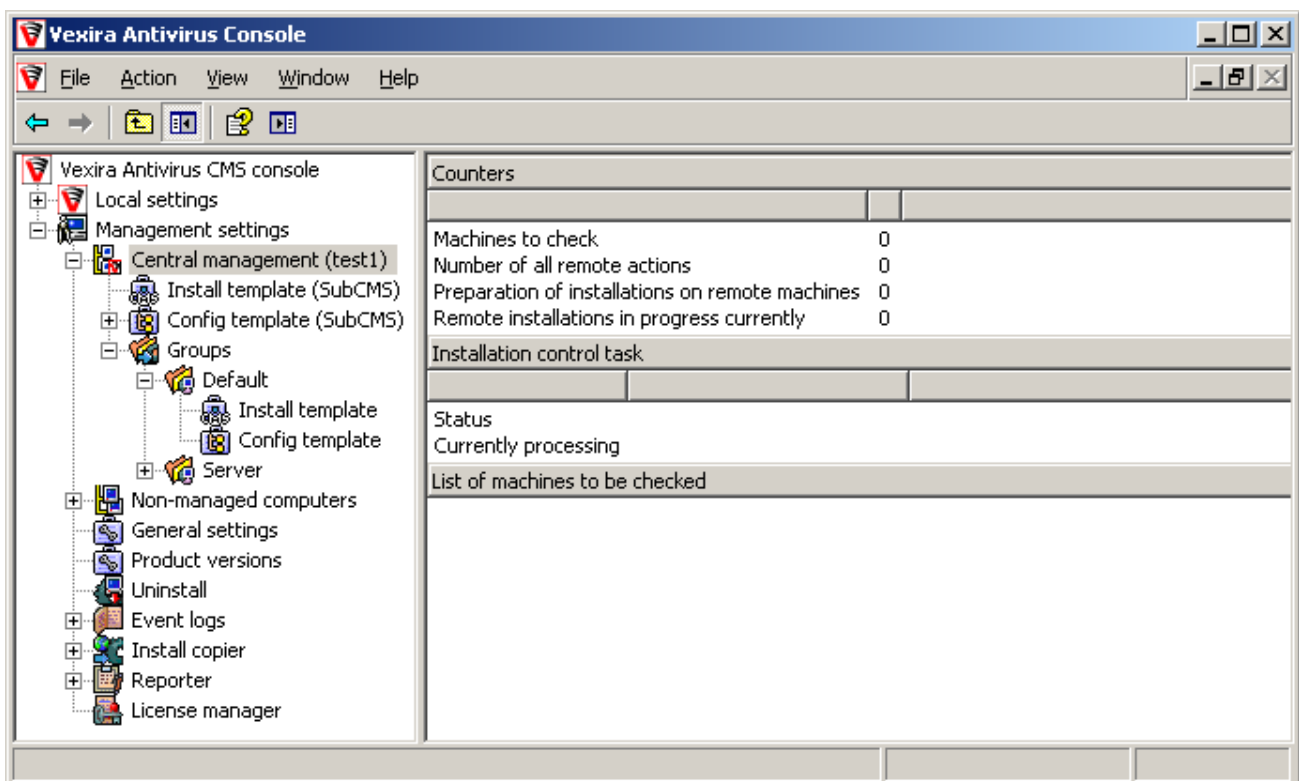
The *List of machines to be checked* contains the names of computers currently managed by the given CMS, their status, the groups they are assigned to, the current action, and the explanations. The computers that the CMS stopped managing disappear from the list.

If you right-click on the *Central management ()* folder, you can select the following menu items (the same ones are available in case of clicking on a subCMS):

- *Add Management Server*
[SubCMS](#) can be assigned to the main (or a sub) CMS.
- *Apply configuration now*
Applies the modification of the installation and configuration templates to the managed machines.
- *VDB reinstall*
The virus database can be reinstalled here on all the clients assigned to the main CMS.
- [Timetable](#) menu item

CMS System – Default Settings

If you open the *Central management ()* folder to the extent shown in the figure below, additional folders are displayed under the main CMS.



CMS – General Settings

The two folders that are directly under the *Central management ()* folder ([Installation template \(SubCMS\)](#), [Configuration template \(SubCMS\)](#)) contain settings only applied to subCMS servers (all subCMS in the system have the same settings). This can be named as the “group” of the subCMSs.



Groups Folder

The *Groups* folder contains the management [groups](#) created in the system. An Installation and a Configuration template can be created for each group storing the products and must be installed on computers in the group and their settings. The created groups are used in the whole system, the main CMS and all subCMS servers use these common groups. The managed computer is displayed in the group under the selected CMS, where it has been assigned. The number of assigned machines to a group are displayed right after the group's name in brackets. The groups' settings (installation and configuration templates) are only displayed in the *Groups* folder under the *Central management ()* folder as all groups – also used by the subCMSs – and are common in the system.

Groups

If you click on the left-side tree on the *Groups* folder, the names of the groups appear in the right side window. By default, only the *Default group* exists, as this group must always be present. If you double-click on the name of a group in the right-side window or click once in the left side tree, the computers and their [parameters](#) added to the group appear in the right side details window. The menu items of the local menu are described in the [Local menu](#) section.

If you want to create a new group, click on the *Groups* folder (only under the *Central management ()* folder) and choose the *Add* option. This option is also available from the right side details window if you right-click on the window, which contains the group list. After having specified the group's name, the group is created.

If the group is empty and is not assigned to any subCMS system, it can be deleted. To delete a group, right-click on the name of the selected group (only under the *Central management ()* folder) and choose the *Delete* option. The default group cannot be deleted.

Templates

[Installation and configuration templates](#) can belong to subCMS servers (the two templates applied to all subCMS servers can be found directly under the *Central management ()* folder in the left side list) or to groups (these are displayed under the name of the selected group).

Installation Template

If you click on the *Install template* folder, the settings of the selected template appear in the right side details window.

You can select the products to be installed on the computers in the needed group in the *Products to install* section on the top of the panel. You can specify the components of each product to be installed.

Installation Parameters

- *Restart after installation*

Never:

The managed computers are not restarted after installation.

If necessary/If necessary (forced)

Always/Always (forced)

If the '*If necessary*' parameter is selected, the managed computers are restarted after installation, if it is necessary, if '*Always*' is selected the computer reboot is performed without exception.



If the parameters' *forced* versions are selected, the system closes all running applications without asking for saving the actual data and restarts the system in a short time.

- **Delayed restart**
Minutes: If the client computer needs restarting and it is allowed, the computer is restarted with the specified time delay.
No delay: In this case, if computer restart is enabled after installation and it is needed, the restart could be performed by the user interaction, not automatically.
- **Progress window during installation**
Allowed:
The progress bar of the update or installation process is displayed on the managed computer.
Denied:
No indication of an installation or update process is displayed on the managed computer.
- **Warning window before system restart**
Allowed:
A window appears on the managed computer that warns for the user before the system is restarted. This action must be confirmed by the user.
- **Language**
The language of the installation used by CMS when installing a product on the managed computer.
- **Custom CFG**
Sends the configuration file to a client in the group.
- **Desktop icon**
Allowed: After installation, the Vexira icon is shown on the desktop of the client machine to start the product easily.
Denied: The Vexira icon is not displayed on the client's desktop.
- **Install path**
You can specify the installation path, i.e. the folder where the installation will be performed.

License Filter ([Included/Excluded] Licenses)

In the *License filter* setting you can control the allocation method of available licenses (listed in the *License manager*) to computers assigned to the actual template. It is possible to set licenses that are allowed or denied to be allocated to the machines assigned to the template.

Right-click on the *License filter* setting and select the *Modify* item to modify the option's value. Set the license allocation method on the appearing panel.

Select the basic handling method in the *Filter type* setting for the licenses listed in the *License manager* module.

If the *Exclusive (all, except selected licenses)* option is selected, all the available licenses are allowed to be allocated to the machines assigned to the template (these licenses are displayed in the *Included licenses* window on the left) except for the ones moved to the right window (*Excluded licenses*) with the help of the arrow button.

If the *Inclusive (only selected licenses)* option is selected, the available licenses are not allocated by default to computers of the template (the left side window contains the *Excluded licenses* now), select the allowed licenses by moving them to the right side window (*Included licenses*).

The initial value of the setting is the *Exclusive (all, except selected licenses)*, so all the available licenses are allowed to register software on the computers by default.

Hold the mouse pointer on a selected license to get the license details.



Configuration Template

The *Configuration template* folder contains the detailed settings of the products selected in the *Installation template* folder. The configuration template belonging to the given group contains a list of the modules of the selected products grouped by product, and all product modules in the *Local Settings* folder. The selected products are installed with the settings specified here on the computers belonging to the configuration template (or to the selected group).

Different components are displayed in the configuration template depending on products selected for the groups. These can be the following:

- Quarantine
- Virus scanner
- Resident protection
(component only available in the Vexira Antivirus Professional product)
- Server Guard
(component only available in the Vexira Antivirus for Windows Servers product)
- MS Office protection
(component only available in the Vexira Antivirus Professional product)
- MS Outlook protection
(component only available in the Vexira Antivirus Professional product)

Refer to the documentation of the given products for detailed descriptions of the above components:

- *Vexira Antivirus Professional User Guide*
- *Vexira Antivirus for Windows Servers User Guide*

The *Modules* to be installed and the used *User security context* are displayed in the left side list by clicking on the product's name. To modify the security context, right-click on the selected module and choose the *Modify access* option in the local menu.

- *Hidden*
The module settings are not available neither in *Admin mode* nor in *Normal mode* while this value is assigned.
- *Visible in Admin mode but not controllable*
The module settings are visible in *Admin mode* only, but the settings cannot be controlled even in *Admin mode*.
- *Visible and controllable in Admin mode*
The module settings are visible and controllable in *Admin mode* only.
- *Always visible but not controllable*
The module settings are visible in both *Admin* and *Normal modes*, but they are not controllable.
- *Always visible but controllable in Admin mode only*
The module settings are visible in both *Admin* and *Normal modes*, but they are only controllable in *Admin mode*.
- *No restriction*

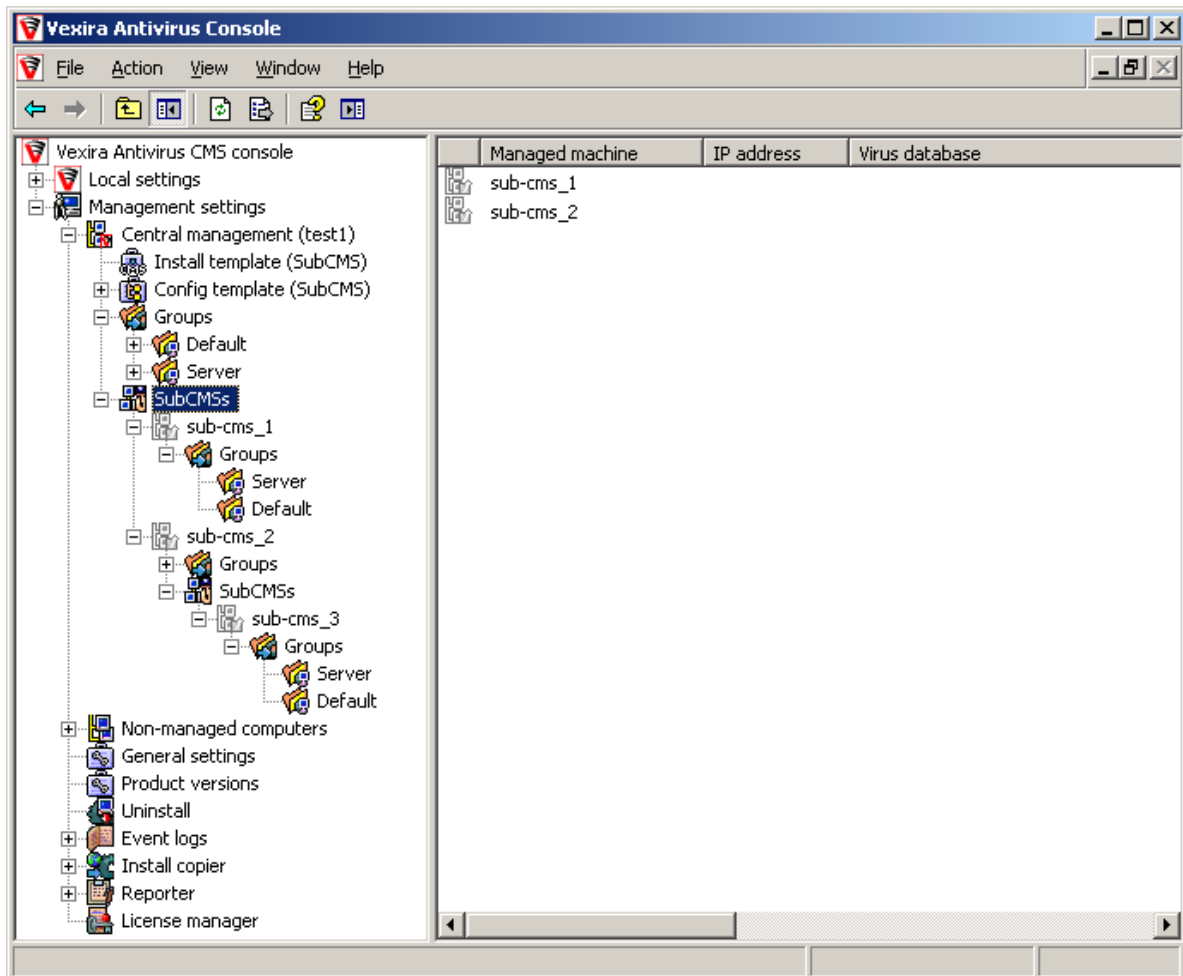
You can access detailed settings of the module by double-clicking on the selected module in the details window and this function is also available from the left side tree. Products are installed or updated with the settings specified here on the computers in a group.



