Secure4U - The Application Firewall

Desktop and Network Security

Version 4.1

User Manual

August 1999

This User Manual is part of:
Secure4U Version 4.1

Thank you for choosing *Secure4U* as your personal desktop security manager!

Secure4U Version 4.1 is the first MS Windows based application firewall. With it you gain back the control over your computer and can see what the applications and its installed components are doing!

If you require further information on the *Secure4U* product family or want to know more about other products and services of Advanced Computer Research, please contact us via the Internet at:

http://www.acrmain.com

or

http://www.Secure4U.com

Content

Introduction of Secure4U Version 4.1

SECURE4U V4.1 IS THE FIRST MS WINDOWS BASED APPLICATION FIREWALL! IT OFFERS PROTECTION AGAINST HOSTILE CODE (ACTIVEX, JAVA, TROJAN HORSES, ETC.), A THREAT TO CORPORATE SECURITY NOT ADDRESSED BY CLASSIC FIREWALL AND ANTI-VIRUS SOLUTIONS!

Secure4U v4.1 uses sandbox technology. It is suited for enterprise environments and includes among other features:

- Encapsulation of any application running within the supported OS environments
- Default sandbox for unknown applications
- Cache and Cookie management
- Fine grain generation of configuration sets down to single system objects
- Central configuration tools and deployment support

EMAIL CLIENTS AND OTHER APPLICATIONS

Secure4U Version 4.1 allows encapsulating of any MS Windows application for example MS Outlook.

DEFAULT SANDBOX

Any application, which is not flagged as trusted or known within *Secure4U* can be limited to a default sandbox. With this user definable minimal environment all system resources can be shielded from untrusted, unknown or hostile applications. Thereby additional protection against i.e. Trojan horse programs or application installed by the user within a LAN can be achieved.

ENFORCEMENT OF FILE AND REGISTRY SECURITY ON MS WIN 9X SYSTEMS

Secure4U Version 4.1 allows the enforcement of file and registry access restrictions with settings compatible to MS Windows NT security ACLs (access control lists).

This allows Administrators to enforce a consistent LAN wide access security, even when working with heterogeneous MS Window's network.

INSTALLATION / CONFIGURATION / ADMINISTRATION

Secure4U Version 4.1's administrative tool set allows all *Secure4U* components (general, active content protection, cookie and cache management, virus scanning etc.) to be set up and configured from a single interface.

The installation of the cookie and cache manager is fully integrated in the *Secure4U* configuration / installation process.

WEB BROWSERS

Secure4U include pre-configured sets for the most common web browsers to simplify setup and configuration, Netscape Communicator from 4.01 up to 4.6 and MS Internet Explorer from 3.02 up to 5.0. However, users can create their own configuration sets for any web browser or other application.

VIRUS SCANNING

A number of the most common virus scanners are supported. Additionally user defined custom virus scanners can be used with command line parameters.

CACHE MANAGER

The *Secure4U* Cache-Manager is completely integrated into the *Secure4U* environment and allows the automatic removal of session information in the browser cache, registry and file system.

PERSONAL FIREWALL FUNCTIONALITY

Additional personal firewall features include:

- Blocking all LAN network access for specific / all applications
- Blocking all Internet access for specific / all applications
- Blocking all network access (LAN and / or Internet) for unknown applications
- Blocking / limiting applications to specific IP ports (or sets of IP ports)
- Blocking specific IP addresses

CENTRAL CONFIGURATION

Secure4U can be centrally configured within LANs. By installing the *Secure4U Network Console* on the server the clients can be remotely configured.

For more information about the *Secure4U Network Console* please see the *Secure4U Network Console* User Manual.

Overview

Today the majority of the most active sites on the Internet are using Active content to enhance their presence. Through this new security issues are arising. Active content can be described as extensions to build additional capabilities into the web browsers (e.g. menus, spreadsheets or animations). To create active content, new types of executables (ActiveX, Java) are used in binary form. If your web browser finds a reference in the page you are viewing, it automatically downloads the active content (often from unknown or untrusted sources) and executes the code. In addition to this, through the spread and use of e-mail numerous unknown/untrusted applications are spread through the world and started by unsuspicious users creating substantial threats to their own computers and corporate networks.

This unknown content arriving at your machine might include malicious or hostile code which can damage resources on your computer, snoop into your computer or network for files or information, or make your computer unusable for your daily work. Secure4U protects you both from Active Content (ActiveX, Java, Java Script or VB Script) as well as any other mobile code (any unknown executable) introduced on your system.

Classic Firewalls acting as Gateways for your network and Virus-Scanners do not address these security threats and can not protect you against them.

What is Secure4U

Secure4U continues to be the only commercially available security solution to protect workstations and networks against attacks from any kind of active content (ActiveX, Java and other executable code) received from the Internet or any other untrusted domains.

With *Secure4U* you can create a closed environment (sandbox) around any application (known or unknown) and restrict its access to any of your computer's resources. Within this closed environment any code can run and all accesses calls of the application to system resources, i.e., drivers, the registry database (all your configurations) and the file system, are shielded and constantly monitored to protect your privacy and the integrity of your system.

Secure4U checks for application activities and does not base its security mechanism on a comparison with a database of hostile applet references. It checks all actions and accesses to resources, but only suspicious or unwanted actions are blocked. Hence, it is the first commercially available behavior checker and does not only protect against intended hostile attacks but also against unintentionally buggy applications. Any other applications within your user environment can run and access resources without being restricted by *Secure4U*. You can see which active content and components are installed and running on your computer, where they came from and monitor what a application does and which resources it accesses.

Secure4U generates an additional ring of security within a Windows workstation, transparently layers into your operating system and integrates into existing network security solutions. With this additional ring of security, *Secure4U* can also protect against flaws and holes within the security mechanisms of the web browser and the Java virtual machine.

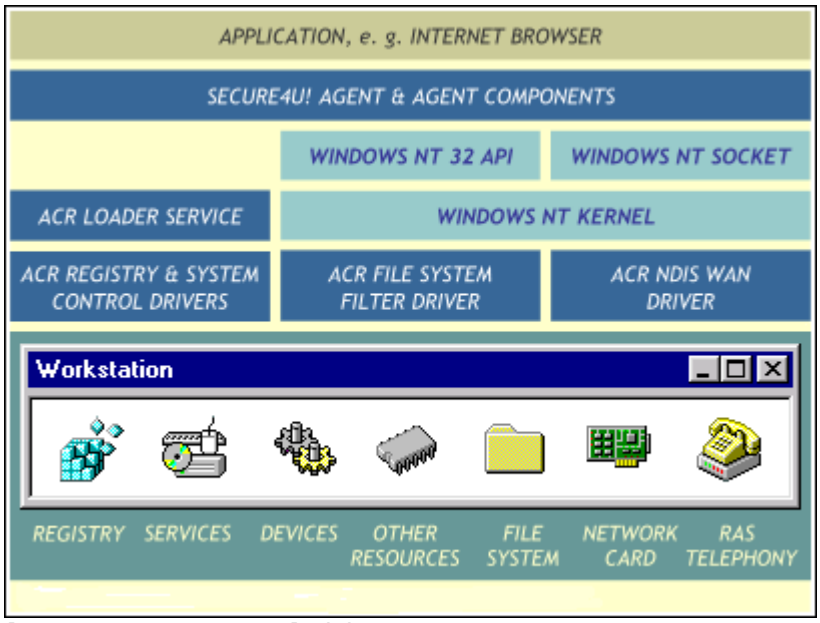
With Secure4U 4.1 installed on your workstation it is possible to:

- Protect the complete operating system and all resources at all times,
- Block and limit any application's access to resources,
- Monitor any activity issued by any application or its extensions,
- Show risk level of action when alerting of suspicious application actions,
- Log all suspicious activities with time, type of action, object accessed, the accessing site and application,
- Indicate when an outside (Internet) connection is alive or an active content enabled web browser is running,
- Inform the user when active content (Java, ActiveX, others) is being installed and started on the computer,
- Display all Applets on the system with their properties, date, time of arrival, executable, origin etc,
- Uninstall suspicious and unwanted Applets,
- Manage and monitor all cache and cookies,
- Enable the administrator to set up additional security policies for active content and cookies,
- Manage access to IP ports,
- Automatically scan all CAB files for viruses and Macro viruses before they install on the workstation.

How and against what does Secure4U protect

Components of Secure4U

Secure4U consist of a series of executables, DLLs and kernel drivers to protect the different parts of your system.



[Secure4U Components] Dialog

Each of the components fulfills a certain task to build a bulletproof protection wall around your system.

The Secure4U agent
The *Secure4U* agent is your interface to the *Secure4U* security solution and displays information to the user. It also monitors restricted accesses to your system's environment and resources.

The Secure4U kernel components
The *Secure4U* kernel components deliver extended protection against certain low level accesses and protect the *Secure4U* runtime environment.

The Secure4U Administrator Tool
With the *Secure4U Administrator Tool* you can quickly install and configure *Secure4U*. The *Secure4U Administrator Tool* scans your system for installed applications and automates most settings for the installed web browsers. A typical installation of *Secure4U* will take you minutes to complete.

The Hostile Applet Database
The database with hostile applet references is an additional security feature of *Secure4U*. These references are used to give additional warnings about received active content or block these applets automatically.

Protection of System Resources and Data

Secure4U protects the following resources within your computer against unwanted and suspicious accesses and changes:

- **The Registry**
  Within the registry database MS Windows 9x and MS Windows NT save all system and application configurations. If a hostile applet changes settings within the registry database it might leave applications or your whole system unusable. By changing the registry database a hostile applet can also gain unwanted access to resources on your computer.

- **Access to Services**
  Secure4U monitors all access to system services issued from your web browser. By changing setting of particular services, stopping services or accessing certain services a hostile applet can make your computer unusable or gain unwanted access to resources or data.

- **Access to Devices**
  By changing setting of your system devices or accessing them a hostile applet can make your system unusable or block access to these devices.

- **Access to the File System**
  By accessing the file system an applet gains access to all your data and files. *Secure4U* restricts access to the file system based on its configuration. You will typically set a directory for saving information received from the Internet and block access to all other areas for your web browser.

- **Access to your Local Area Network (LAN)**
  When a hostile applet access your LAN it can gain access to all network resources and files you have access to. *Secure4U* closely monitors all access to network resources issued by your web browser and by default will block all accesses.

- **Access and monitoring of IP Ports**
  Any use of IP ports by your restricted applications is monitored by *Secure4U*. By using certain IP ports an applet can e-mail information to the Internet or connect by any other protocol.

Monitoring and managing Active Content
With *Secure4U* you can monitor all installed applets on your computer. You see when a new applet comes on board and when applets become active. You can find out who created the applet, from which site it was downloaded and how it interfaces with your system. Any installed applet can also be deleted.

Database with Hostile Applet References
As an additional security feature we have added a database with references of hostile applets to *Secure4U*. When an applet comes on board it is automatically checked against the entries within this database. If *Secure4U* finds a reference for the applet it will issue an additional warning to the user or automatically block the starting of the applet.

Communication Monitoring
Secure4U also checks access to IP ports to block unwanted access or use.

Logging of Application Activities
Any activity of your restricted applications is displayed in the *Secure4U* activity window and can be saved to the MS Windows NT application event log file. You can configure *Secure4U* to log all activities, or only monitored, blocked and alerted activities to the MS Windows NT application log. These log files can then be accessed with the MS Windows Event viewer.

Scanning for Viruses
If you have a virus scanner installed that *Secure4U* supports, all CAB files received through your web browser will be opened by your browser and scanned for viruses and Macro viruses before they are installed on the computer. To undertake the actual virus scanning process, *Secure4U* calls a virus scanner installed on your computer through an API or command line. *Secure4U* can use the most common virus scanners.

Managing Cookies
A Cookie-Manager is included to maintain and handle all cookies for all users / profiles on a computer and to restrict cookie placement by web site / URL.

Managing Cache
A Cache-Manager is included to maintain and handle all cache and thereby gain back disk space and enable you to protect your privacy by removing traces of Internet sessions within the system.

What can happen if I don't protect my computer

When your computer is not protected by *Secure4U* hostile or malicious applets might access any files or resources on your computer/LAN you have access to. Your computer is wide open to anybody on the Internet with malicious, destructive or criminal intention. Recent studies and surveys stated out that most corporate networks and computers connected to the Internet have been attacked and reported damages by illegal accesses from the Internet or through the use of email attachments. Malicious mobile code (ActiveX, Java as well as other executables) is more and more used to issue these attacks.