Subtree Folder

[SubCMS computers](#) can be appointed to have management tasks. SubCMS computers are listed in the *Subtree* folder available after creating the first subCMS computer. If you click on the *Subtree* folder with the left mouse button, the list of the subCMS machines (found on the actual level) with [parameters](#) are shown on the right panel. The items of the local menu are described in the [Local menu](#) section.

Right-clicking on the *Subtree* folder, the available items of the local menu are the same as the ones of [the local menu of the main CMS](#) but there is a new option ([Promoted CMS](#)) that is described below.



SubCMS Servers

SubCMS

To create the first level subCMS, right-click on the name of the *Central management ()* folder in the left side list and choose the *Adding subCMS* option. The [Timetable](#) option and its settings are also available here and from the local menu of the folder that lists all subCMS servers. When adding a subCMS, the computer's name must be specified to be used as a subCMS (for more information about creating subCMS servers, refer to the [Assigning Computers to CMS / Assigning Computers to group](#) section).

When creating a subCMS, the group folders in the system are also created under the name of the subCMS and computers assigned to this server can be included in these. The groups' settings (installation and configuration templates) are only displayed in the *Groups* folder under the *Central management ()* folder as all groups used by the subCMS servers are common in the system. Settings for individual subCMS servers can be found in the two folders which are directly under the *Central*



management () folder (Install template (SubCMS), Config template (SubCMS)).

It is possible to create multi-level management in the system; therefore, subCMS servers can also be created under another subCMS, not just under the main CMS.

To delete a subCMS, right-click on the computer's name and choose the *Delete* option. You can only delete a subCMS if there is no machine assigned to it. Of course, any assigned machine can be deleted from a subCMS environment as well.

Promoted CMS

In some cases, the computers of a separated network to be managed cannot be seen (you cannot browse the system for the machine names), and they cannot be reached from the network trying to manage them (that is, the source network) via SMB, RPC, or NetBios protocols. These clients can be managed even in such cases if there is at least one computer in the separated network, which can communicate with the source network's CMS machine (that is, it can be reached from both networks). This special machine must be configured as a subCMS, and then designated as promoted CMS. For this, right click on the subCMS, and select the *Promoted CMS* option. The *promoted CMS* can:

- Map available networks
- Send them via replication to the main CMS
- The networks to be managed must be [enabled](#), and the [user accounts](#) to reach them must be set.
- They are sent back to the promoted CMS by the replication task; now that the network has been enabled, the promoted CMS maps the machines on the given network.
- Via replication, these machines are passed on to the main CMS where they can be put into groups (of course under this subCMS only).

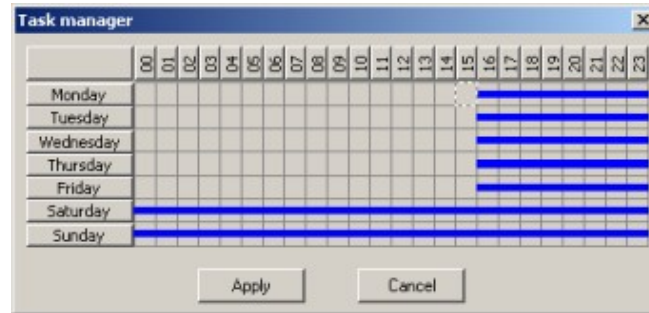
The networks which were entered by the promoted subCMS are shown on the main CMS in the following format: <name of the mapping subCMS>.<network name> (for example, alcms1.privatenetwork). From this point, the computers can be ordered into the various groups.

The icon of the promoted CMS has an asterisk to distinguish it from an ordinary subCMS icon.

Timetable

The timetable can be used to specify intervals, which are – for some reason or another – not suitable for the CMS (or subCMS) to perform the needed installation or update procedures. In these intervals, the CMS does not perform any installations on the managed computers. The virus database update tasks (and tasks which do not require computer restart) are always performed if needed – independently on this setting.

The timetable can be valid for the *Central management ()* folder, which contains subCMS servers and for groups. The timetable for the main CMS and the common timetable for subCMS servers can be found at the *Central management ()* folder and the folder containing subCMS servers. A separate timetable can be defined for groups.



Timetable

The columns indicate the 24 hours of the days and the rows indicate the days in a week in the *Task manager* window. By selecting (holding the left mouse button), the intervals can be specified when installation is not allowed on the managed machines. The forbidden intervals are indicated by empty cells, the permitted intervals are indicated by blue lines (on the above picture installation is forbidden on every business day until 4 p.m.).

After having selected the needed interval, you can select the needed option from the local menu by right-clicking:

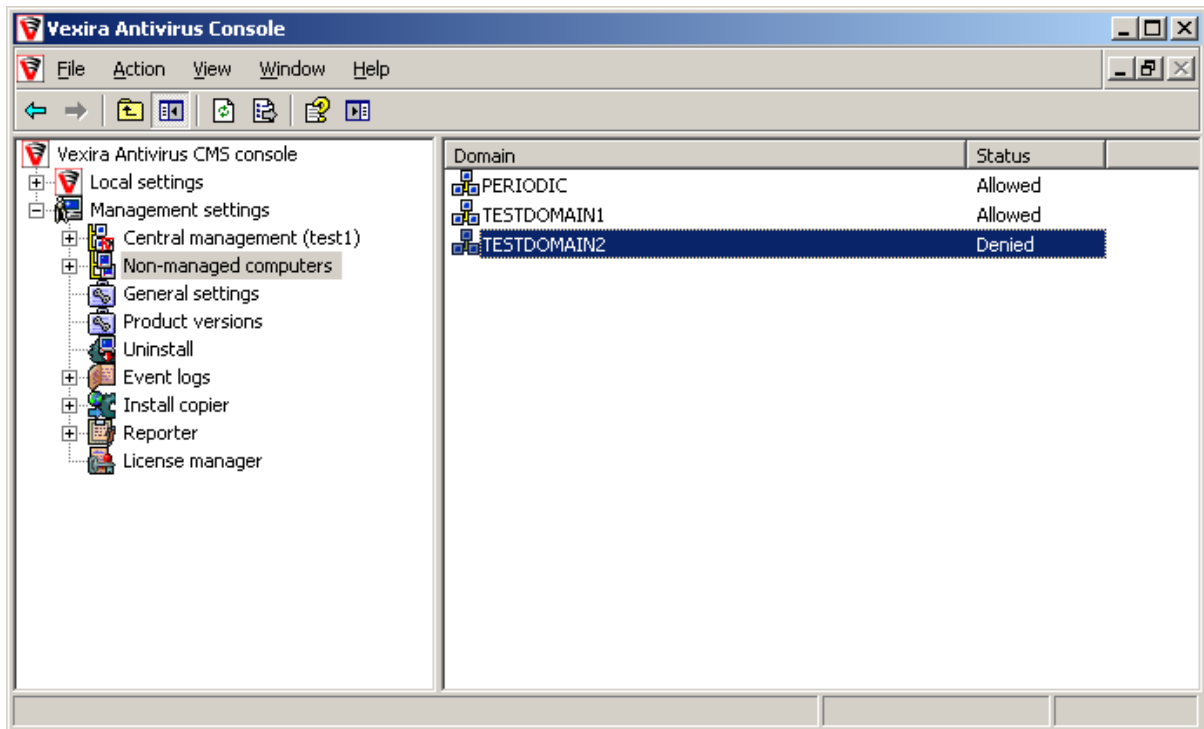
- *Allow*
Installation is allowed in the selected interval.
- *Disable*
Installation is forbidden in the selected interval.
- *Select all*
Selects all cells.
- *Delete selection*
Removes the selection.

The settings can be applied by clicking on the **|Apply|** button, or you can exit without modifying the settings by clicking on the **|Cancel|** button.



Network

The menu displays and administers the managed network(s) (domains, workgroups). From here, the client computers (workstations and servers) mapped in various networks can be easily added under the CMS as managed machines or even as subCMSs manually or automatically (refer to the [Automatic Monitoring Tasks](#) section).



Non-managed Computers

Handling Domains and Workgroups

By clicking on the *Non-managed computers* component on the left side, the right side details window displays the currently browsable domains and workgroups. The domains and workgroups can be handled by using the local menu. To display the local menu, right-click on an empty part in the right side window or on the *Non-managed computers* component in the left side menu.

The explanation of *Add...* and *Add all* options:

- *Add...*
You can enter the name of the domain or workgroup to add to be displayed in the list.
- *Add all*
All domains and workgroups in the network are added to, and displayed in the list.

If you right-click on a domain or on a workgroup, you can also choose the *Modify* and *Delete* options:

- *Modify*
The second column of the domain and workgroup list indicates if the management of an item is *Allowed* or *Denied* by the CMS: You can modify this setting in this option. If you allow CMS to manage a domain or a workgroup, it is displayed in the left side tree under the *Non-managed computers* component. To check computers in the domain or workgroup, double-click on the selected item in the right side window, or on the domain's name on the left side.



By default, the management of recently added domains or workgroups is not allowed.

- **Delete**
Removes the selected item from the list. Removal requires approval in a dialog box.

Managing **Several Domains or Workgroups**

CMS allows the management of several different workgroups and/or domains. After specifying the required settings, the networks added are accessible for the CMS. In this way, these clients can be managed from one, central location. (see also: Promoted [CMS](#)).

Note!

The newly-added networks are disabled by default.

Network Settings

For each network, you have to set the relevant user account (in the User settings section to have system administrator permissions in the given network. In order to [manage workgroups](#), it must be present on each managed computer in order to provide access to the clients. The account must be specified in the following format: NETWORK\User (for example, WORKGROUP\Admin).

[LDAP support](#), to be discussed below, can be enabled in the *General settings* section.

LDAP

Introduction

The goal of the function of assigning computer according to LDAP is that computers, which are stored in LDAP (active directory) are assigned automatically (following rules) to the proper (sub)CMS and to the proper group. Currently the function can assign (add) computers.

Operation

The queries set in the LDAP rules are performed by the Browsing for active computers in the network automated task. When it runs, all added rules are performed. During this operation, the system ignores the items already assigned and returned as a result of the query, and possible new items are added to the proper group/network.

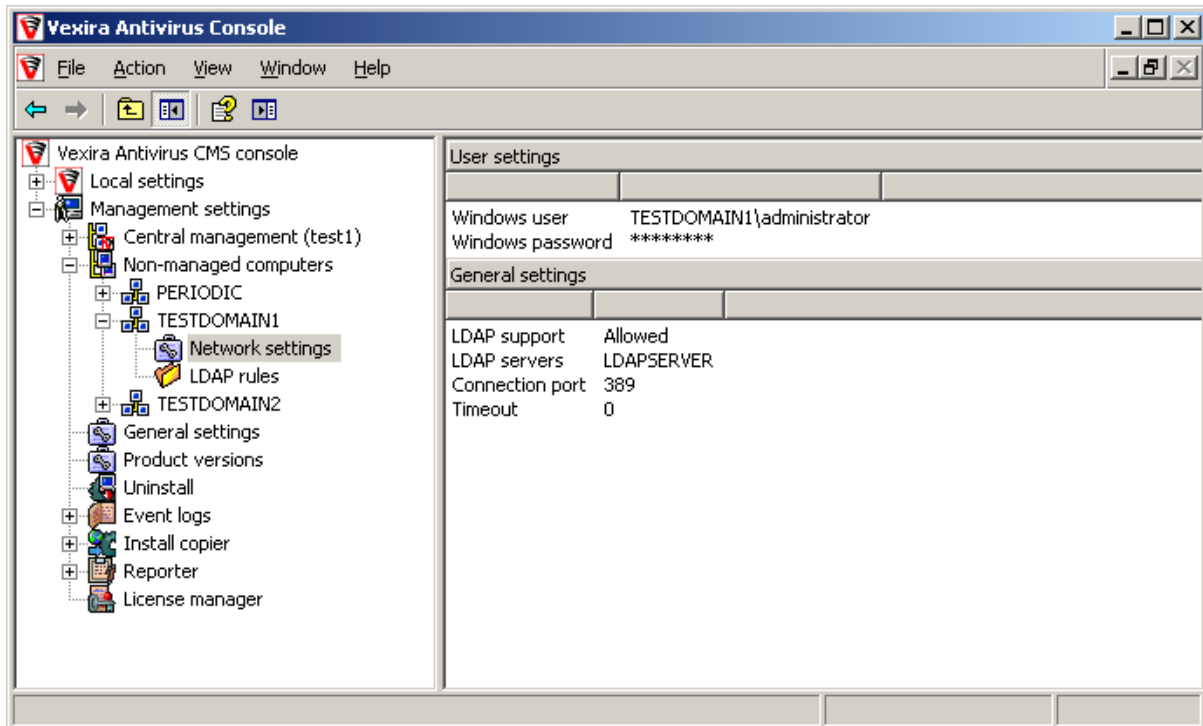
Important!

Assigning a subCMS to the system when adding new computers from *LDAP* is currently not supported in the product.

Currently the name attribute of specific computer objects are assigned as a computer in the CMS.

General Settings

LDAP can be enabled under the Non-managed Computers menu inside the needed network. The LDAP support setting can be found under the Network settings menu.



LDAP Enabled

After enabling the function, three more menu items are displayed under *Network settings*, where we can adjust general settings:

- *LDAP servers*
The name(s) of the server(s) – NetBIOS or FQDN name – (separated with spaces), on which the LDAP structure (active directory) can be found.
- *Connection port*
The port through which LDAP communicates (389 by default)
- *Timeout*
The product waits for data during the query for the adjusted time.

Setting Up Rules

This section describes the options needed to add rules and the process of adding rules.

Settings

LDAP rules can be added by right-clicking on the LDAP rules page next to *Network settings*.

The options which can be set in each rule:

- *Rule name*
The name of the added rule. You can give a name for a rule when creating a new rule. Note that later this name cannot be modified.
- *Base DN*
Path (object or direct) in the LDAP structure where specific computers are stored.
Example 1: CN=Computers, DC=periodic, DC=table
This maps the objects in the Computers directory under the periodic table domain in Active Directory.
PL2: CN=CMS_1, CN=Computers, DC=periodic, DC=table



Vexira Antivirus Central Management Solution

CMS_1 is the name of a specific object here and in this case we are referring to only this object (computer) (SCOPE > Search only on BASE DN level)

- **Scope**
 - *Search only at BASE DN level*
If an object is set as BASE DN, it only searches for the *name* attribute in this specific object.
 - *Search only at the children level of the BASE DN*
Only searches for direct child items under the BASE DN.
 - *Search full subtree*
Searches for all direct and indirect child items under the BASE DN.
- **Assign to CMS**
Sets the CMS (or subCMS) under which all computers are assigned according to the rule (the CMS and subCMS computers are displayed here).
If nothing is selected, the computers are not assigned to any CMS or group: they are added to the *Non-managed computers* node in the CMS under the proper domain/workgroup and they must be assigned manually.
- **Assign to group**
This function has an effect if a (sub)CMS is selected. The computers are added to the group set here according to the rule (all groups, which have been added to the CMS are displayed here).
- **Raw filter**
In this case the query can be added in a raw format following RFC 1960 and 4515 standards. If we have added something on the others settings pages, it is displayed here as well.

Neg.	Attribute	Relation	Value	Link as
<input type="checkbox"/>	objectClass	present (=*)		
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

LDAP Rule

- **Detailed filter**
 - *Neg.*
The negative of the condition set in the given row is applied.
 - *Attribute*
The attribute to be filtered.
 - *Relation*
The selection of computers in relation with the *added values* according to the following: *equal, approx* (not supported by some LDAP structures), *less, greater, begins with, ends with, substring*
or



- present* (in this case no value must be set).
- *Value*
A value must be set here for the relation (in case of exists, this is not needed).
Tokens can also be added as a value: `%%INACTIVETIME%%`
Its real value is a date, which is created in the following way:
[The date of the computer running the main CMS] – [90 days] = `%%INACTIVETIME%%`
The date, when the computer received a password in the domain for the last time is stored in the `pwdLastSet` attribute of the computers. With the help of this token, we can filter computers, which have not received a password for more than 90 days (which are inactive).
- *Link as*
We can add rules, which are set up from several conditions, and different conditions are connected to each other by the operators set here.

Available action buttons:

- *Getting attributes*
Performs a query for all possible attributes, and if the query was successful (an [ok] is displayed on the button), these values can be selected from the drop-down list of the *Attribute* column.
If the query was not successful, a warning dialog is displayed.
- *Query results*
The results of the query can be checked by clicking on this button (the computers that were found by the rule during the query will be displayed here). In case of an unsuccessful query a warning message is displayed on the results panel.

Creating an LDAP Rule

1. First, enable LDAP support.
2. Specify an LDAP server.
3. Specify a user for connecting to the LDAP server(s):
"Workgroup" > Network settings > User settings
4. By selecting the "Workgroup" > LDAP rules setting, you can add/delete/modify rules on the right panel by right-clicking on it.
5. After setting the parameters of the query, click on the *Getting attributes* button.
6. Before finalizing the rule, check the computers with the *Query results* button.

Important!

LDAP rules can be enabled and disabled on the interface. Disabled rules are indicated by a different icon in the list. Disabled rules won't run, thus they won't add any machines.



Non-managed Computers

The computers in a domain or workgroup can be displayed by clicking on the managed domain or workgroup (one click on the left side tree, double-click on the right side window). The computers in the domain or workgroup are mapped periodically by an automatic [built-in task](#), but it is also possible to add computers manually with the local menu ([New computer](#), [Import computer](#), [Search for computers](#)).

Important!

The computers in the list are not yet assigned to any CMS, therefore they are not managed!

The list of machines is displayed in the window on the right side. The following data appear:

- *Non-managed computer*
- *IP address*
- *Domain*

Assigning Computers to CMS or Group

A CMS must be selected for the computer to be managed and a group containing the settings, which is used to determine the products and components, which is installed on the computer.

After opening the CMS and group structure in the tree on the left, grab the selected computer in the list of non-managed computers by dragging and dropping it to the needed CMS (which manages the computer) in the selected group (which defined the computer's configuration). This must only be performed when the management structure is already set up (subCMS servers appointed, groups created).

Computers can also be assigned to a CMS or group in the local menu (right-clicking), which is described in the [Assigning Computers to CMS / Assigning Computers to Group](#) subsection of the Local menu section.

List of Assigned Computers

The computers are displayed under the group they are assigned to. If you click on a group, the list of computers appears in the right side window. The following data can also be displayed after further examination of the computer:

- *Computer name*
- *IP address*
- *Virus database*
The virus database version of the computer.
- *Threat status*
It displays if a virus incident occurred recently on the given client machine. For more information, see the [Threat Status](#) section.
- *Status*
This indicates the actual status of the computer as a combination of the following messages:
 - Installation/uninstallation denied*
 - Installation in progress*
 - Uninstallation in progress*
 - Installation/uninstallation in progress*
 - Restarting in progress*
 - Error*
 - Preparing reinstallation*



Preparing uninstallation

Preparing restart

Under examination

The computer has not been restarted after installation/uninstallation

Available information is not sufficient

The right side local menu's functions are described in the [Local menu](#) section.

Find machine

You can get quick information about an assigned machine (group and CMS to which it is assigned) by the help of the find machine function. Click the right button on the *Management settings* item in the left side tree and select *Find machine* option. Enter the name of the machine you would like to find in the *Filter* field, joker characters (* and ?) are available.

Threat Status

Threat status shows if there was a virus incident on the given machine and it also displays if the resident protection successfully blocked or removed the malware. The statuses displayed can be one of the following:

Clean

There is no virus infected or suspected element on the machine according to the antivirus program.

Infected/suspicious

The scan engine found a virus infected or suspected element on the machine and this element cannot be removed (for example, because the user blocked this action). This status is displayed in this case under the given machine in the list of machines.

The resident protection tries to check and remove these malware after a certain period of time. This action is performed by the *Checking threat status* task, and when it is done successfully, it is reported to the CMS.

Not infected (removed)

The resident protection successfully blocked the malware (removed or quarantined). This status is displayed at the given machine for a week after the action was performed showing that a virus incident occurred on the given machine recently.

Enabling/Disabling Column Display

You can enable or disable the columns in the right side window to be displayed. Click on the *Local Menu* option, *View*, then *Enabling/Disabling Column Display* option.



General Settings

Machine Management

This group of settings contains the options, which are used to assigned managed computers to CMS servers.

- *Add new machines to database automatically*
Denied:
If a new computer appears in the managed domains or workgroups, it is not added to the database automatically.
Allowed:
In this case CMS checks [at given intervals](#) the number of computer in the managed network and if a new computer is in the network, it is automatically added to the database.
- *Delete inactive machines*
The intervals (in months), after which inactive computers are deleted from the system can be set here.
- *Keep incident events*
The system stores the incidents detected in the managed network. This data enables creating statistics and reports about incidents with the help of the [Reporter](#). You can specify the number of days that the system stores incidents here. The default setting is 365 days.

Installation Management

Settings for the installation/uninstallation operation of CMS:

- *Display statistics on subCMS*
Denied:
The statistics about the selected subCMS are not displayed in the right side details window when clicking on a subCMS in the left side tree.
- *Limit of parallel remote installations*
The number of parallel installation and uninstallation can be limited here.

License Management

In the *Log entries* setting, you can control the log messages created by the *License management* module to inform the user about license allocations. It is possible to set a log level to disable some notifications that are not so important in a given case. The following values are available:

- *On errors*
These messages are created to notify about cases when:
 - There are not enough licenses to register a computer (it had no license so far, either or it had but lost it).
 - The license is not valid for every product installed on the computer.
- *On errors and warnings*
Informs about events mentioned in the previous point and about:
 - The license is valid for more products on the computer than needed.
- *On errors, warnings and successful actions*
Informs about events mentioned in the previous two points and about:
 - The computer has the required license(s), everything is OK.
 - The product(s) installed on the computer is registered, it needs no additional license.



Automatic Assignment of New Machines

Machines newly-detected by the CMS can be assigned automatically to CMSs or groups by the system. For this, groups must be created and set carefully for the new workstations and servers.

- *Assign workstations to this CMS*
The CMS selected here manages the new workstation appearing in the network.
- *Add workstations to this group*
All the new workstations appearing in the network are managed by the group selected here.
- *Assign servers to this CMS*
The CMS selected here manages the new server appearing in the network.
- *Add servers to this group*
All the new servers appearing in the network are managed by the group selected here.



Local Menu

In the left tree if you click on a selected [group](#), the [Subtree folder](#) or a [managed domain or workgroup](#) in the *Non-managed computers* folder, the following functions are available through the local menu in the right side of the windows. The local menu appears by right-clicking on a computer. Some of these options can also be used when selecting multiple items. The available functions:

Reinstall

If the selected computers are not assigned to any of the CMS servers, they are assigned to the current CMS in the default group and CMS reinstalls the products defined on the installation template on all selected computers. This function cannot be used on computers, where an installation or uninstallation process is in progress.

Remove

If the selected computers are not assigned to any CMS servers, the computer is assigned to the current CMS in the default group and CMS removes all Vexira Antivirus products from them. After the removal, the installation/uninstallation option is disabled. This function cannot be used on computers, where an installation or uninstallation process is in progress.

Restart

If the selected computers are not assigned to any CMS servers, the computer is assigned to the current CMS in the default group and CMS initiates a system restart.

Reinstall VDB

CMS (re)installs the virus database on every computer that is selected.

Enable installation

CMS enables installation/uninstallation on the selected computers. This option cannot be used on computers, where installation is already enabled.

Disable installation

CMS disables installation/uninstallation on the selected computers. This option cannot be used on computers, where installation is already disabled.

New machine

Adds a new computer to the database. Specify the name of the computer that can be found in the managed domain or workgroup if it is not yet in the computer list.

Add comment

You can add a comment to the selected machine. By default this column is not displayed in the list, you have to [enable it](#).



Import machine

Imports computer into the database from a text file. All computers must be written in a separate row. If you want to assign a computer to a CMS, use the COMPUTER, CMS format.

Search for new machines

Starts the default [Search for active computers in the network](#) task.

Delete

Removes all selected computers from the CMS database. If the computer is still in the network, and the [Add new machines to database automatically](#) option is enabled, it is added again to the database as a computer, which is not managed, but all information about the computer is deleted.

Assign machine(s)

With these two menu options of the Local menu, you can select the CMS or group that you wish to assign a given machine to.