The following list outlines the most common attacks:

- **Deleting of Files**
  An applets is deleting system or user files in the background while running on your computer. This attack can make your computer / operating system unusable and lead to loss of data and information.

- **Denial of Service**
  By changing the configuration of your operating system or applications your system or parts of it can become unusable.

- **Theft of Information and Data**
  An applet can access data and files on your computer and send them to any computer (e.g. to your competitors) on the Internet via email or by issuing certain HTTP commands.

- **Remote Access to your computer via the Internet**
  An applet can generate a proxy on your computer enabling computers on the Internet remotely accessing all resources on your computer or your LAN.

- **Installation of Unwanted/Hostile Application**
  An applet could change your system configuration in a way that the next time you start your computer a hostile application is automatically started. This application could then undertake all its malicious tasks in the background or block access to particular or any resources on your computer.

- **Manipulation of your Internet Connection**
  An applet could filter, manipulate or falsificate all information sent or received from the Internet.

- **Impersonation**
  An applet could impersonate with your User ID on the Internet or your local area network and initiate malicious, destructive or unwanted actions. It therefore could also use personal or sensitive information collected from your computer (e.g. credit card information)

Getting started

System Requirements

To install *Secure4U* on your computer the following is required:

- PC with Intel Pentium Processor

One of the following operating systems:

- MS Windows 95
- MS Windows 95 with Shell integration
- MS Windows 98
- MS Windows NT 4.0 (Service pack 3, 4 and 5)
- MS Windows NT 4.0 SP 3, 4 and 5 with Shell integration
- (MS Windows NT 5.0 / MS Windows NT 2000) Beta version.

- 15 MB hard disk space

Secure4U include pre-configured sets for the most common web browsers to simplify set up and configuration:

- Netscape Communicator from version 4.01 up to 4.6
- MS Internet Explorer from version 3.02 up to 5.0

Please Note: If you are using MS Internet Explorer we recommend setting the advanced options to "Browse in a new process." This is found in MS Internet Explorer 4.0 in View/Internet Options/Advanced/Browsing/Browse in a new process and in MS Internet Explorer 5.0 in Tools/Internet Options/Advanced/Browsing/Browse in a new process.

Users can create their own configuration sets for any other web browser or application.

PLEASE NOTE: TO INSTALL *SECURE4U* UNDER MS WINDOWS NT YOU NEED TO BE LOGGED ON AS ADMINISTRATOR FOR THE COMPUTER.

Installing Secure4U

To install*Secure4U* on a MS Windows NT workstation **you need to be logged in as administrator or** as a **user with administrator rights**. If you do not have administrator rights to your computer please contact your network support team or the administrator for your computer.

download **Installing via ESD:**

After downloading the installation file from the Internet run the SETUP.EXE file from the MS Windows Start Menu with the [Run] command or double click the file in the MS Windows Explorer. The installation of *Secure4U* will then automatically unpack all necessary files and start the setup program.

 **Installing from CD-ROM:**

While running *MS Windows* insert the *Secure4U CD-ROM* into your CD-Drive. The installation program for *Secure4U* will automatically start. If your CD-Drive does not start the installation automatically, run SETUP.EXE directly from your CD-Drive. The installation of *Secure4U* will then ask you for the necessary entries and settings.

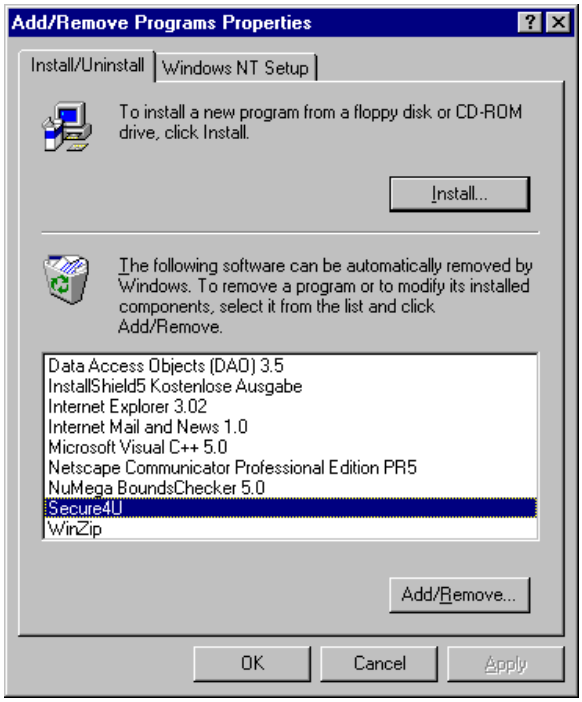
Removing Secure4U

To uninstall *Secure4U* on a computer running MS Windows NT you have to be logged on as Administrator for your computer.

When *Secure4U* is running unload it first with the *Secure4U Unloader Tool*.

Then open the MS Windows Control panel.

Click on the [Add/Remove Programs] symbol to open the following dialog:



[MS Windows Add/Remove Programs] dialog

Within this dialog select *Secure4U* from the list of installed programs and click the [Add/Remove] button. The *Secure4U uninstall program* will then start and remove all *Secure4U* files and registry entries from your system.

Manually removing Secure4U

If the deinstallation of *Secure4U* did not complete properly or certain parts could not be removed from your computer, you can also manually remove *Secure4U* from your system.

Note: *Before manually removing Secure4U you should first use the Secure4U uninstall program from the Control panel to remove at least parts from your system.*

To manually remove *Secure4U* from your system, perform the following steps:

Note: These steps should be undertaken by experienced users or administrators only! Errors within manually removing Secure4U might lead to undesirable results and problems in running MS Windows.

MS Windows NT

1. Log on as Administrator
2. If *Secure4U* is running, unload it with the *Secure4U Unloader Tool*
3. Remove all *Secure4U* files from the *Secure4U* working directory (e.g. C:*Secure4U*). Then delete the *Secure4U* working directory.
4. Start the Registry editor
5. Delete the *Secure4U* tree and all keys under:
   HKEY_LOCAL_MACHINE\SOFTWARE\ACR\Secure4U
6. Open the Command prompt (DOS box)
   Enter the following commands:
   NET STOP agentsvc
   NET STOP krnguard
7. Remove the following keys in the registry:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AgentSvc
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KrnGuard
8. Remove the reference to filespy.dll under
   HKEY_LOCAL_MACHINE\ SOFTWARE\ MICROSOFT\Windows NT\CurrentVersion\Windows\AppInit_DLLs
9. Reboot your system
10. Delete the file FILESPY.DLL from MS Windows SYSTEM32 directory.
11. Delete the *Secure4U* program group with its shortcuts from all user profiles.

MS Windows 9x

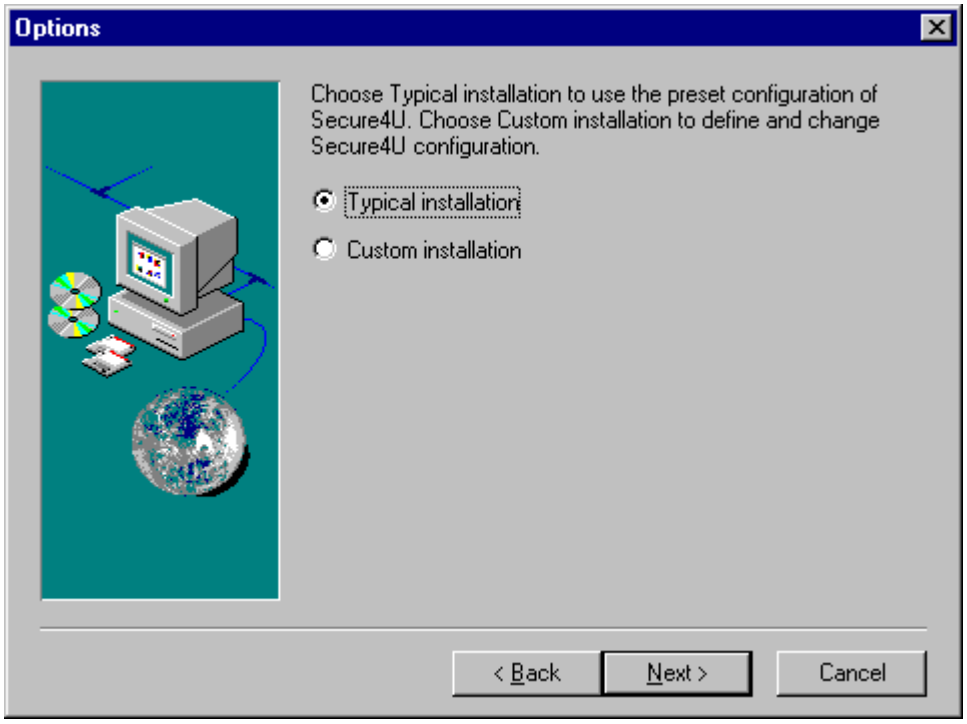
1. If *Secure4U* is running, unload it with the *Secure4U Unloader tool*
2. Remove all *Secure4U* files from the *Secure4U* working directory (e.g. C:*Secure4U*). Then delete the *Secure4U* working directory.
3. Start the Registry editor
4. Delete the *Secure4U* tree and all keys under: HKEY_LOCAL_MACHINE\SOFTWARE\ACR\Secure4U
5. Remove the following keys in the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Vxd\Guard
6. Reboot your system
7. Delete the *Secure4U* program group with its shortcuts.

Secure4U Wizard

In the Install Shield wizard you are asked to select for one of the following installation routines:

- Typical Installation (Using the *Secure4U Wizard* for easy setup).
- Custom Installation (Uses no Wizard, you will be shown directly to *Secure4U Administrative Tool*).

Please Observe! It is not recommended to use Custom Installation of Secure4U unless you are already familiar with *Secure4U* and the *Secure4U Administration Tool.*



If you select Typical Installation then, after the *Secure4U* Installation program has installed all necessary files on your computer, *Secure4U* will automatically start the *Secure4U Wizard* to configure your *Secure4U* installation.

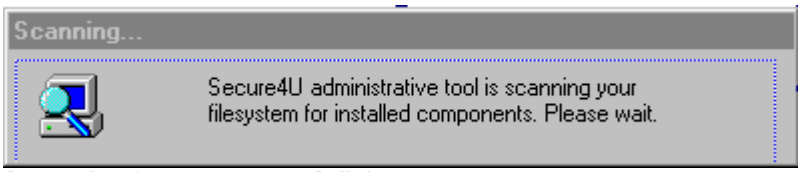
During the configuration the following steps are undertaken:

- Searching for all installed components on your computer
- Select download directory
- Selecting the virus-scanner to be used by *Secure4U*
- Setting up the cookie-management
- Setting up the cache-manager

NOTE: A silent Installation can be done when installing *Secure4U* through some remote network installation programs. Please see the chapter Deploying and using Secure4U within LAN's in this manual.

1. Searching for all installed components on your computer

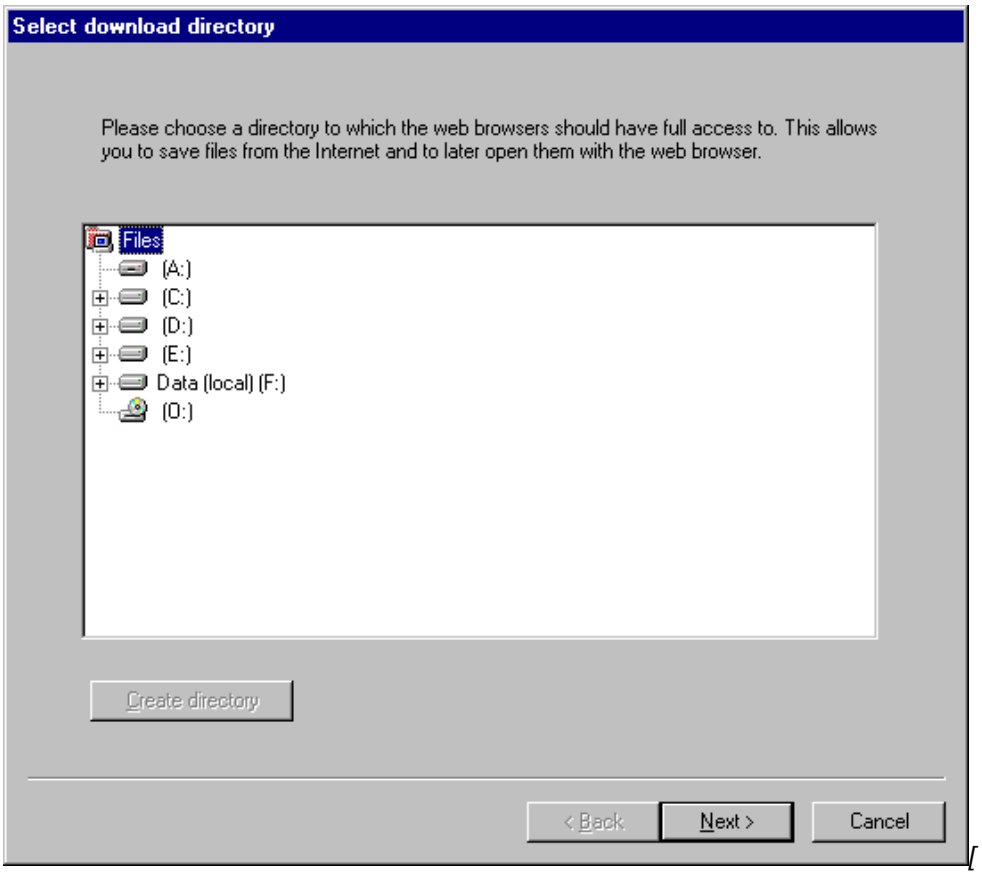
When the *Secure4U Wizard* is started it automatically scans all hard disks within your computer for installed components.