After right-clicking on the chosen machine, select the *Assign machine* option in the local menu. A pop-up window appears where you can select the CMS or group to which the machine running it is to be assigned.

The machine can be assigned as a subCMS, which means that this machine manages the computers assigned to it, so that the main CMS is not overloaded. Select the checkbox at the bottom of the pop-up window to assign it as a subCMS within the network.

Machine details

An information window (with two separate tabs) is displayed about the selected computer and the event logs of the given machine.

All the information and data about the product and the given machine are available under the *Details* tab. You can also use the arrow keys to display details of consecutive machines in the list.

1. The information about the product is displayed in the top window. They are the following:

- *License key*
The license key that the given product is registered with.
- *Product status*
The status of the given product: valid or expired.
- *Guard status*
The Guard is enabled or disabled.
- *Threat status*
The threat status of the given machine. For more information, see the [Threat Status](#) section.
- *Quarantine*
The file(s) in the quarantine and its (their) size are displayed here.
- *Virus database*
The virus database version is displayed here.



- *Scan engine*
The scan engine version is displayed here.
- *Loader version*
The scanner loader version number is displayed here.
- *CMS*
It displays the CMS that the given machine is assigned to.
- *Group*
It displays the group that the given machine is added to.
- *Current operation/status*
It displays the status of the given machine and the operation that is currently run on it.
- *Install message*
It displays a message with the current status of installation.
- *Custom settings*
It displays the configuration file containing the custom-made settings.

2. The data about the machine is displayed in the bottom window:

Computer name, IP address, Operating system, Operating system architecture, Domain, Processor, Processor architecture, Physical memory, Hard drive (the data of the drive where the product is installed), *Machine status*

If the client does not send this data (for example, before installation is done, an error occurred), they are not displayed in this window.

The log messages concerning only the given machine are available under the other tab, the *Event logs*. This log operates the same way as the [Event logs](#) under the *Management settings* tab.

Check if managed machines are online

Runs the built-in [Listing active computers in the network](#) task.

Check managed products

Runs the built-in [Listing the status of the protection on the managed computers](#) task.

Quick Replication

Runs the built-in [Replication](#) task.

Filter

The filtering function is available in several elements of the product (for example, in the central log messages).

The filtering function can be selected by right-clicking on a given element. The *Filter settings* pop-up window appears with the options that you can filter:

- You can select the categories and the event types (for more information, refer to the [Central Alert](#) section).
- You can filter machines, users, or message content by entering text in the empty field beside the element to be filtered.
- From a drop-down list, you can select the modules to be filtered.
- And you can also select the period to be filtered by specifying the start and end date of



the logs.

Depending on which element you are at in the GUI when opening the *Filter settings* window, some options may not be defined, so that you cannot select them.

Minimum one category and event type must be selected in order to start filtering.

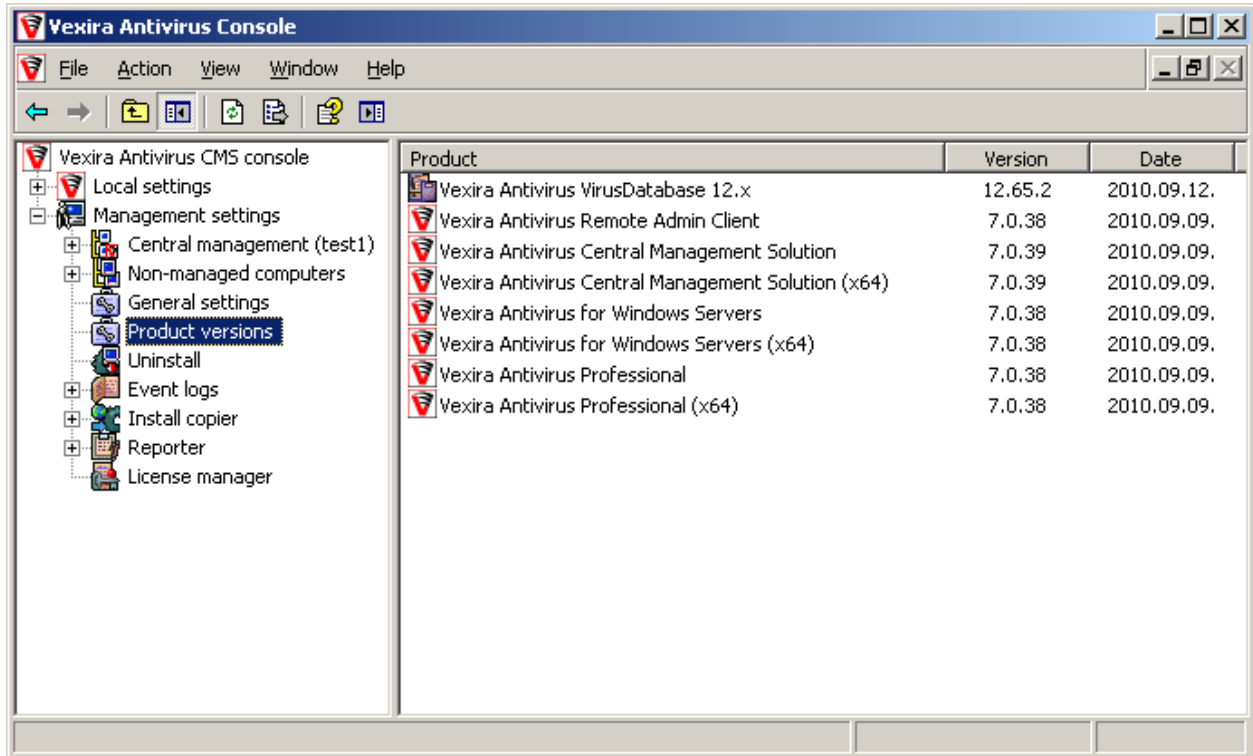
When filtering by machine or user, enter the search text between asterisks (*) (e.g. user=**test**). For filtering for message content, no asterisks need to be used.

If you specify a period for filtering, the start date must be earlier than the end date, otherwise filtering cannot be used.



Product Versions

The managed products and their version numbers are displayed on the right after clicking on the folder. These products are installed and updated on the managed computers by CMS.



Product Versions

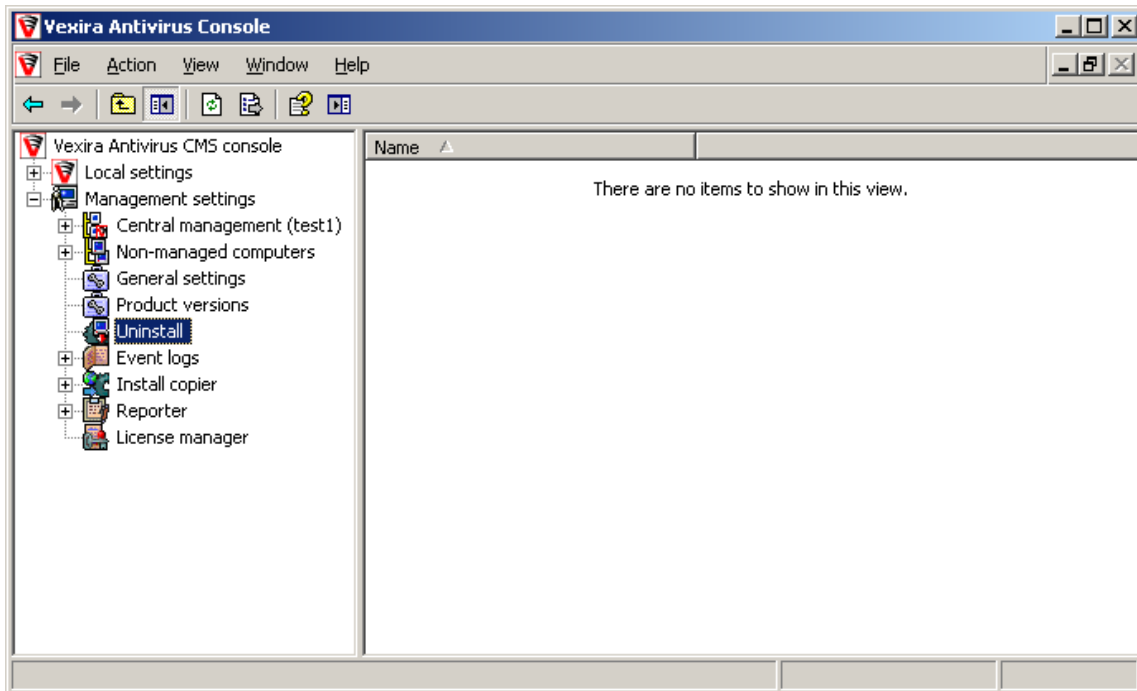
If the window contains no products, CMS has probably not yet been initialized. Start the initialization task with the right settings, so that products can be added to CMS.

It is described in the [Default Install Copier Task](#) section.



Uninstallation

The *Uninstallation (Uninstall)* folder contains the applications to be uninstalled. The listed software is removed from managed computers after the built-in uninstaller task is executed.



Applications To Be Uninstalled

To create the list of these applications, right-click on the right side window to display the local menu.

Select the *Import* option and select a computer. The products collect the list of installed applications. Select the applications to be uninstalled by choosing the *Add ...* option. The added applications are removed from all managed computers, when the built-in uninstallation task is performed.

The order of uninstallation can be also set: right-click on an application, and move the item with the *Move up*, *Move down* options.

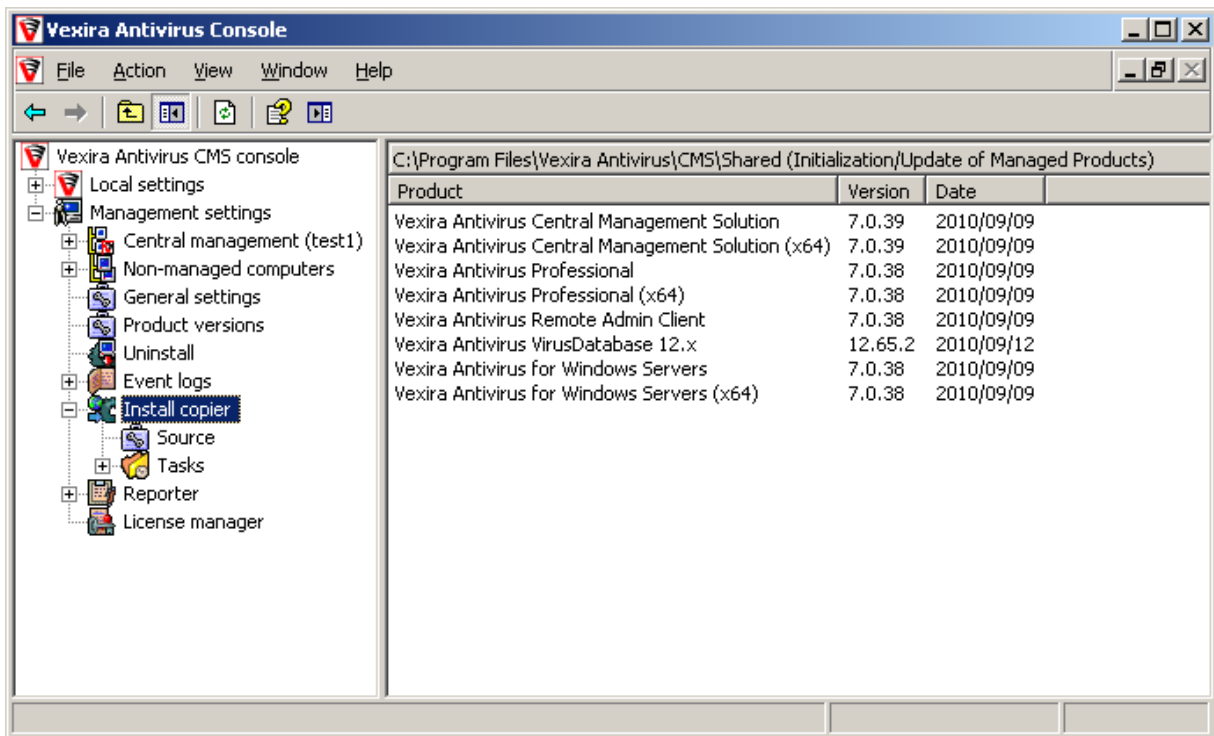


Install Copier

With the help of the tasks that can be added in this component CMS updates the Vexira Antivirus products on the managed computers. CMS stores the products in the set [directory](#). This enables to schedule the update frequency and specifies the update source from where new product versions are downloaded to the storage directory that stores the product and is used to update/install new computers. Install copier operates based on tasks: updates can be started with a few clicks according to the pre-defined settings, or can be scheduled.

By clicking on the *Install copier* component, the products stored in the above directory and their versions are displayed in the right side details window. If the window contains no products, CMS has not yet been initialized. Run the initialization task with the right settings, so that products can be stored in the CMS server's folder. It is described in the [Default Install Copier Task](#) section.

By clicking on the plus sign (+) in front of the component, the icon of the *Source* panel appears and the *Tasks* folder, which can be used to set up the component.



Install Copier

Source Settings

The detailed description of *Source* settings can be found in the [Source settings](#) section.

Tasks

The usage of tasks is described in the [Tasks](#) section.

Default Install Copier Task

The default task in the task list is a general initialization/update task connecting to a defined source and trying to download the available – or set – Vexira Antivirus products versions. The management system



is only operational if this – or a similar – task has already been performed and the products has been downloaded (all those products which were selected during install) to the storage folder to be used by CMS to update products on the managed computers. This [task](#) is run in the network in every hour by default.

Important!

The source of the default task is the source, from where CMS have been installed.

Settings of the Install Copier Task

The update source can be selected at the *Type* option where the program checks, if there is a newer version of the selected products. Only active update sources are available, which can be set on the [Source](#) panel.

Select the products that must be updated in the storage folder at the *Products to copy* option.

Selecting a storage folder:

Specify the storage folder at the *Target path* option, where the task downloads new product versions. This folder is used as a source for CMS to update managed computers.

If *Progress dialog* is enabled, the download process is displayed. If *Interactivity* is enabled, the download progress is displayed, and the task's settings can be modified temporarily and the user must interact with the software during the process.

If the source is available through a network, you can specify the information needed for the connection in the *Network connection's parameters* section. If you select the *Always on-line* option, the started task does not try to establish a network connection and generates an error if no connection is available. If the *Dialup connection* option is selected, the task establishes a connection and terminates it after performing the needed actions if the task created the connection. In this case a password can also be specified for the connection.



Event Logs

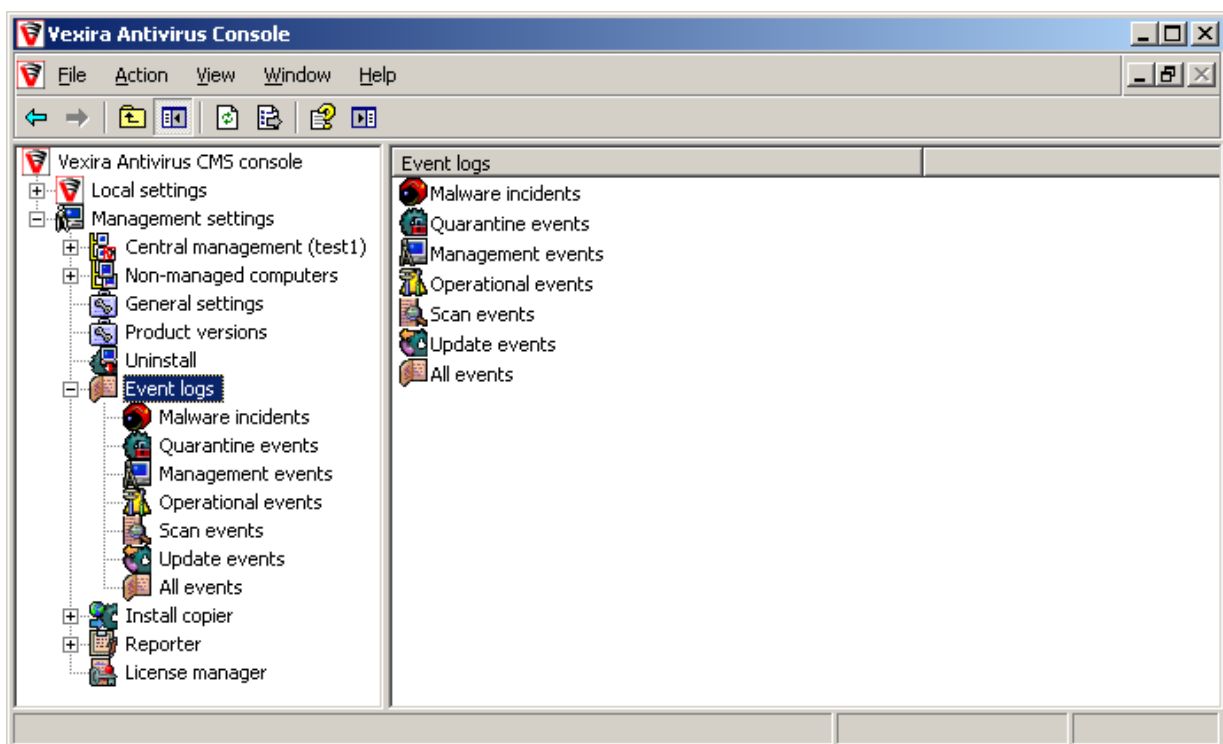
All the messages concerning the managed system are stored in the *Event logs* option and grouped into categories and without grouping. So events generated by the CMS can be checked at a single, central location.

The messages in the Log can be filtered, so that you can see only the relevant data. For information on the filtering function, read the [Local Menu](#) section.

Events concerning only the CMS is available in the same structure under the following path: *Local settings* > *Log*. So the messages about the main CMS are not available in the *Event logs*.

Message reports generated by *Central Alert* and the *Reporting* functions are based on the messages of the *Event logs* element.

By clicking on the *Event logs* option in the tree on the left side, its elements (the event categories) appear. They enable an easy understanding and tracking of the events that are logged. The event categories are available in the [Central Alert](#) section.



Event Logs

The details of an element appear when selecting the element in the right-side window. One entry shows the following information according to which the log can be further filtered:

- *Symbol*: it displays the type of the message. The [Central Alert](#) section describes the event types.
- *Details*: If there is a paperclip icon displayed in the column, the details of the message are available.
- *Date*: the date when the event occurred
- *Message*: the message about the event
- *User*: the user causing the event



Vexira Antivirus Central Management Solution

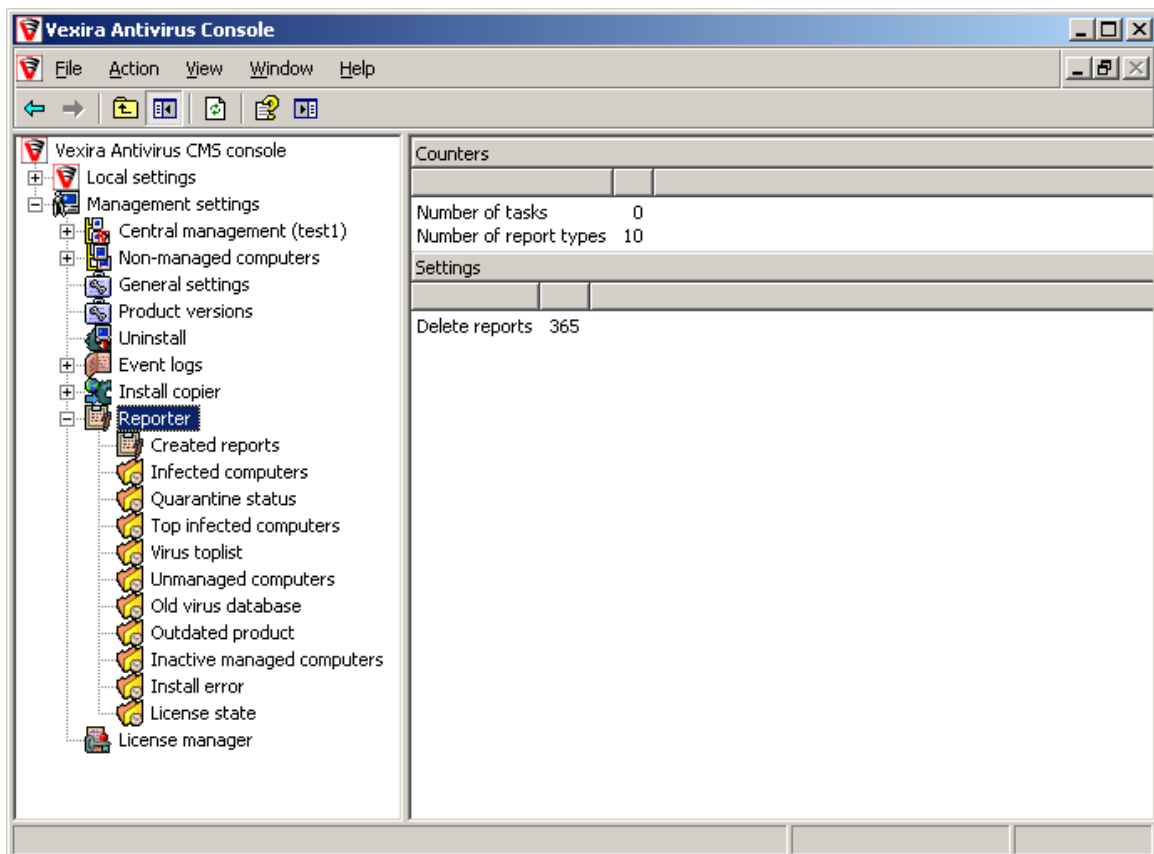
- *Module*: the location of the occurrence of the event

Message details: When double-clicking on the line of the message in the right-side window, a pop-up window appears with the detailed description of the message.



Reporter

With the help of this component, reports, statistics can be created about the status of the management system to inform the user about events, the status of computers and possible problems. With the help of pre-defined report types, reports can be created about the current status of the system and they are available frequently because of scheduling and can be sent in e-mails as well after being generated automatically. You can also create reports on a subCMS, but of course only those report types will be generated which are relevant in that context.



Reporter

By clicking on the *Reporter* component, a window appears on the right side in the *Register* tab. about the number of added tasks and report types In the *Settings* tab, you can specify the number of days for the system to store the given reports. Its default setting is 365 days.

A task must be defined in the reporter for the certain reports to be created once or frequently. The same actions can be performed on the reports specified as on the tasks specified for the reports in the Task manager (but they are not displayed in the task manager). For more information on these actions, refer to the [Task manager](#) section.

If you click on the plus (+) sign in front of the Reporter option, the following elements appear below it in the tree:

- *Created reports*
The previously-created reports that are stored currently by CMS are available here.
- *Infected computers*
It is the list of the computers in the system that are shown as currently infected. The report



Vexira Antivirus Central Management Solution

contains the name and IP address of the computers, threat status, the first detection, the most detected virus, the number of infected files on the computer.

- *Quarantine status*
This list contains the computers that have content in their quarantine. This report includes the name and IP address of all the computers with quarantined elements, the size of the quarantine, and the number of quarantined files.
- *Top infected computers*
This is a complete list of the most infected computers in the order of their infection rate. The report contains the name of the infected computers, the first and last detection, the most detected virus, the domain name, the CMS and group that the computer is assigned to.
- *Virus toplist*
This is a complete list of the most frequently occurring viruses. The report contains the name of the malware, the first and last detection, the number of infected computers, the name and the IP address of the most infected computer.
- *Unmanaged computers*
This is a complete list of the non-managed computers grouped according to their domains. The report contains the name and IP address of all the computers in the network that are not managed by the CMS, their status (online/offline), and the date and time when this status started.
- *Old virus database*
This is a complete list of the computers with old (outdated) virus databases. A virus database is considered old if it was not updated for more than two days.
In certain cases, the report begins with some kind of important additional information, i.e. a warning. If, for example, the virus database on the main CMS is older than 2 days, then the report will contain a warning about a possible malfunctioning of the system. In this case, please check if the operation of the install copier and the network connection to the update source. If a report is generated within 2 hours since an update performed by the install copier, the report warns that the system is being updated, i.e. the data are subject to change, so it is recommended to run the report again a couple of hours later.
- *Outdated product*
This is a complete list of the computers with old (outdated) product versions. A product version is considered outdated if it is older than the version appearing as current in the *Product versions* menu. The report contains the number of managed computers, the list of the up-to-date product versions with the number of computers on which they are installed, the number of computers that have the same version of outdated products grouped according to the product versions, and the number of online computers that have old product versions installed.
- *Inactive managed computers*
This is a list of the managed computers that are currently inactive. The report contains the name and IP address of all the computers that are currently inactive, the date and time since it has been inactive, and a note column where an explanation is displayed in case of an error.
- *Install error*
This is a list of the last errors occurring during installation grouped according to domains, CMSs, or groups. The report contains the name and IP address of the computers and a note column where an explanation is displayed in case of an error.
- *License state*
This is a list of all the license keys. The report contains the license key, the username, the date of expiry, the total and the registered number of license keys and the list of registered products.

If you right-click on a report type, you can create a new reporter task in the *Add menu* point of the local menu displayed. Then a new pop-up window appears where the following can be specified:

- *Task name*
You can enter the name of a new task here.

Note
The name of a reported task cannot be modified after it is created.