[Scanning for components] dialog

2. Select download directory

Then the Wizard will ask you to please choose a directory to which the web browser should have full access. This allows the user to save downloads from the Internet/Intranet and later open them with the web browser.

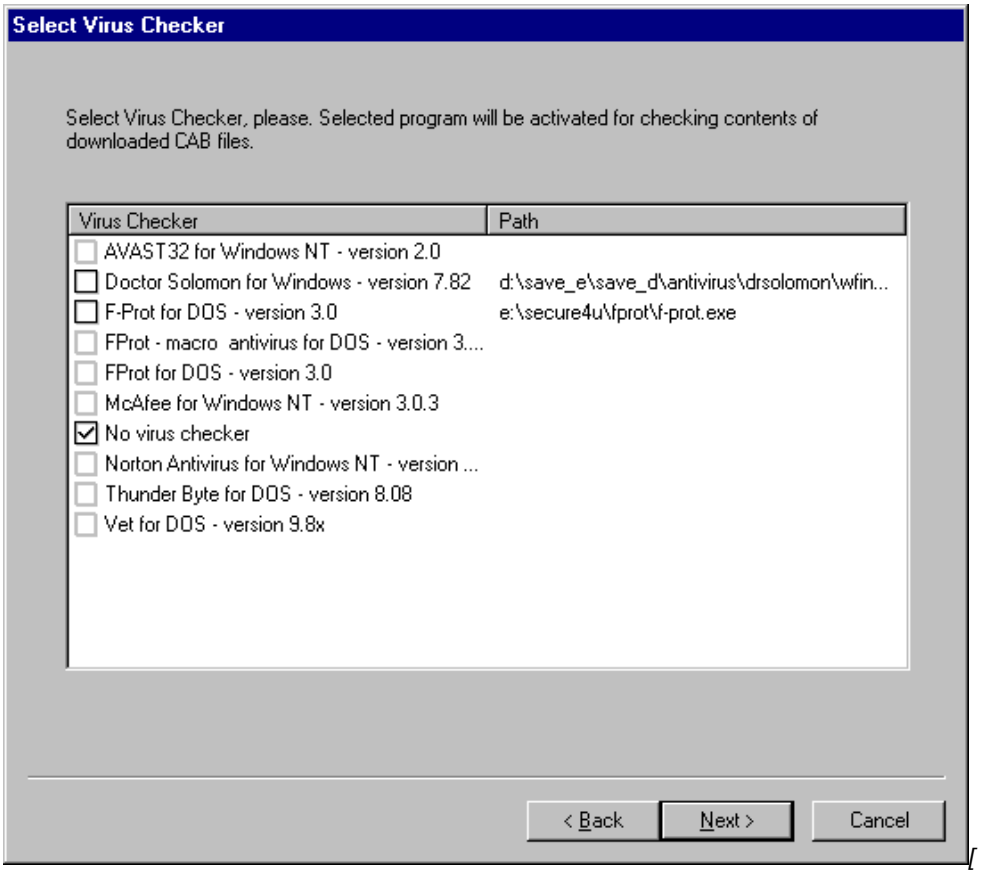


Select download directory] dialog

By clicking [Next] you move to the next section.

3. Selecting the virus scanner to be used by Secure4U

After having searched your hard drives for installed components all virus-scanning software found by *Secure4U* will be displayed and the following dialog is opened:



[Virus scanner] dialog

Within the list box *Secure4U* displays all found virus-scanners it can use. *Secure4U* comes with a copy of the popular F-Prot virus scanner, which is copied to your hard disk during installation of *Secure4U*.

***Note**: If you select this virus scanner, please visit the F-Prot / Datafellows web site (http://www.datafellows.com) and check for the latest virus data files.*

Secure4U supports the most widely used virus scanners on the market. A list of virus scanner, *Secure4U* can use for automatic virus scanning of incoming documents, component and archives, is available in the support area of the *Secure4U* web site (http://www.Secure4U.com/Support/).

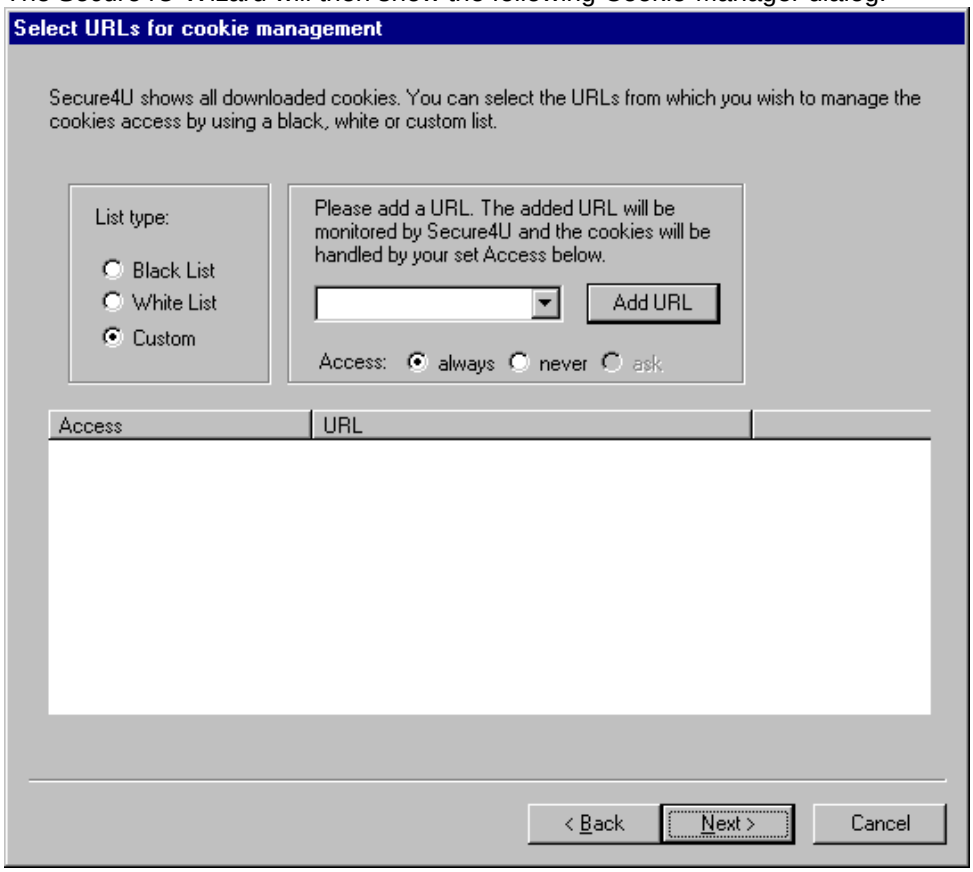
Additionally user defined custom virus scanners can be used with command line parameters. To do this please see the chapter *Secure4U Administrator Tool* about how to configure a virus scanner.

After selecting one entry from the above list, click the [OK] button and the configuration will continue.

By clicking [Next] you move to the next section.

4. Setting up the Cookie-Manager

The *Secure4U* Wizard will then show the following Cookie-Manager dialog:



[Cookie-Manager] dialog

How does the Cookie-Manager work?

You can here create a list of sites and restrict/allow cookies from them to be saved on your computer. You can either type in URLs directly or use the customer list, self-learning mode, when accessing a site. When a cookie tries to install on your computer, the *Secure4U* Cookie-Manager checks its configured cookie list if the URL/site the cookie was received from is registered or not. Depending on the set policy the Cookie-Manager undertakes the action set for this site. The following actions can be set up for the Cookie-Manager for each entry in the list:

- **Never save (Always block)**
  If a cookie from this URL/site is received it will automatically be blocked. No cookies from this URL/site are allowed
- **Always ask**
  If a cookie from this URL/site is received the Cookie-Manager will display a dialog to set actions for this cookie and URL/site.
- **Always save**
  If a cookie from this URL/site is received it will be automatically saved on your computer. You will see an entry in the *Secure4U* activity window that the saving of the cookie was granted.

Select the type of list you want to use (Black list, White list, Custom list)

Secure4U allows you to set up the Cookie-Manager in a way that best fits your needs. Each type of the cookie list fulfills different run time requirements and approaches to stop unwanted cookies. You might choose or change to a different list type after adding Sites/URLs to a list. All your entries will remain within the list of the new type while related actions might change to the corresponding type within the new list.

Black list: If this list type is chosen, all cookies from the Sites/URLs included in the list, will automatically be blocked from being installed on the computer. The cookies from all other Sites/URLs will be allowed to install on the computer. For each entry in the list you can set the *Secure4U* action to:

- Never save (Always block)
- Always ask

White list: If this list type is chosen, only the cookies from the Sites/URLs included in the list will be saved. All other will automatically be blocked. For each entry in the list you can set the *Secure4U* action to:

- Always save
- Always ask

Custom list: With this type of the cookie list, *Secure4U* will ask you when a cookie arrives from all Sites/URLs which are not included in the list. You can then decide if you want to block/allow this or all cookies from the current URL.
For each entry in the list you can set the *Secure4U* action to:

- Always save
- Never save (Always block)

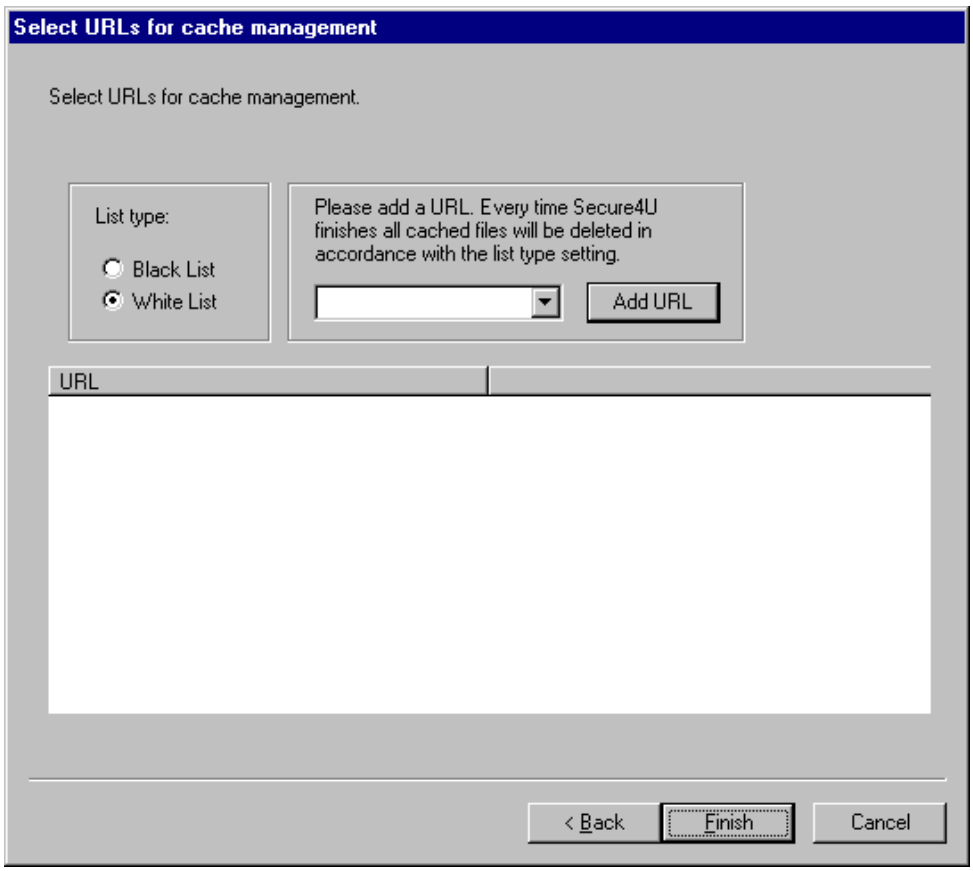
We recommend using the Custom list, at least for some time as many sites on the Internet use different URLs for the cookie placement (i.e. excite.com / preferences.com). Also the URL resolving mechanism within this version of the *Secure4U* cookie manager needs the precise address to be able to properly block all cookies from a site. The Custom list can also be used as a self-learning mode for the other two list types.