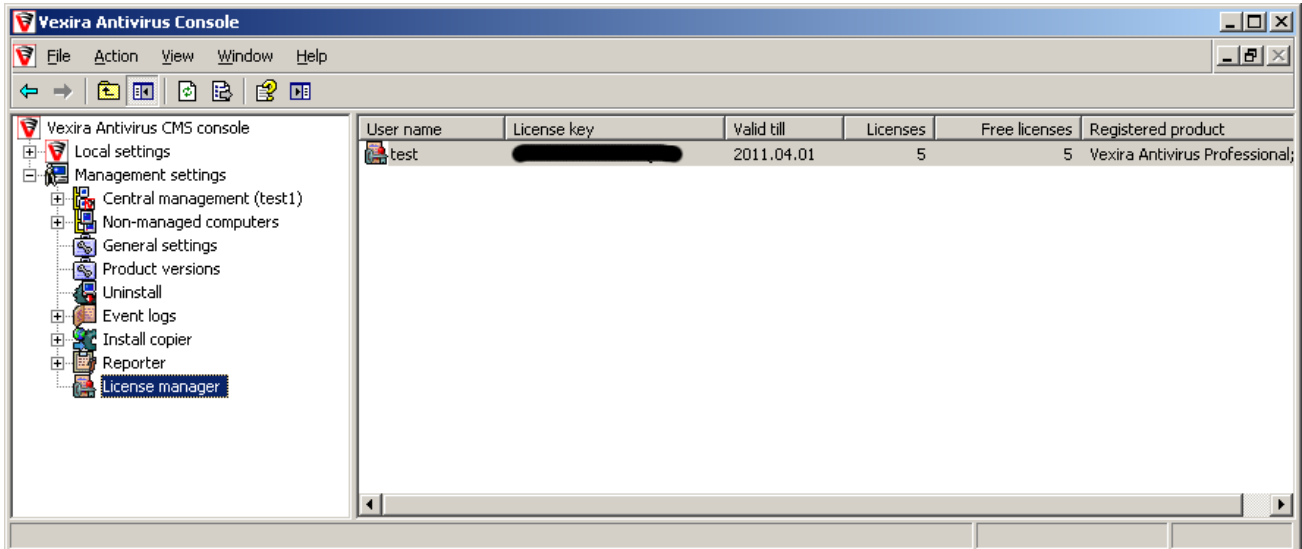
- *E-mail address*
You can enter the e-mail address(es) that receive(s) the reports. You can add several e-mail addresses separated by commas or semi-colons.
- You can specify the period to be included in the report in case of the *Top infected computers* and the *Virus toplist* reports. There are two ways of it:
 - Specifying the *start and end date*: After selecting the checkbox in front of the start and end date menu points, you can specify the date with the help of a calendar and the time (hour:minute:second). The start date must be earlier than the end date, otherwise, the task is not created.
 - Specifying the *period*: After selecting the checkbox in front of the the period menupoint, you can select the period to be analyzed from a dropdown menu; it can be the last day(s), week(s), month(s), complete week(s), complete month(s) with the number specified.

The name of the report type and the date of the report creation are available in the header of the reports. The name and the IP address of the computers are available in the footer of the reports. The system also notifies the administrator if a report has no information to display.



License Manager

The task of the license manager is to store the license key used by CMS and to distribute these to the managed computers and to track the products installed on these computers.



License Manager

By clicking on the component, the added license keys and related information appear in the right side details window. By default, this list is empty. The displayed information is the following:

- *License key*
The license key itself.
- *User name*
Username, which was used when creating the key
- *Valid till*
The expiration date of the license key.
- *Licenses*
One license key can store multiple licenses; therefore, several users can use the same key. The number of all licenses in the key is displayed here.
- *Free licenses*
The number of remaining licenses in the key is displayed here.
- *Registered product*
The displayed products can be registered with the key.

To add a new license key, right-click in the right side window for the local menu to appear and select the *Add* option, specify the *Username* (Registration name) and the *License key*.

When a computer is managed for the first time, it receives a license key from the keys listed here. Besides, an automatic [built in monitoring task](#) is run once a day, which optimizes the distribution of the keys. If a computer cannot receive a license key, CMS cannot register it and it is installed on the computer as a trial version.

If the *Reallocation* option is selected in the local menu, CMS optimizes the distributed keys on the managed computers according to the installed products on these computers.



LOCAL SETTINGS

The modules which are grouped under the *Local settings* node provide general functions for the current product.

General Settings

Security Context for Network Connections

The user account with system administrator permissions in the network of the computer running the main CMS must be specified here. When managing a workgroup, this account is present on all client computers belonging to the network, and it is the means of accessing clients. The account must be specified in the format NETWORK\User (for example, WORKGROUP\Admin).

General Settings

If the *Close dialog after operations* option is enabled, the dialog window (if there is one) is closed automatically after an operation. If it is disabled, the program waits for the user to close the window.

You can change the language of the product by selecting a new language from the available values of the *Language* setting. After selecting a new language, restart the product to apply the new setting to it. For changing the language in the tray menu as well, restart the computer.

Task launching delay: If starting a task is triggered by an event, it may be needed to delay task launching, so that the task can be performed. A task can be scheduled to start at system startup, for example. In this case, it may be needed to delay it for some time after the login process, so that initialization processes can be performed and applications can be loaded. The delay can be set in seconds.

Data collection: With the help of this option, the software can send reports about virus incidents to Central Command to further improve antivirus protection. Information only about the installed product and the detected malware incidents, but no personal data are sent.

Language setting option is only available for the main CMS [1].

SMTP Client

It is possible to send a direct message to Vexira Antivirus from the program if you have a question or a problem. Proper SMTP settings must be specified for this with the following values set:

- *SMTP server*
Name of the server delivering the e-mails, usually this name is given by the Internet Service Provider (ISP) or it is the name of the Exchange server (this information can be found in the mailer client settings /Outlook, Thunderbird, and so on/ or you can ask your system administrator or ISP).
- *Port number*
The port number of the mail server (25 by default).
- *Username*
This name is displayed in the mail you sent us as 'sender'. Tokens can also be used in this field:
%m% - computer name
%u% - username
- *E-mail address*



This is your e-mail address, to which the response is sent.

Log Settings

You can modify the settings of storing log messages here. If you double-click, a pop-up window appears where you can choose the value from a drop-down list. The two elements of this setting are:

- *Storing period of log entries*
You can specify the number of days the system stores log messages here.
Default value: 30 days
- *Maximum number of log entries*
You can specify the maximum number of log messages to be stored by the system.
Default value: 100000

Additional Scan Settings

- *Grayware detection*
If this switch is enabled, the program can detect products in the grayware category and perform the action specified for the applications detected.
Grayware is software which may fall into different categories, depending on its use. Normally, if the user approved the installation and use of these applications, they cannot be considered malware. However, they may also be installed without the user's consent, and their functionalities may be abused for malicious activities. Such software may include ftp server programs and remote access applications. So the presence of such a program in itself is not necessarily harmful. Whether it is harmful or not on a given machine is determined by the circumstances of its installation.
- *Hosts protection*
With the help of this option, the protection of the hosts file of a machine (that is in the System32\drivers\etc folder inside the Windows system folder) can be specified. It is enabled by default.
- *Autorun.inf protection*
With the help of this option, you can set that the autorun.inf files (running software automatically) in CD/DVD and plug-in drives cannot be accessed in order to be protected.
In this option, you can select the protection level of the autorun.inf file from a dropdown menu. The following protection levels are:
 - *Disabled*
The autorun.inf file is available with no restrictions, it is not protected.
 - *Normal*
The autorun.inf file is only readable, but cannot be modified.
 - *Full*
The autorun.inf file is read- and write-protected. This is the default value.Autorun.inf protection is enabled in case of active *Resident protection* for servers.



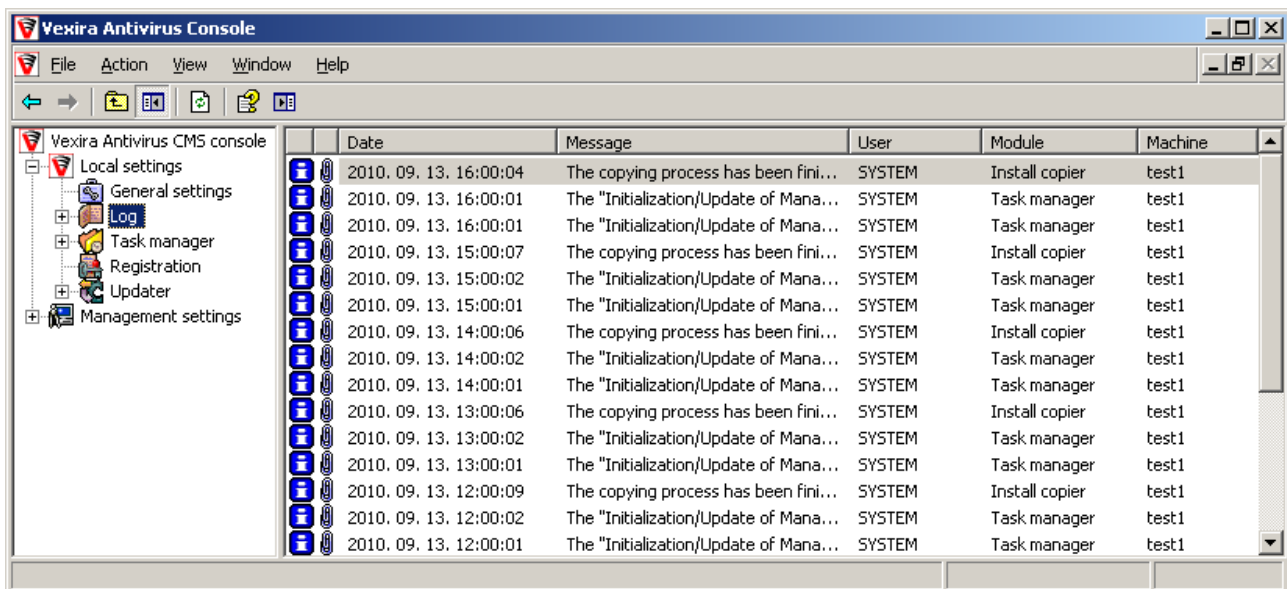
Log

Its main task is to store the messages generated by the various parts (modules) of the software and to forward these to the user if needed.

Physically, the log file is located in the *Bin* folder of the installation path. It is an SQLITE type database file called *local.db*.

The log entries are displayed in the right side details window by clicking on the component. By clicking on the plus (+) sign in front of the component, you can display the icon of the panel containing the other settings of the Log component.

In this log, only the messages about the CMS are displayed. Events about the client machines are available at *Management settings > Event logs*.



Log

Default structure of the messages:

- *Machine*
The name of the computer where the message was created.
- *User*
The name of the user who started the application generating the message.
- *Module*
The name of the module creating the message.
- *Date*
The date when the message was created.
- *Message*
The content of the message.

The first icon indicates the message's type and the second, paper clip indicates if the message has a detailed description.

The program refreshes the list automatically if the new message is created or deleted. The refresh cannot modify the selected item provided it is not the one which has just been deleted.



A local menu appears by right-clicking on the items, in which the separate fields of the messages can be switched on or off and the following actions can be performed:

- *Save as...*
Saves the content of the message to the specified file.
- *Send...*
Sends the message and the log file to the support division of Central Command, Inc. You can finish sending the message in the *Mailer component* window.
- *Refresh*
Refreshes the list.
- *Delete*
Deletes ALL messages from the list.

If you double-click on a message, the details of the message are displayed and you can view its detailed description.

Hiba! A könyvjelző nem létezik.

Central Alert

The task of the component is to send a warning after a new log entry belonging to the category and message type specified appears. This component creates and sends the warnings by using the log messages stored by the *Event log* component. The *Central alert* component requires correct e-mail settings to be able to operate.

Central Alert operation is based on rules (that is, notification settings can be specified in (several) rules). In order to manage rules, select the *Central alert* component in the left-hand tree, then use the local menu (by right-clicking) in the right-hand window. The options are *Add rule*, *Modify rule*, and *Clone rule* (cloning means to create a new rule from an existing one with identical settings).

When adding a new notification rule or modifying an existing one, the following settings of the Central alert appear in a pop-up window:

1. General settings window:

When creating a notification rule, the following must be specified:

- *Rule name*
A unique name to identify the rule.
- *Send detailed message*
You can choose if the system sends a detailed message or not.
- *Type of notification*
E-mail – the notification is sent to a specified e-mail address (Check the mail settings.)
Event logs – the notification is put into the Event logs.
Central database
- *E-mail address* (appears only when e-mail was selected)
The e-mail address Central Alert sends the messages to.

2. Filters settings window:

You can select the events which *Central Alert* sends a message about.
You can choose the event categories and types of the possible filtering settings.
The event categories and types are described below.

3. Flood settings window:



Vexira Antivirus Central Management Solution

You can enable or disable the given rule. The other options are only available when it is set as enabled.

You can specify the period of frequency when to send the notification or the number of messages to be reached when sending the notification.

And you can also set that the system sends the central alert notification automatically when CMS is started.

There is a default rule in the *Central Alert* component that cannot be deleted, only modified.

The event categories are the following:

- *Malware incidents*
It contains messages about malware incidents on a client (every malware detected, suspicious files).
- *Quarantine events*
It contains messages about the quarantine in a client (for example, restoring, rechecking, saving the quarantine, and so on).
- *Management events*
It contains messages about installation on a CMS (for example, remote installation, allocating licenses, messages about the install copier, and so on).
- *Operational events*
It contains messages created during the operation of the antivirus software (for example, enabling/disabling modules, modifying settings, changing the status of the antivirus protection, and so on).
- *Scan events*
It contains messages about virus scanning (for example, corrupt file, starting/stopping scanning, attachment type not supported, and so on).
- *Update events*
It contains messages about antivirus software updates (for example, outdated virus database, update does not start/started/stopped, update with errors, and so on).
- *All events*
It contains all the messages created on the CMS or clients, which enables an easy understanding and tracking of processes (for example, processes running on one client machine).

The event types can be one of the following:

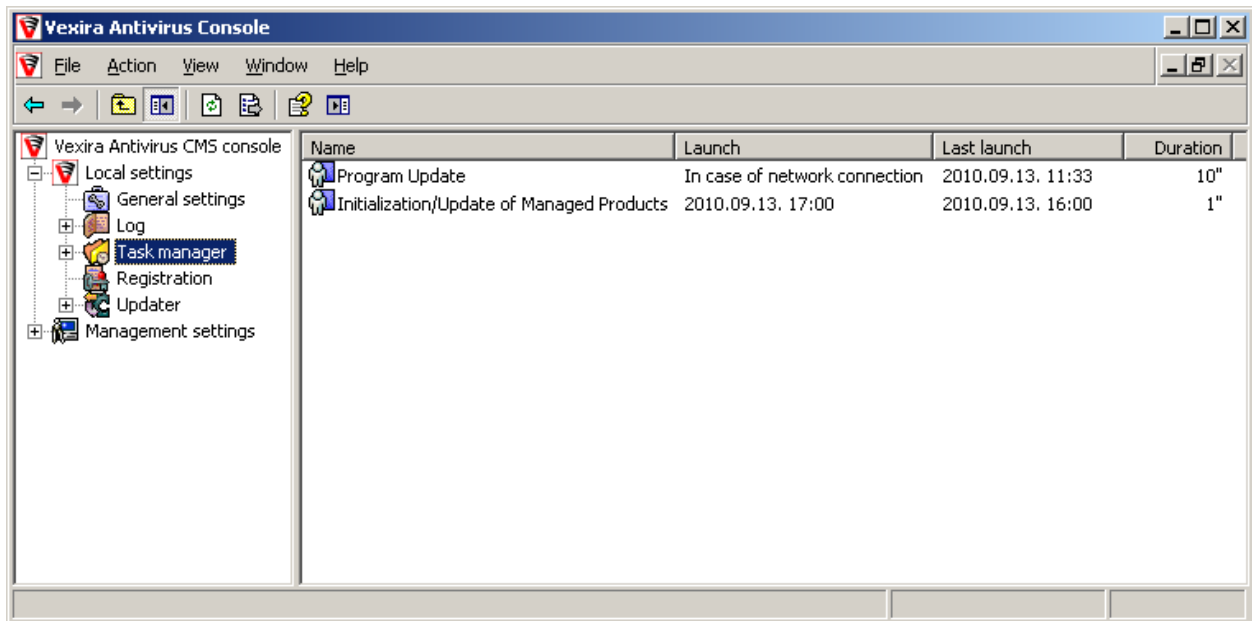
- *Critical*
An event that requires immediate interference (for example, virus database error, scan engine problem, malware detection, and so on)
- *Error*
An event that requires interference (for example, problems with update and installation, lack of license key, and so on)
- *Warning*
An event with lower importance that may cause problems (for example, disabling resident protection, suspicious file detected, file access denied, and so on)
- *Information*
Event not causing any problem (for example, tasks/installation executed successfully)



Task Manager

This component collects all the tasks of the system modules. All tasks added in the program can be managed in this component.

By clicking on the component, all existing (added and default) tasks are displayed in the right side details window. By clicking on the plus (+) sign in front of the component, these tasks are displayed and their types are indicated with the icons in front of them. The icon in front of the name of the task in the details window indicates its status (started, stopped, or paused).



Task Manager

Tasks and Task Settings

You can display the task settings by clicking on it once in the left side list or by double-clicking on it in the details window. The detailed explanation of the settings is available in the section describing the related component.

The following information is displayed next to the name of the task in the details window:

- **Launch**
The method of starting the task. You can read detailed information about this topic in the [Scheduling](#) section.
- **Last launch**
The date when the task was started for the last time.
- **Duration**
The duration of the operation of the task during the last launch.

Functions in the Local Menu

By right-clicking on the task either in the tasks list or in the details window, the local menu appears containing the following functions:

- **Start/Pause/Resume/Stop**

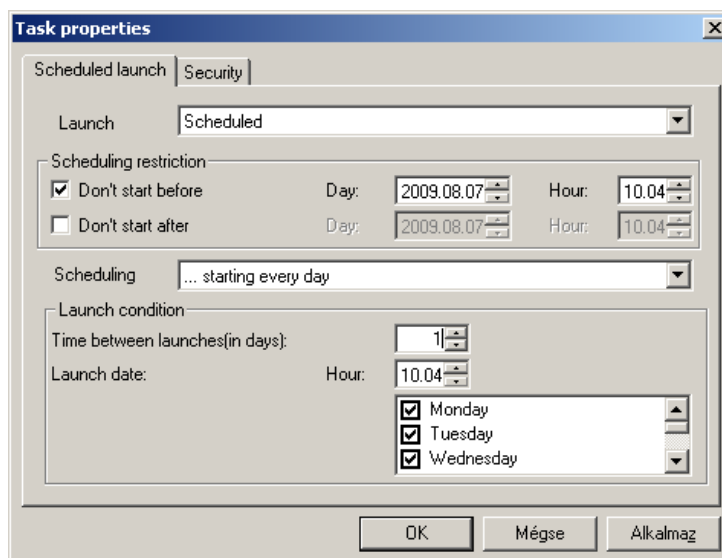


You can start a selected task, pause it, resume a paused task, or stop a running task.

- **Disable/Enable**
It is possible to disable a task. In this case, it cannot be started manually or scheduled until it is enabled again.
- **Manual operation**
It can be used if the task is not started by the user. If you choose this option, the task is set to manual and the user must start it manually. All the specified scheduling parameters are invalid. You can read about scheduling in the [Scheduling](#) section.
- **Modify**
You can modify the selected task settings here. If you select this option, the task settings are displayed in the details window. Default tasks cannot be modified.
- **Delete**
It deletes the selected task from the system.
- **Schedule**
Scheduling of the selected task

Scheduling

You can schedule the task in the local menu. The settings can be specified in a dialog window.



Scheduling

You can select several scheduling options like frequency or a specified date or event. Depending on the task type (update or virus scanning task), the following options can be selected:

- Manual: the task can be started by the user.
- Started in case of a network connection (only in case of virus scanning tasks).
- Scheduled: the start time can be specified in this case.
- Started in case of user login (only in case of virus scanning tasks)
- Started in case of user login and network connection

The *Schedule* type can be selected from a drop-down list:

- Once
- Minutes
- Hours



Vexira Antivirus Central Management Solution

- Days
- Weeks
- Months
- Years

You can set the intervals after which the task must be started on the specified days using the *Time between launches*, *Day and Hour* (hour.minute) settings. For example, if the scan must be started every third week, the *Schedule type* is weekly, the *Time between launches* option is three.

You can assign a user profile to individual schedule settings in the *Security* panel and the task is performed with the specified user's security settings and only if that user is logged in.

- *Anyone*
The tasks are started in case of any user.
- *Default*
The security context of the user defined in the Local settings/General settings panel is used.
- *Custom*
You can specify a custom user.

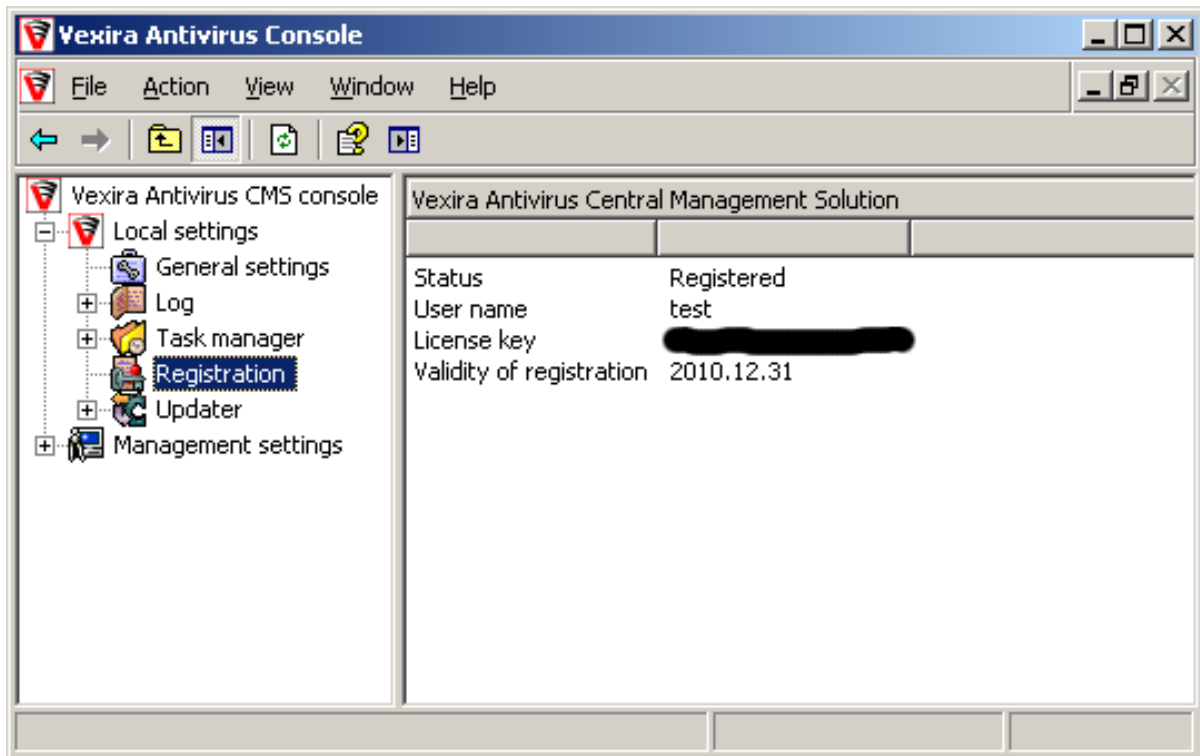
The reports specified in the Reporter are also defined as tasks in the system, but they are only displayed in the Reporter, not in the Task manager.



Registration

The task of this component is to check and store the registration data specified by the user. The registration data includes a username and a license key.

After clicking on the Registration component, the installed Vexira Antivirus products and their registration data are displayed. To modify these, right-click on the registration data of the needed product and select Registration from the local menu.



Registration

Select the needed product in the registration window – this is only needed if several Vexira Antivirus products are installed – and specify the registration data in the appropriate fields and click on the **OK** button. In case of a successful registration, the following items are displayed under the name of the product:

- *Status*: Registered
- *User name*: the specified name
- *License key*: the specified registration code
- *Validity of registration*: the date of expiry, the product is registered until this date.



Updater

Updating the software and the virus database is vital for maintaining the protection effective. The software update is based on tasks: the update can be started with a few clicks or can be scheduled for a date or an event and it is performed with the pre-defined settings.

The product uses an incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program does not need to download the whole virus database file every time (its size is several MBs) but usually only a small additional database package including the virus signatures processed and released recently. Using this mechanism, the download time is decreased to a minimal level, so additional virus database packages can be released several times a day to improve security. Users can obtain protection against new malware without spending a long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses were processed in our virus lab.

By clicking on the Update component, the *Last started update task* and the *Last performed update* information is displayed, which are the following:

- *Task name*
- *Task started*
The date when the task was started
- *Task source*
The update source assigned to the task
- *Tasks result/updated product*
The result of the task/The name of the updated product

The difference between the two groups is that the last started task may not have been successful, but the last performed update was a successful update process.

By clicking on the plus (+) sign in front of the component, the icon of the Source panel and the Tasks folder are displayed, with the help of which the module settings can be modified.

Source Settings

By selecting the Source panel, the available update sources are displayed in the details window. The sources can be activated by selecting the checkbox next to them. If a source is selected, it is possible to perform an update from it, and it can be selected when adding or modifying a task.