For more information on the use of the Cookie-Manager please turn to the chapter *Secure4U Administrator Tool* and *Cache & Cookies.*

By clicking [Next] you move to the next section.

5. Setting up the Cache-Manager

The *Secure4U* Wizard will then show the following Cache-Manager dialog:



[Cache-Management] dialog

How does the Cache-Manager work?

Data arriving on your computer are stored in cache files. The stored cache may take up a lot of memory space on the computer if not deleted from time to time. In addition it is possible to track Internet sessions through the stored cache files. The *Secure4U Cache-Manager* allows the automatic removal of session information in the browser cache, registry and file system. When *Secure4U* is turned off the Cache-Manager checks if it finds the URL/site the cache was received from its configured cache list. If the URL/site was found, the Cache-Manager undertakes the action set for this site. If the URL/site could not be found in the list, the action undertaken depends on the type of cache list selected. The following actions can be set up for the Cookie-Manager for each entry in the list:

Select the type of list you want to use (Black list, White list)

Secure4U allows you to set up the Cache-Manager in a way that best fits your needs.

Black list: If this list type is chosen, all cache from the Sites/URLs included in the list will automatically be removed from your computer when Secure4U is turned-off. The cache from all other Sites/URLs will be spared.

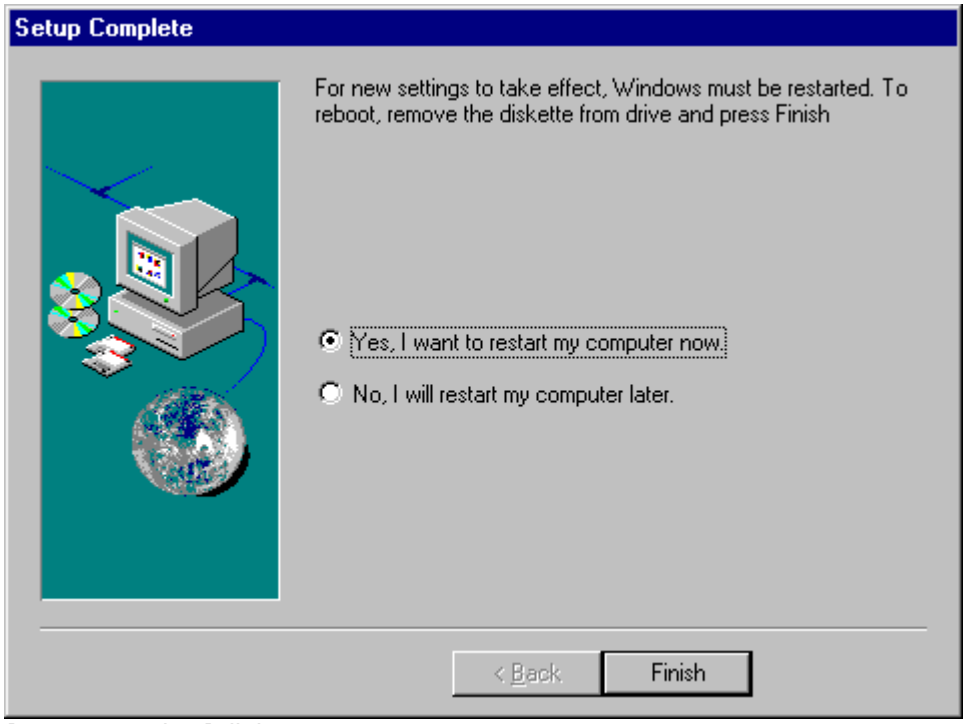
White list: If this list type is chosen, only the cache from the Sites/URLs included in the list will be spared when Secure4U is turned-off. The cache

from all other Sites/URLs will automatically be removed from your computer.

You find more information on the use of the Cache-Manager in the chapter *Secure4U Administrative Tool* and *Cache & Cookies.*

By clicking [Finish] you move to the next section.

The InstallShield will show you the following dialog:



[Setup Complete] dialog

Congratulations the Setup is complete. In order for *Secure4U* to function you need to restart the computer.

Please Note: If you are using MS Internet Explorer we recommend setting the advanced options to "Browse in a new process." This is found in MS Internet Explorer 4.0 in View/Internet Options/Advanced/Browsing/Browse in a new process and in MS Internet Explorer 5.0 in Tools/Internet Options/Advanced/Browsing/Browse in a new process.

Secure4U Display

Overview

After a typical installation you find *Secure4U* displayed in the Start Menu and if selected the following dialog will be shown:

[Secure4U Display] dialog

The next chapters will describe the functionality of the three shown items.

Secure4U Agent

Overview

By selecting *Secure4U* in the Start Menu, the *Secure4U Agent* will be started.

Unloader

Overview

By selecting *Unloader* in the Start Menu, *Secure4U* will be closed and removed from memory.

Secure4U Administrator Tool

Overview

The new *Secure4U Administrator Tool* provides a single consistent interface and allows an administrator to interactively configure all parts and components of *Secure4U* on a particular machine.

During installation of *Secure4U* the *Secure4U* installation program automatically runs selected parts and wizards of the *Administrator Tool*.

Like an inventory list the *Administrator Tool* displays all protected system objects on a particular machine. Furthermore it enables the administrator to enumerate and set up fine grain restrictions by access type and *Secure4U* activities for each single system object.

[Secure4U Administrator Tool] dialog

The *Secure4U Administrator Tool* uses an MS Explorer like interface with two panes, whereby the left tree contains all components of the *Secure4U* configuration and the right pane displays additional information about the selected item in the tree.

With this approach setting restrictions of a particular component, i.e. a download directory, for multiple applications at once, is far simplified.

Within the left pane (component tree) you will find the following two top-level branches:

- **The current local *Secure4U* configuration (The item in the tree is displaying the local computer name)**
- **The *Secure4U* default configuration**

The current local Secure4U configuration

Within this top-level branch you can enumerate and setup the *Secure4U* configuration of your computer. Each of the included components within a *Secure4U* configuration is described in detail in the following chapters.

The Secure4U default configuration

The *Secure4U* default configuration branch contains default file components and default registry components**.** These settings are loaded from the basic configuration file, which is used during installation of *Secure4U*. Further information on the *Secure4U* default configuration can be found later in this document.

System Configuration

Within this *Secure4U* configuration component you can enumerate and set up access rights for core system components and functionality (i.e. system shutdown access). You also can limit resource quotas of applications for the number of windows and the amount of memory they can use.

To setup the system configuration component, do the following:

Select the [System] component in the Local configuration branch of the tree pane

[Secure4U Administrator Tool] dialog

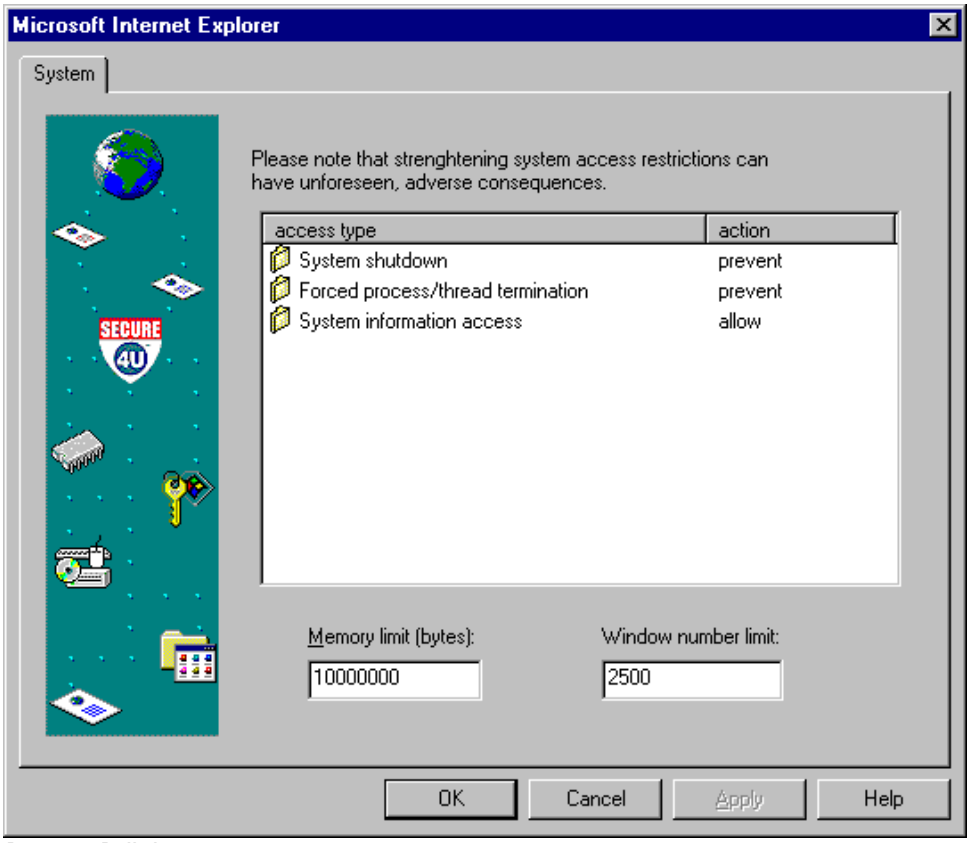
The *Secure4U* Administrator will then display a list of restricted applications in the right window pane.

Within this list double-click the entry you would like to configure. You can also right-click the entry and select [Properties] within the displayed popup menu.

Hint: You also can select multiple entries in the list to set their configuration at once.

The entry [Unknown application] will configure restrictions and *Secure4U* activities for the Default sandbox.

The *Secure4U Administrator Tool* will then display the following dialog box



[System] dialog

The *Secure4U* Configuration items you can setup here are:

- System Shutdown access
- Forced process / thread termination
- System information access
- Memory quotas
- Windows / GUI resource quotas

WARNING: Changes to the default configuration Secure4U sets during installation for these items might lead to potential problems with the applications you are restricting. Certain application might not even run when you are too restrictive. We recommend not changing these settings!

The following settings are available for each of the items:

Setting	Secure4U activity
Allow	Secure4U will grant all access of this type
Monitor	Secure4U will monitor all access of this type
Block	Secure4U will ask the user for granting the access or blocking it (interactive blocking)
Prevent	Secure4U will automatically block and monitor all access request of this type

To change a setting for an item right-click the item and select the required *Secure4U* action from the Pop-up menu.

The following gives a brief description of the currently available *Secure4U* configuration items:

System Shutdown Access
When this option is set to prevent, no system shutdown requests will be allowed to the selected application. *Secure4U* can also warn you when a request of this type is in the queue and gives you the possibility to grant this request.

Forced Process / Thread Termination
When this option is set, all thread and process manipulation of the selected application are restricted in accordance with the set policy by *Secure4U*. *Secure4U* can also warn you when requests of this type are in the queue and give you the possibility to grant these requests or will automatically block them.

System Information Access
When this option is set to monitor accesses and reading of system information, for instance type of operating system, the name of the current user etc., are monitored by *Secure4U*. If any of these accesses occurs it is displayed in the Secure4U activity windows.

Memory Quotas
With this number you can limit the amount of memory the selected application can allocate for its use. The number you enter here is the number of bytes, which the application or instances of a particular application will be allowed to allocate before *Secure4U* will reject further requests of memory allocation from the particular program.

Limiting the amount of memory one application with its instances is allowed to use can protect against various denial of service attacks.

Windows / GUI Resource Quotas
With this number you can limit the number of windows the selected application can open. The number you enter here is the number of windows or controls, which the application or instances of a particular application will be allowed to open before *Secure4U* will reject further requests to open new windows from the particular program.

Limiting the number of windows one application with its instances is allowed to open can protect against various denial of service attacks.

Activation of changes / settings
Memory and Windows quotas become active after the specific application is restarted.

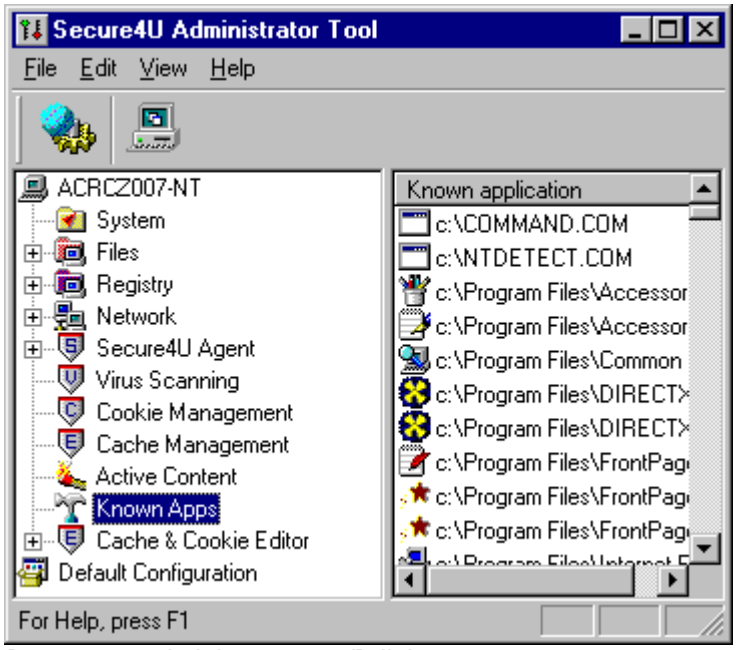
Known, Restricted and Unknown Applications

Secure4U divides the applications into three groups:

- **Known**
- **Restricted**
- **Unknown**

Known Applications

Secure4U uses this configuration component to exclude known and trusted applications from any restrictions.



[Secure4U Administrator Tool] dialog

During installation *Secure4U* scans local drivers and includes all found non-restricted applications in this list. We recommend that you review the listed applications after installation to make sure you know all the applications installed on your computer.

If an application is not included in the Known Applications list or as a restricted application, *Secure4U* will handle it as an unknown application . Hence, it will either be restricted with a specific *Secure4U* configuration for single applications or limited to the default sandbox.

Please Note! Secure4U does not scan for applications located on network drives or other network resources. Used "Known Applications" located in these locations should be manually added to the configuration. If they are not, Secure4U will treat them as unknown applications and restrict them in accordance with the set policy.

To add or remove applications from the Known Application list right-click the list in the right hand window and a popup menu with two alternatives, Add and Remove, will be displayed.

Add

To add a new entry to the list right-click the list and select the [Add] command in the popup menu. Within the then displayed dialog select the application path and specify other settings for this program.

Remove

You can remove entries in the list by right clicking an entry and selecting the command [Remove] from the Popup menu. *Secure4U* will treat a removed known application as an unknown application.

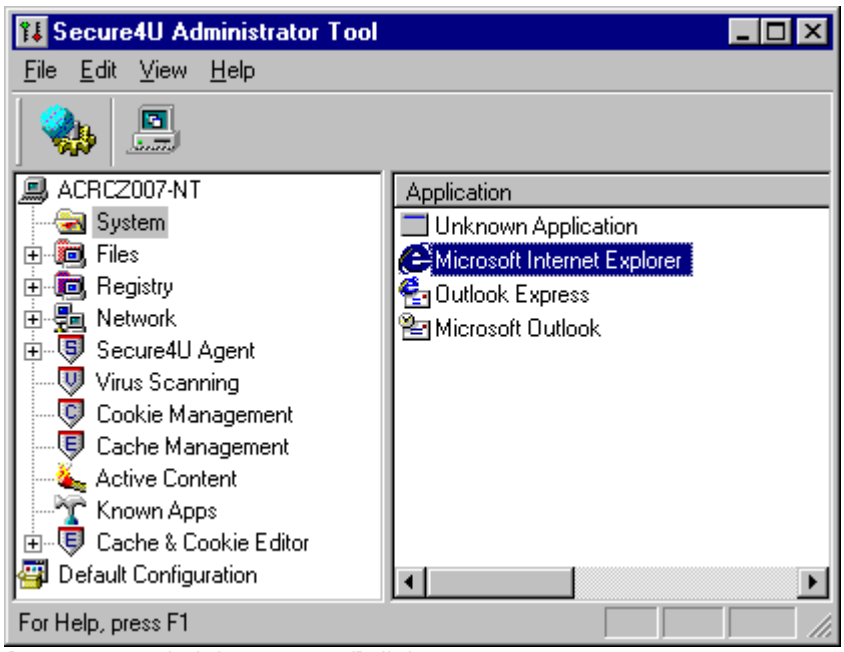
Activation of changes / settings

All changes for this *Secure4U* configuration component become active after the *Secure4U Administration Tool* is closed.

Restricted Applications

How to add a Restricted Application?

By selecting for example System the restricted applications are shown in the right hand pane.



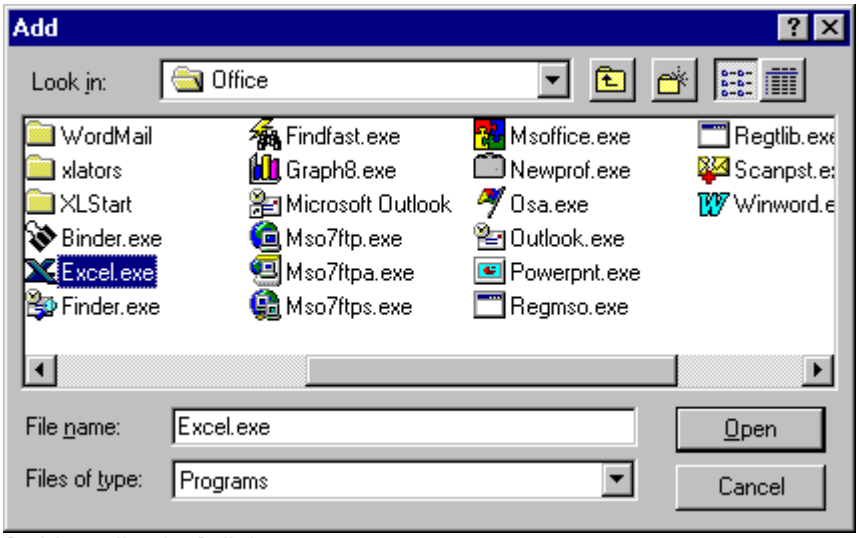
[Secure4U Administrator Tool] dialog

Right click one of the restricted applications a popup menu will display the following commands:

- **Add**
- **Remove**
- **Properties**

Add

To add a new entry to the list right-click the list and select the [Add] command in the popup menu. Within the then displayed dialog select the application path and specify other settings for this program.
When selecting the [Add] command the following window will be displayed:



[Add Application] dialog

By selecting the application you wish to restrict *Secure4U* ads it to the list of configurable applications in the right hand pane. You can then create a dedicated restriction set for this specific application.

PLEASE OBSERVE! A too restrictive sandbox around a program can lead to unwanted results or malfunctions within the restricted program.

Before you set blocking activities, you should know all the necessary accesses the program need. If you don't know all the necessary accesses you can start the application and then review its access calls in the *Secure4U Activity Window.* By using the *Secure4U Activity Window* and the *Secure4U Administration Tool* you can through trial and error find the necessary accesses the application need to function. For more information about the *Secure4U Activity Window* please consult the specific chapter in this manual.

Remove

You can remove entries in the list by right clicking an entry and selecting the command [Remove] from the Popup menu. *Secure4U* will treat a removed known application as an unknown application.

TIP! Right clicking the computer symbol will show a popup menu in which you can also select the command [Add] to add a restricted application.

Changing the access rights of a restricted application

The access rights of the default Sandbox can be changed by the Administrator to apply to the company security policy. This can be configured in accordance with any restricted application's setting as described in this manual.

Activation of changes / settings

All set restrictions to an added application become active immediately.

Default Sandbox (Unknown Applications)

Secure4U uses a default sandbox in order to protect from unknown applications. This is shown among the other restricted applications in the right hand window of the *Administrator Tool.*

Setting up a default sandbox

When installing *Secure4U* the default Sandbox is automatically created with our default settings.

Please Observe! By default the Unknown Application's configuration is very unrestricted.

Changing the access rights of the default sandbox

The access rights of the default Sandbox can be changed by the Administrator to apply to the company security policy. This can be configured in accordance with any restricted application's setting as described in this manual.

File Configuration

Within this *Secure4U* configuration component you can enumerate and set up access rights for all restricted applications and the default sandbox to the file system. On MS Win9x systems you can enforce file security compatible to the MS Windows NT file access security.

You can setup the following access restriction types:

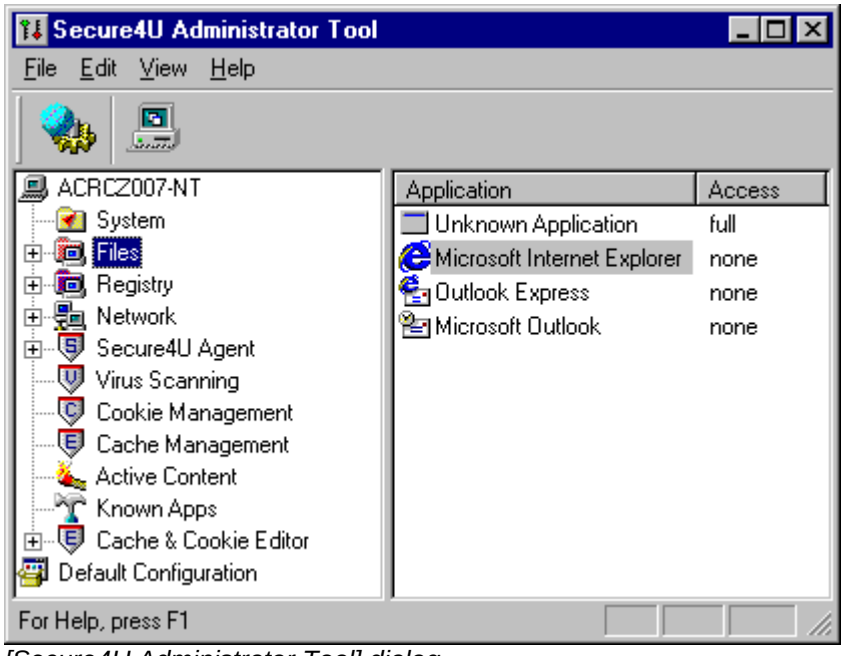
- Default access to the File subsystem or a drive for an application
- Specific access to directories for an application

Note: If you want to set restrictions for single files you must first activate the displaying of files with the [File restrictions] command in the Menu [View].

Setting Default access rights for applications

Secure4U comes with pre-configured default settings and always use the default access rights for an application when no other customized access rights exist. You can change the default access for an application. To do this please complete the following steps:

In the Local configuration branch of the configuration component tree, select the [Files] component and the following dialog will be displayed:

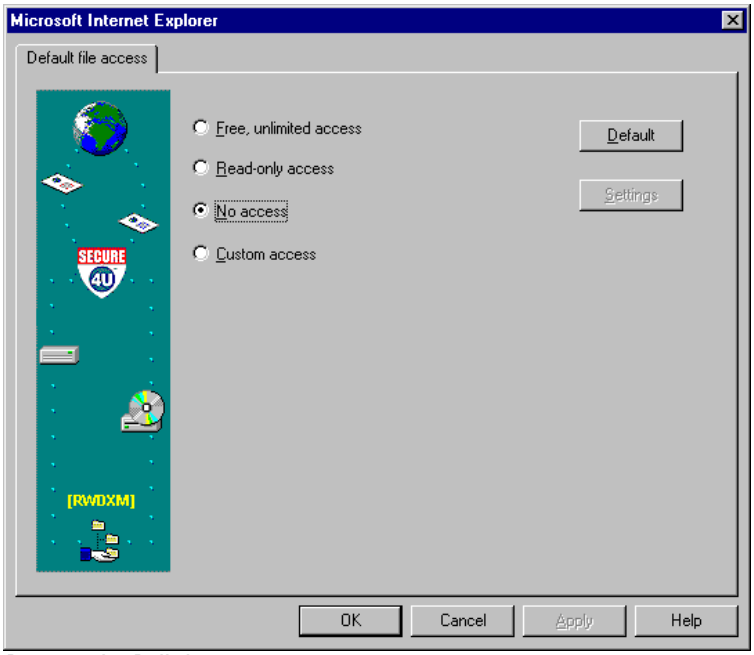


[Secure4U Administrator Tool] dialog

The *Secure4U* Administrator will display a list of restricted applications in right hand window pane.

Within this list, double-click or right-click the entry you would like to configure. If you right-click the entry please select [Properties] within the displayed popup menu.