The possible update sources and their settings are the following:

- HTTP
Update through the HTTP protocol. Specify the name, of the HTTP server, the used port (default is 80) and path where the descriptor file can be found. The default setting is:
www.upd.vexira.com:80/pub12
If the connection needs a proxy server to access the update source, you can specify additional settings:
 - Proxy
 - *None* – There is no need for a proxy to access the network.
 - *Specified in Explorer* – The application obtains pre-defined proxy settings from Windows Internet Explorer.
 - *Customized proxy* – If this option is selected, you can manually set proxy settings.
 - Proxy server/port – Address and port settings required to access the proxy server.
 - Proxy user/password – Username and password if the proxy server needs authentication.
- FTP



Update through the FTP protocol.

- The following must be specified:
- The name of the FTP server
- The port used by the server (default is 21) and the path
- The path where the descriptor file can be found
- The username and password

If you use the 'Anonymous' username, type your own e-mail address in the password field. The default setting is: [anonymous@ftp.upd.vexira.com:21/pub12](mailto:anonymous@ftp.upd.vexira.com)

- NetWare path
The update can be performed from a Novell NetWare server if the needed path is typed in the field in the UNC format (`\\servername\sharename`).
- Path
The update can be performed from a local or a network drive. The path can be specified by clicking on the `[...]` button.
- CD drive
If the update is performed from a CD, select the letter of the drive from the drop-down list.

Important!

The update can only be performed from a local or a network path if the user is logged in to the domain.

The update can only be performed from a Novell NetWare network path if the user is logged in to the server.

Tasks

After clicking on the Tasks group, all the existing – default and added – tasks are displayed in the details window. The icon in front of the task name indicates its status (started, stopped, or paused).

Tasks can be modified, deleted, or scheduled from the local menu described in the [Tasks and Task Settings](#) section. The method of adding a new task is detailed in the [Adding New Task](#) section.

Update Task Settings

You can select the update source in the *Type* option, where the program checks if there is a new version available. Only active sources that are set in the [Source](#) panel can be selected.

You can select the products to be updated in the *Products to be updated* option.

If the *Dialog window* option is enabled, you can check the update process step-by-step and the program prompts you at every step if the *Interactivity* option is enabled.

If the update source can be accessed through the network, you can specify the information needed for the network connection in the *Network connection parameters* option. If the *Continuous network connection* option is selected, the task does not try to create a connection and it generates an error if the connection is not available. If the *Dial-up connection* option is selected, the task tries to establish a connection and terminates it after it is performed if the task created the connection. In this case, you can specify a password for the connection.

The *Restart computer* option controls the system restart. If you deny it, the computer is never restarted after an update process is finished.

Important!

Do not disable computer restart unless you have a relevant reason to do it, because there may be changes performed during the update process that need computer restart to be activated. If it is disabled, the resident protection of the computer may not be activated and your computer is not protected.



END USER SOFTWARE LICENSE AGREEMENT

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL OR USE THE VEXIRA ANTIVIRUS SOFTWARE (referred to hereafter as the "Software"). BY CLICKING "YES", "I ACCEPT", "I AGREE", "OK", "CONTINUE", "NEXT" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS END USER SOFTWARE LICENSE AGREEMENT (referred to hereafter as the "License"). IF YOU DO NOT ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE, THEN CENTRAL COMMAND, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU. YOU MAY, WITHIN THIRTY (30) DAYS OF YOUR INITIAL PURCHASE OF A COPY OF THE SOFTWARE, RETURN THE ENTIRE COPY OF THE SOFTWARE (INCLUDING ALL COMPUTER MEDIA, PACKAGING AND DOCUMENTATION) WITH PROOF OF PURCHASE EITHER TO CENTRAL COMMAND, INC. DIRECTLY AT ITS CUSTOMER SERVICE DEPARTMENT OR TO THE RETAILER FROM WHICH YOU PURCHASED THE SOFTWARE, FOR A FULL REFUND OF THE AMOUNT INDICATED BY YOUR SALES RECEIPT OR PROOF OF PURCHASE FOR THE SOFTWARE.

IF YOU ARE INSTALLING THE SOFTWARE ON A COMPUTER THAT IS NOT OWNED BY YOU, YOU ARE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE BOTH IN YOUR INDIVIDUAL CAPACITY AND AS AN AGENT OF THE OWNER OF THE COMPUTER, AND YOUR ACTIONS WILL BIND THE OWNER OF THE COMPUTER. YOU REPRESENT AND WARRANT TO CENTRAL COMMAND, INC. THAT YOU HAVE BOTH THE CAPACITY AND AUTHORITY TO ENTER INTO THIS LICENSE ON YOUR OWN BEHALF AS WELL AS ON BEHALF OF THE OWNER OF THE COMPUTER ON WHICH YOU ARE INSTALLING THE SOFTWARE. FOR PURPOSES OF THIS LICENSE, THE "OWNER" OF A COMPUTER IS THE INDIVIDUAL OR ENTITY THAT HAS LEGAL TITLE TO THE COMPUTER OR THAT HAS THE POSSESSORY INTEREST IN THE COMPUTER IF IT IS LEASED OR LOANED BY THE ACTUAL TITLE OWNER.

This End User License Agreement ("License") is a legal agreement between you (either an individual, agent of the owner, or a single entity end user) and Central Command, Inc. for use of the Central Command, Inc. software product identified above (i.e. Vexira Antivirus), which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (collectively referred to as the "Software"), all of which are protected by U. S. copyright laws and international treaty protection. By installing, copying, or otherwise using the Software, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, do not install or use the Software.

The Software and the name "Vexira Antivirus" is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold. If you agree to be bound by all of the terms of this License, you will only own the media on which the Software has been provided and not the Software itself.

THIRTY DAY MONEY BACK GUARANTEE: If you are the original licensee of this copy of the Software and are dissatisfied for any reason with it within the first thirty (30) days after your purchase or delivery date, you may return the complete product, together with your original proof of purchase to Central Command, Inc. or the retailer from which you purchased the Software, for a refund of the amount indicated by your original proof of purchase. If this purchase was completed using electronic delivery you are required to complete a Letter of Destruction (referred to hereafter as an "LOD") and return it within thirty (30) days after your purchase date to receive a refund. Central Command, Inc. uses the postmark or fax date of the completed and returned LOD to determine compliance. You can receive a LOD by contacting your electronic retailer from which you purchased the software or directly from Central Command, Inc. via e-mail at service@centralcommand.com, postal mail at P.O. Box 468, Medina, Ohio, 44258, or fax at +1 330-266-7661. For assistance you may also contact Central Command, Inc. by calling +1 330-723-2062 and requesting Customer Service.

GRANT OF LICENSE: Central Command, Inc. hereby grants you and only you a non-exclusive license to use the Software subject to and upon all of the terms and conditions set forth in this License.

APPLICATION SOFTWARE: You may install and use only one copy of the Software, and only on a single computer terminal.

NETWORK USE: You may also store or install a copy of the Software on a storage device, such as a network server, which is used only to install or run the Software on your other computers over an internal network; however, you must purchase and dedicate a separate license for each separate computer terminal on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers or computer terminals. You are required to purchase a license pack or multi-use license if you require multiple licenses for use on multiple computers or computer terminals.

If you purchase a License Pack and you have acquired this License for multiple licenses of the Software, you may make the number of additional copies of the computer software portion of the Software specified above as "Licensed copies." You are also entitled to make a corresponding number of secondary copies for use on a single home computer as specified above in the section entitled "Application Software".

If you purchase a License for the Software to be used to virus scan electronic messages or you install the Software in such a way to virus scan electronic messages you are required to purchase a license for each domain name and each sub domain name that is virus scanned. If your total electronic mail addresses exceed 6000 you are required to purchase a special Internet Service Provider (ISP) License for use of the Software.



Vexira Antivirus Central Management Solution

TERM OF LICENSE: The License granted hereunder shall commence on the date that you install, copy or otherwise first use the Software. You may terminate this License at any time. This License shall terminate automatically (and you shall have no right to use the Software) upon your breach of any term of this License. Upon termination, you must destroy the Software and all copies, if any, you made pursuant to this License.

UPGRADES: If the Software is labeled as an upgrade, you must be properly licensed to use a product identified by Central Command, Inc. as being eligible for the upgrade in order to use the Software. A copy of the Software labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License. If the Software is an upgrade of a component of a package of software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

COPYRIGHT: All right, title and interest in and to the Software and the name "Vexira Antivirus" and "Vexira" and all copyright rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software), the accompanying printed materials, and any copies of the Software are owned by Central Command, Inc. and/or its suppliers. The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software and the term "Vexira Antivirus" or "Vexira" like any other copyrighted material except that you may install the Software on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the Software. You may not use the name "Vexira Antivirus" or "Vexira" or any similar name except when referring to the Software. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which the Software exists. You may not sub-license, rent, sell, or lease the Software. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for the Software or any part thereof. Except as expressly permitted by applicable law, you may not remove from the Software, or alter, any of the trademarks, trade names, logos, patent or copyright notices or other proprietary rights notices or markings, or add any other notices or markings to the Software.

DATA COLLECTION AND PROCESSION: The Software contains technology and functions which will collect computer files and samples of potentially previously unknown, new or known computer malware, spyware, viruses or other similar potentially harmful computer code, instructions or commands and transmit them to Central Command, Inc. together with information about the computer Operating System, hardware, the computer location such as computer name, domain name, IP address and other software programs which are installed or in operation. As part of this data and information collection and transmission configuration data of the Operating System, the Software and other software programs installed or in operation may be sent. This is only a representative list of a limited set of data and information that could be collected by the technology and functions. It is possible that the transmitted data and information may contain additional data and information not published in this list and may include personal information that could identify you, your computer or other personal information that may be valuable to you. Central Command, Inc. will make an effort to limit the collection of personal data and information however it is possible that the forwarded data and information will contain personally identifiable information and data. Central Command, Inc. will use the data and information obtained only to improve the services and the Software and to react and respond to new malware, spyware and viruses. Central Command, Inc. will also sanitize and repurpose only generic data and information to use within its website and other marketing materials. Central Command, Inc. will handle all data and information as confidential and erase, delete and destroy the data and information as soon as it is no longer necessary to retain. Central Command, Inc. may share and redirect all collected data and information with its affiliated companies, business partners and software development contractors. By accepting this Agreement you full understand and accept that you specifically authorize the collection and use of all data and information that is transmitted and forwarded to Central Command, Inc. and grant Central Command, Inc., its affiliated companies, business partners and software development contractors the consent necessary pursuant to local and international laws and regulations to process, store, retain and repurpose the obtained and collected data and information as it deems appropriate within its website and other marketing materials.

LIMITED WARRANTY: Central Command, Inc. warrants that the media on which the Software is distributed is free from defects for a period of thirty (30) days from your date of receipt or purchase date of the Software. Your sole remedy for a breach of this warranty will be that Central Command, Inc. at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for the Software. Central Command, Inc. does not warrant that the Software will be uninterrupted or error free or that the errors will be corrected. Central Command, Inc. does not warrant that the Software will meet your requirements. **CENTRAL COMMAND, INC. HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR THE SOFTWARE, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.**

DISCLAIMER OF DAMAGES: Anyone installing, using, testing, or evaluating the Software bears all risk to the quality and performance of the Software. In no event shall Central Command, Inc. be liable for any damages of any kind, including, without limitation, direct, indirect, exemplary, special, consequential or incidental damages of any kind (including without limitation lost profits or damage to other systems) arising out of the use, performance, or delivery of the Software, even if Central Command, Inc. has been advised of the existence or possibility of such damages. **SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL CENTRAL COMMAND, INC.'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR THE SOFTWARE.** The disclaimers and limitations set forth above will apply regardless of whether you accept or use, evaluate, or test the Software.



Vexira Antivirus Central Management Solution

IMPORTANT NOTICE TO USERS: THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact Central Command, Inc., at P.O. Box 468, Medina Ohio 44258-0468.

GENERAL: This License is deemed delivered in, and will be governed by, the laws of the State of Ohio, in the United States of America. This License may only be modified by a license addendum, which must accompany this License or by a written document which has been signed by both you and Central Command, Inc. This License has been written in the English language only and is not to be translated or interpreted in any other language. Prices, costs and fees for use of the Software are subject to change without notice to you. In the event of invalidity of any provision of this License, the invalidity shall not affect the validity of the remaining portions of this License. Vexira, Vexira logo, Central Command, Central Command's logo, EVRT, Emergency Virus Response Team, Without us, there's no defense, are trademarks of Central Command, Inc. Microsoft, Windows, Excel, Word, the Windows logo, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks or trade names are the property of their respective owners..

CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address Central Command, Inc.
Medina, Ohio 44258,
P. O. Box 468.
United States

Phone (+1) 330 723 2062

Fax (+1) 330 722 6517

Web <http://www.centralcommand.com>

Support <http://www.centralcommand.com>

E-mail sales@centralcommand.com

support@centralcommand.com