The *Secure4U* Administrator Tool will display the following dialog box:



[Properties] dialog

You can select one of the following access types:

- **Free, unlimited access**
- **Read-only access**
- **No access**
- **Custom access**

Any of the above access restrictions will be applied by default to all file object within the file system or for the selected drive.

This means that the application you are configuring will have the selected access type to the whole file system or drive, if you do not customize specific access rights for an application to i.e. a specific directory on a drive. These settings will then be applied to all other file objects below the selected object (File system => Drive => Directory => Files).

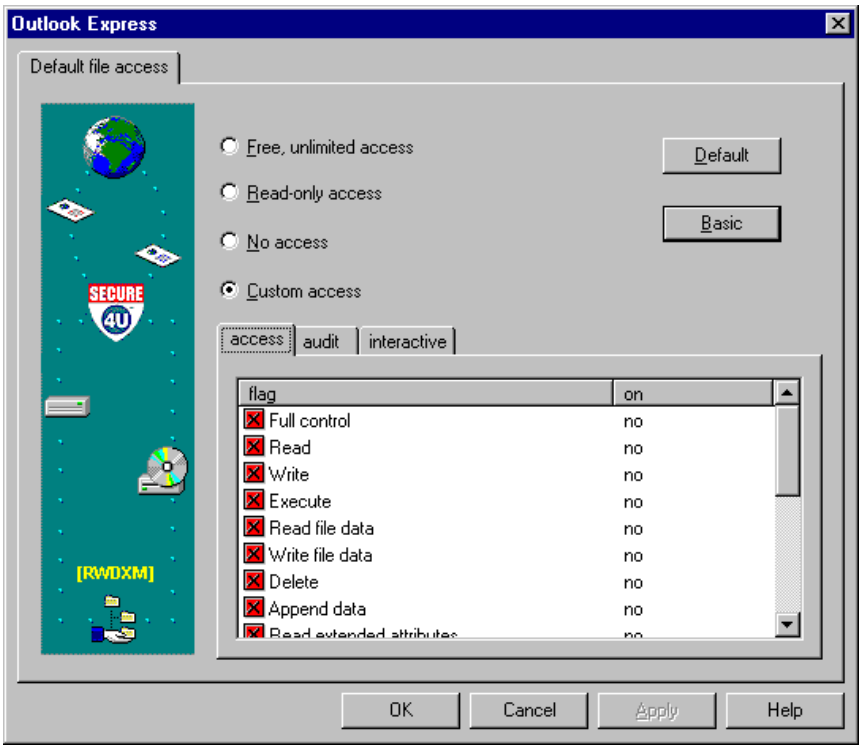
Free, unlimited access
With this access type you give free access by default to all objects within the file system or to the selected drive.

Read-only access
With this access type you give read-only access by default to all objects within the file system or to the selected drive.

No access
With this access type you block access by default to all objects within the file system or to the selected drive.

Custom access
With this access type you can fine grain access rights and *Secure4U* actions by combining different access rights and *Secure4U* activities to a custom access type.

To create a custom access type, press the [Settings] button. The following dialog will be displayed:



[Properties] dialog

Within the lower part of the dialog you will see three panes for access, audit and interactive *Secure4U* actions.

Within the list box you find all available options for each of the panes. These setting are based on the settings MS Windows NT uses for file access security. Additionally, you can set the grade of interactivity *Secure4U* will use. That means for which actions *Secure4U* will ask the user before it will commit its activities, i.e. before it will block a specific access request.

Activation of changes / settings

All changes for the default file access restrictions become active immediately after a change.

Setting Specific access rights for applications

After you have setup default access rights to the file system, you might want to exclude / set different access rights for specific directories.

Setting up specific access rights for an application works in the same way as setting up the default access rights.

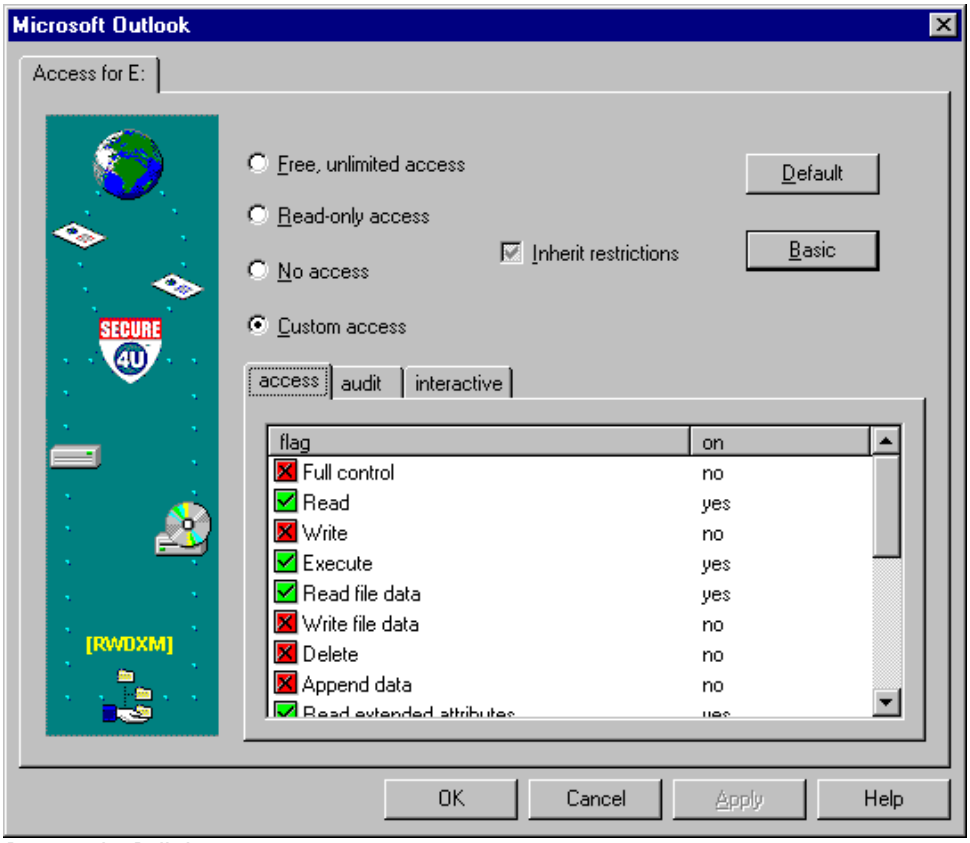
TIP! To display all files within the drives/folders right-click the [Files] component in the left-hand window tree. Activate the show file restrictions in the displayed popup menu.

To setup specific access rights complete the following steps:

- Select the directory you want to set access for in the left tree-pane of the *Secure4U Administrator Tool*.

- Select the application(s) you want to restrict in the right window pane.
- Double-click or use the [Properties] command of the popup menu.

A dialog similar to this one will be displayed:



[Properties] dialog

Select the appropriate access type or create a custom access type.

You can use the [Inherit restrictions] checkbox to apply your settings to all subdirectories. If you clear it, restrictions will only applied to the folder. Before you decide on the inherit restrictions for the first time the check box will be shaded.

After you finished your configuration click [OK] to save your changes.

Activation of changes / settings

All changes for specific file restrictions are activated immediately after a change.

Registry Configuration

Within this *Secure4U* configuration component you can enumerate and set up access rights for all restricted applications and the default sandbox to the Registry database. On MS Win9x systems you can enforce registry security compatible to the MS Windows NT Registry access security.

[Secure4U Administrator Tool] dialog

The options of the *Secure4U* Registry configuration settings are very similar to the settings for the File configuration and are accomplished in the same way.

You can setup the following access restriction types:

- Default access to the Registry database for an application
- Specific access to Sub-trees or keys for an application

Setting Default access rights for applications

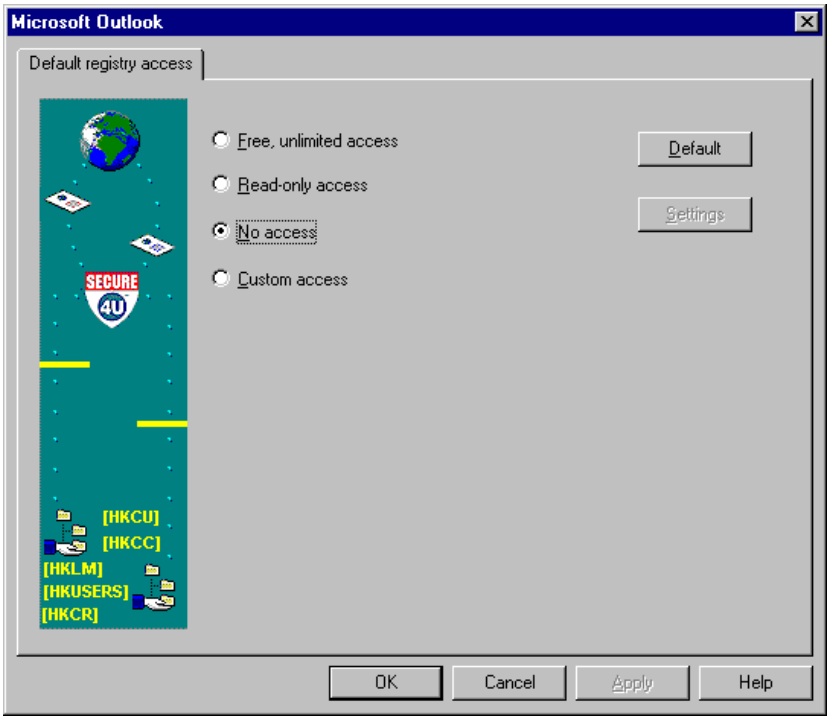
Secure4U comes with pre-configured default settings and always use the default access rights for an application when no other customized access rights exist. You can change the default access for an application. To do this please complete the following steps:

In the Local configuration branch of the configuration component tree, select the [Registry] component.

The *Secure4U Administrator Tool* will then display a list of restricted applications in right hand window pane.

Within this list double-click the entry you would like to configure. You can also right-click the entry and select [Properties] within the displayed popup menu.

The *Secure4U Administrator Tool* will display the following dialog box



[Properties] dialog

You can select one of the following access types:

- **Free unlimited access**
- **Read-only access**
- **No access**
- **Custom access**

Any of the above access restrictions will be applied by default to all registry object within the Registry database or for the selected sub-tree.

This means that the application you are configuring will have the selected access type to the whole Registry database or sub-tree, if you do not set specific access rights i.e. for branches or key(s). These settings will then be applied to all other Registry objects below the selected object (Registry database => Sub-Tree => Branch => Key) if you do not otherwise specify different settings.

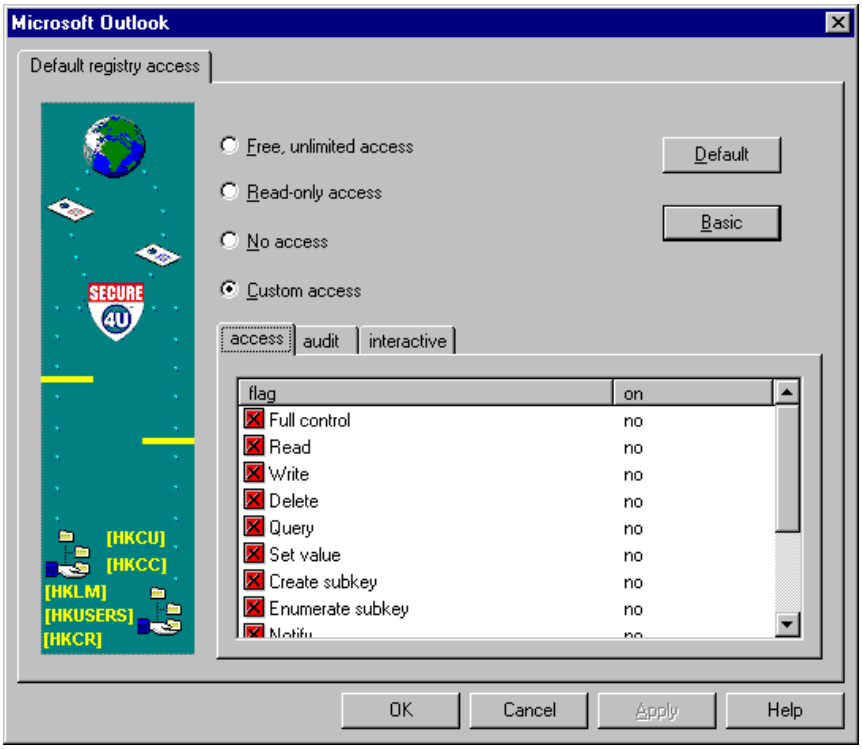
Free unlimited access
With this access type you give free access by default to all objects within the Registry database or to the selected sub-tree.

Read-only access
With this access type you give read-only access by default to all objects within the Registry database or to the selected sub-tree.

No access
With this access type you block access by default to all objects within the Registry database or to the selected sub-tree

Custom access
With this access type you can fine grain access rights and *Secure4U* actions by combining different access rights and *Secure4U* activities to a custom access type.

To create a custom access type, press the [Settings] button. The following dialog will be displayed:



[Properties] dialog

Within the lower part of the dialog you will see tree panes for access, audit and interactive *Secure4U* actions.

Within the list box you find all available options for each of the panes. These setting are based on the settings MS Windows NT uses for registry access security. Additionally you can set the grade of interactivity *Secure4U* will use. That means for which actions *Secure4U* will ask the user before it will commit its activities, i.e. before it will block a specific access request.

Activation of changes / settings

All changes for default Registry database restrictions are activated immediately after a change.

Setting Specific access rights for applications

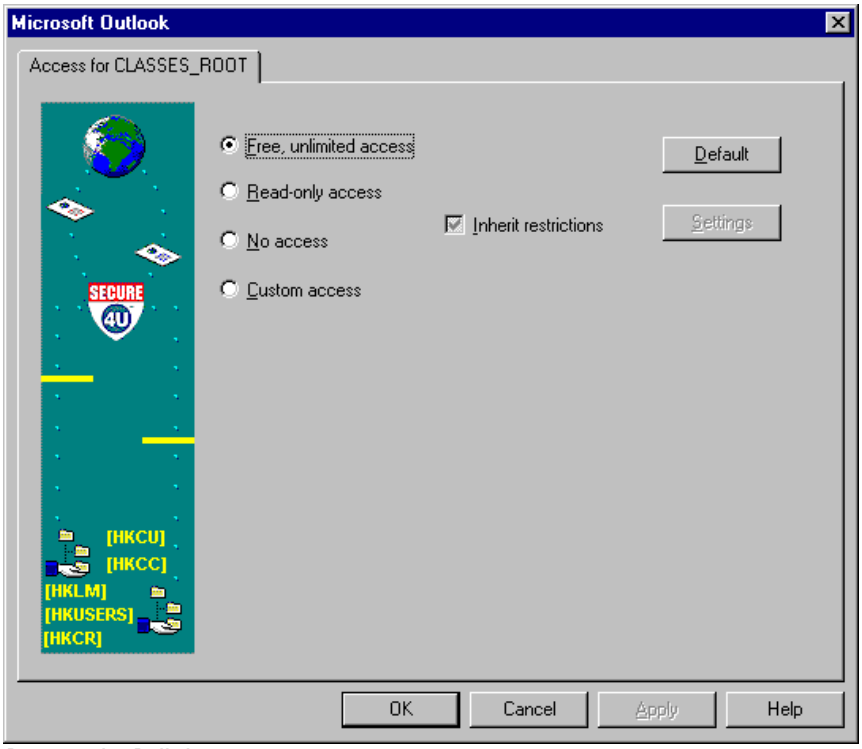
After you have setup default access rights to the Registry, you might want to exclude / set different access rights for a sub-tree/key.

Setting up specific access rights for an application works in the same way as setting up the default access rights.

To setup specific access rights complete the following steps:

- Select the Sub-tree / Key you want to set access for in the left Tree-pane of the *Secure4U Administrator Tool*.
- Select the application(s) you want to restrict right hand window pane.
- Double-click or use the [Properties] command of the popup menu

A dialog similar to this one will be displayed:



[Properties] dialog

Select the appropriate access type or create a custom access type.

After you finished your configuration click [OK] to save your changes.

Activation of changes / settings

All changes in this configuration component are activated immediately after a change.

Network Configuration

Setting up the Network configuration access components in the *Secure4U Administrator Tool* works similar to restricting access to the files system or the Registry database.

Network Neighborhood

Setting up the Network Neighborhood access components in the *Secure4U Administrator Tool* works similar to restricting access to the files system. By clicking the Network Neighborhood the computers in the Network will be shown. If one of the computers is selected its stored folders will be displayed and specific access can be set in accordance with the above explained file configuration.

[Secure4U Administrator Tool] dialog

Microsoft Windows Network

By selecting the MS Windows Network in the left tree an applications access to the Server Message Block (“SMB”) can be restricted.

PLEASE NOTE! Disabling MS Windows Network leads to no access for an application to Network Neighborhood.

Setting access rights for applications

When no specified access restrictions exists, *Secure4U* will always use the pre-set default access rights. To setup the specific access rights complete the following steps:

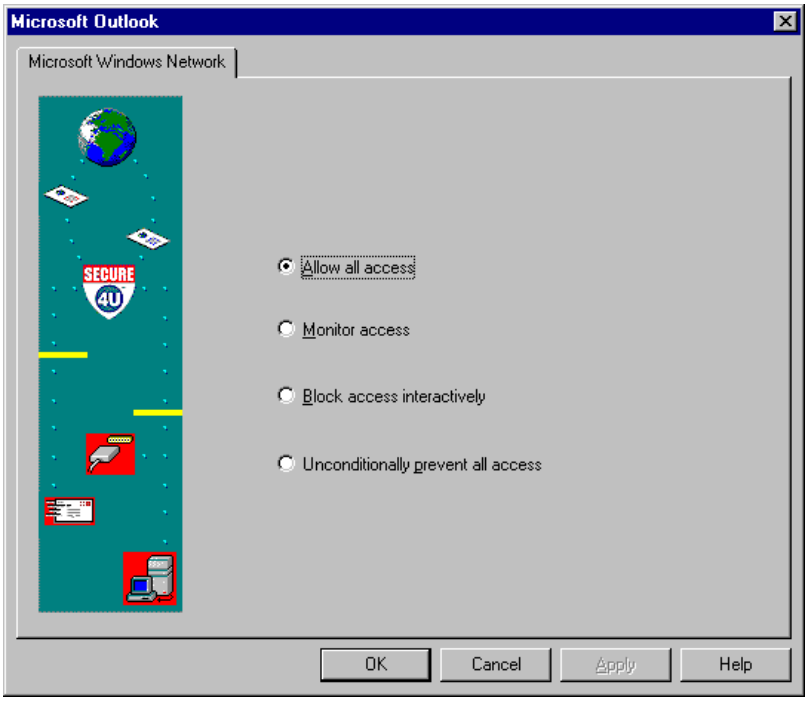
In the local configuration branch of the configuration component tree, select the MS Windows Network component.

The *Secure4U* Administrator will then display the restricted applications in the right window pane.

[Secure4U Administrator Tool] dialog

Within this list, double-click or right-click the entry you would like to configure. If you right-click the entry please select [Properties] within the displayed popup menu.

The *Secure4U Administrator Tool* will display the following dialog:



[Properties] dialog

You can set one of the following access options to the MS Windows Network for the selected application(s):

- **Allow all access**
- **Monitor access**
- **Block access interactively**
- **Unconditionally prevent all access**

Allow all access

With this option *Secure4U* will allow all accesses to the MS Windows Network for the selected application. *Secure4U* will automatically forward all requests from this application and will not display any message.

Monitor access

Secure4U will monitor all access requests to the MS Windows Network from the selected application(s) and forward them to the MS Windows Network. At the same time an entry will be displayed in the *Secure4U* Activity window and written to the Event log, if this option is selected in the *Secure4U Agent* settings.

Block access interactively

When this option is selected, *Secure4U* will display an alert box to the user, before taking any action. The user can then decide if the particular request should be blocked or granted. Any access will also monitored in the *Secure4U* activity window and can be written to the Event log if *Secure4U Agent* settings include this type of *Secure4U* action in the logs. See also the chapter *Work with Secure4U, Alert Messages for Administrator* use in this User Manual.

Note: *This option should only used for testing as it can substantially slow down overall system performance, while waiting for the user response and holding other activities of applications.*

Unconditionally prevent all access

With this option checked *Secure4U* will automatically block and monitor all access requests to the MS Windows Network of the selected application(s).

All *Secure4U* actions will be displayed in the *Secure4U* Activity window and can be logged to the event log.

Activation of changes / settings

Changes to Microsoft Windows Network restrictions are activated immediately after a change.

IP Ports

Setting up the IP Ports access components works similar to restricting access to MS Windows Network.

You can setup the following access restriction types:

- Default access to ports / Network for an application
- Access to specific ports for an application

Setting Default access rights for an applications

The *Secure4U* default accesses for restricted applications are to unconditionally prevent all access to IP Ports. The accesses to IP Ports not visible in the Secure4U Administrator Tool are therefore automatically prevented. We recommend this setting. However, if you want to change the default setting for one or more restricted applications please complete the following steps:

In the Local configuration branch of the configuration component tree, select the [IP Ports] component.

The *Secure4U Administrator Tool* will display the restricted applications in the right window pane.

[Secure4U Administrator Tool] dialog

Within this list double-click the entry you would like to configure. You can also right-click the entry and select [Properties] within the displayed popup menu.

The *Secure4U Administrator Tool* will display a dialog similar to the one shown above for the MS Windows Network.

You can set one of the following options as default access to IP Ports for the selected application(s):

- **Allow all access**
- **Monitor access**
- **Block access interactively**
- **Unconditionally prevent all access**

Allow all access

With this option *Secure4U* will allow all accesses to IP Ports for the selected application. *Secure4U* will automatically forward all requests from this application and will not display any message.

Monitor access

Secure4U will monitor all access requests to IP Ports from the selected application(s) and forward them to the ports. At the same time an entry will be displayed in the *Secure4U* Activity window and written to the Event log, if this option is selected in the *Secure4U Agent* settings.

Block access interactively

When this option is selected, *Secure4U* will display an alert box to the user, before taking any action. The user can then decide if the particular request should be blocked or granted. Any access will also monitored in the *Secure4U* activity window and can be written to the Event log if *Secure4U Agent* settings include this type of *Secure4U* action in the logs. See also the chapter *Work with Secure4U, Alert Messages for Administrator* use in this User Manual.

Note: *This option should only used for testing as it can substantially slow down overall system performance, while waiting for the user response and holding other activities of applications.*

Unconditionally prevent all access

With this option checked *Secure4U* will automatically block and monitor all access requests to ports of the selected application(s).

Any *Secure4U* action will be displayed in the *Secure4U* Activity window and can be logged to the event log.

Activation of changes / settings

Changes to IP Port restrictions are activated immediately after a change.

Setting Specific access rights for applications

You can also set different access rights for specific ports.

Setting up specific access rights for an application to an IP port works in the same way as setting up the default access rights.

To setup specific access rights complete the following steps:

- Select the IP Port you want to set the access to in the left Tree-pane of the *Secure4U Administrator Tool.* By clicking the [IP Ports} component all configurable IP Ports will be displayed. To add additional IP Ports see below.
- Select the application(s) you want to restrict in the right window pane.
- Double-click or use the [Properties] command of the Popup menu.

A similar dialog to the one described above will then be displayed:

Select the appropriate access type.

After you finished your configuration click [OK] to save your changes.

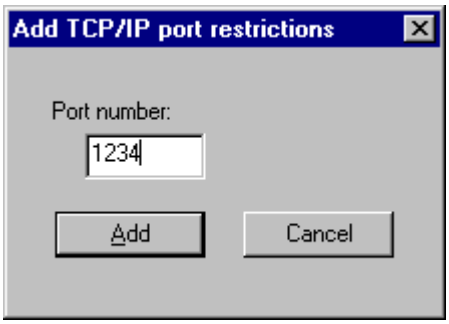
Activation of changes / settings

All changes for specific port restrictions are activated immediately after a change.

Creating a new port entry in the Port / Network component

You can create specific access restrictions to a port, which is not included in the current port component tree. To add an entry for this port number right-click the [IP Ports] component root entry in the tree pane.

Within the displayed Popup menu select [Add port]. A dialog where you can specify the port number for the new port will be displayed.



[Add TCP/IP restrictions] dialog

Press [Enter] to confirm your settings and add the new port to the tree.

You can now setup specific access right to this IP port for each of the restricted applications in the application list.

Activation of changes / settings

All changes for specific IP Port restrictions are activated immediately after a change.

The specific action of an application can be seen in the *Secure4U Activity Window.*

IP Addresses

In order to restrict a users access right to certain IP Addresses , you can set up IP Address ranges in *Secure4U.*

To setup the restricted access complete the following steps:

In the Local configuration branch of the configuration component tree, select the [IP Addresses] component.

The *Secure4U Administrator Tool* will display a list of restricted applications in right window pane.

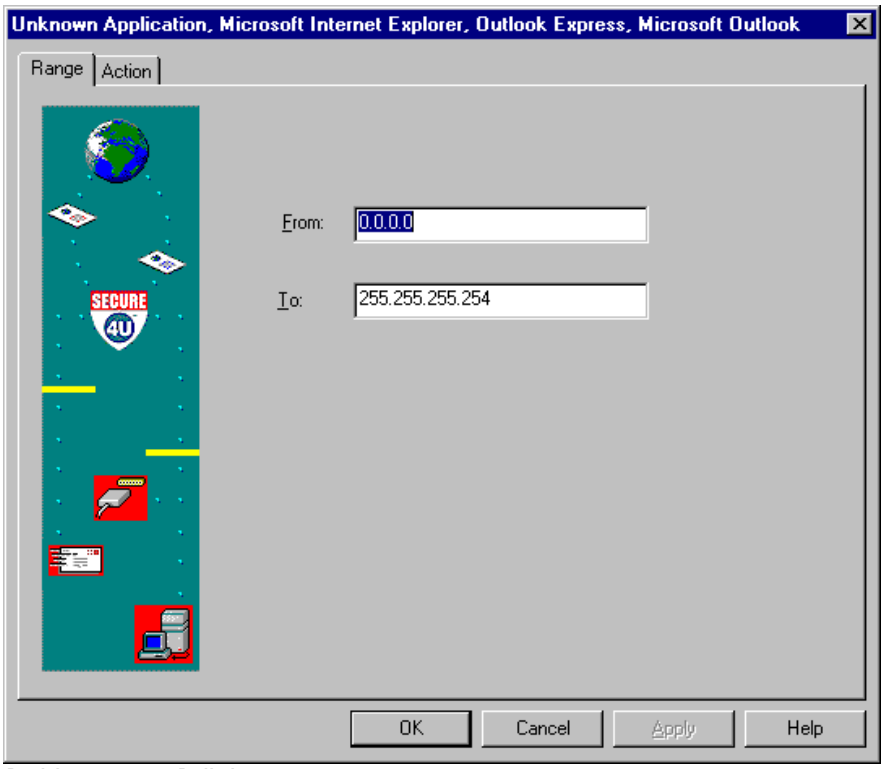
[Secure4U Administrator Tool] dialog

By right clicking the [IP Addresses] component a popup menu will give you two alternatives:

- **Add address range**
- **Remove all ranges**

Add address range

If Add address range is selected the following dialog will be displayed:



[Add IP Range] dialog

You can now insert the appropriate IP range. To set up the access rights for the specific range please click [Action] on the dialog to display a dialog similar to the one described above for the MS Windows Network and the IP Ports.

In the [Action] dialog you can set one of the following access right options to the specified IP Address range for the selected application(s):

- **Allow all access**
- **Monitor access**
- **Block access interactively**
- **Unconditionally prevent all access**

These commands work similar to the above described in the IP Ports chapter.

Remove all ranges

Currently you can only remove all IP Ranges at once.

Activation of changes / settings

All changes for this *Secure4U* configuration component become active immediately.

Agent configuration

Within this *Secure4U* configuration component you can enumerate and set up all program configurations for the *Secure4U Agent*.

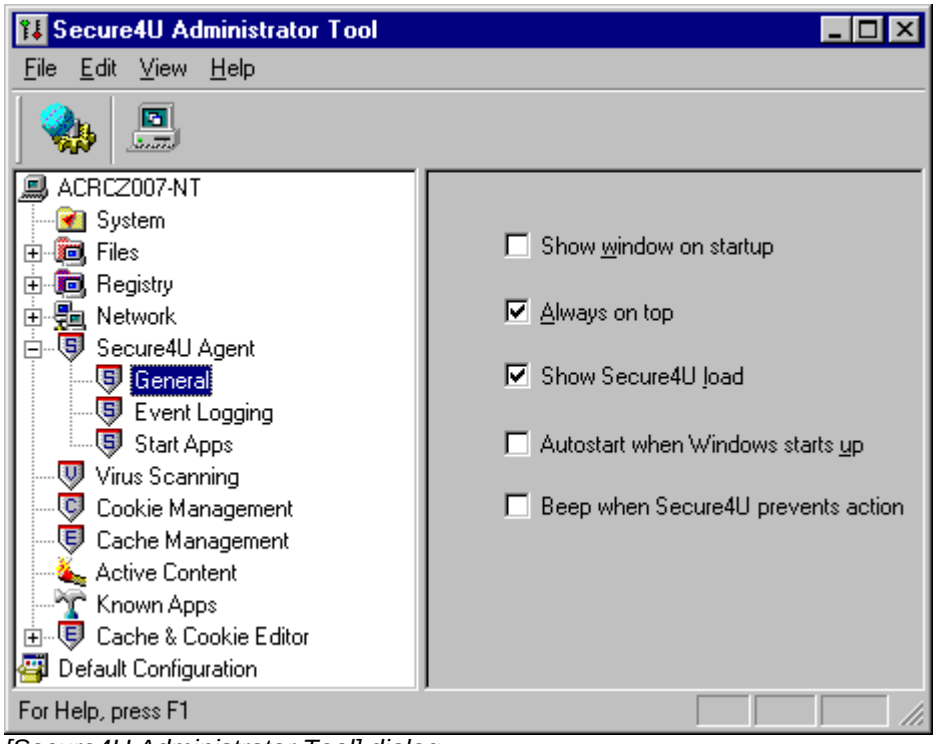
To change or enumerate the *Secure4U Agent* settings, select the *Agent* configuration component on the left tree pane.

The *Secure4U Agent* configuration component contains 3 configuration groups:

- **General**
- **Event logging**
- **Start Apps**

General

If General is selected the following dialog will be displayed:



[Secure4U Administrator Tool] dialog

On this pane you can configure the general behavior of the *Secure4U Agent*.

Within this pane the following options are available:

Show window on startup

When this option is checked *Secure4U* will display the Activity window when starting up

Always on top

With this option *Secure4U* will display the *Secure4U* Monitor window always as the topmost window

Show *Secure4U* load
When this option is selected, *Secure4U* will display the current work within the *Secure4U* Monitor window

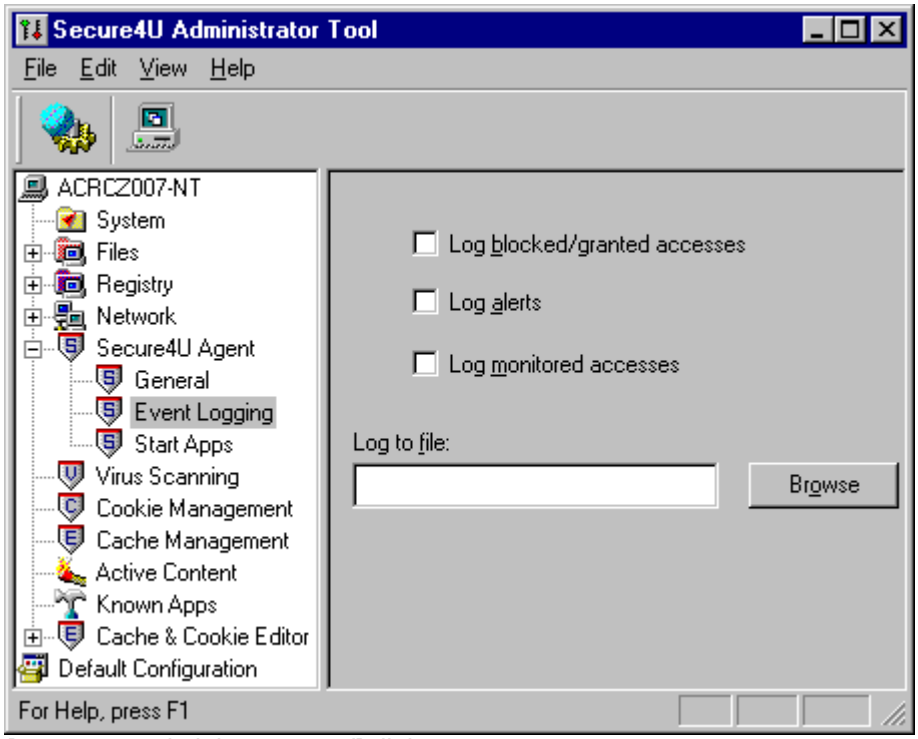
AutoStart when Windows starts up
When this option is checked *Secure4U* will automatically start the *Secure4U Agent* during the MS Windows Start up process.

Beep when Secure4U prevents action
With this option you will hear a beep any time *Secure4U* prevents or blocks an access request.

Activation of changes / settings
All changes on this pane become active when the *Secure4U Agent* is restarted.

Event logging

On this pane you can define which information *Secure4U* should log to files or the MS Windows NT Event log



[Secure4U Administrator Tool] dialog

The following options are available:
- **Log blocked/granted accesses**
- **Log alerts**
- **Log monitored accesses**

Depending on the selected option(s) *Secure4U* logs this information to the Event log for later inspection. Besides saving the selected information to the Event log, you can also specify the file within the [Log to file:] field *Secure4U* should use for

additional logging. The possibility of logging to an additional file is especially useful for MS Windows 9x where no Event log exists.

Be aware that some of the options produce large amounts of data when checked.

Activation of changes / settings

All changes on this pane become active when the *Secure4U Agent* is restarted.

Start Apps

This configuration component allows you to specify what *Secure4U* should do, when one of the applications in the application list (left pane) is started.

[Secure4U Administrator Tool] dialog

When set to [yes], *Secure4U* will automatically start the *Secure4U Agent*.

The application you want to change can be done so by double-clicking it or right-click and select [Toggle] from the displayed dialog.

Activation of changes / settings

All changes become active after reboot of the system.

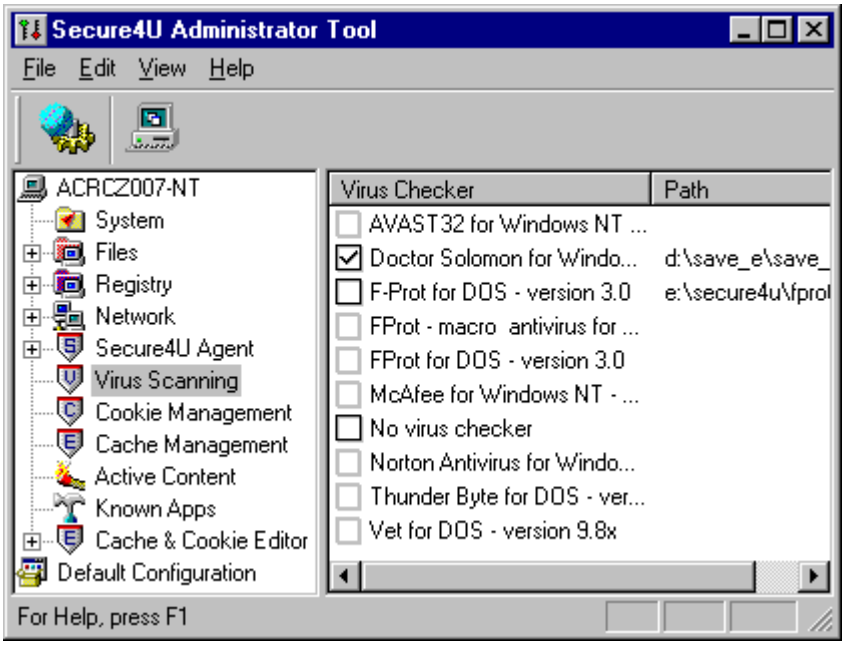
Virus Scanning

Search for installed virus scanners

During installation, the *Secure4U* Administrator runs a full search of the file system to find all copies of virus scanners that can be used by *Secure4U*. If you have subsequently installed a virus-scanner and this is not displayed in the listbox you can rescan the system. Do this by right clicking the Virus scanning configuration component in the configuration tree. A message box Scan for anti-virus programs will be visible. Please click the box and *Secure4U* will rescan the file system.

Selecting a virus scanner

When selecting the virus scanning configuration component in the configuration tree, *Secure4U* will display the following list:



[Secure4U Administrator Tool] dialog

Within the list *Secure4U* displays all found virus-scanners it can use. *Secure4U* comes with a copy of the popular F-Prot virus scanner, which is copied to your hard disk during installation of *Secure4U*.

***Note**: If you select this virus scanner, please visit the F-Prot / Datafellows web site (http://www.datafellows.com) and check for the latest virus data files.*

All virus scanners *Secure4U* is pre-configured for, but have not found on your hard drive(s), are grayed within the list of available virus scanners.

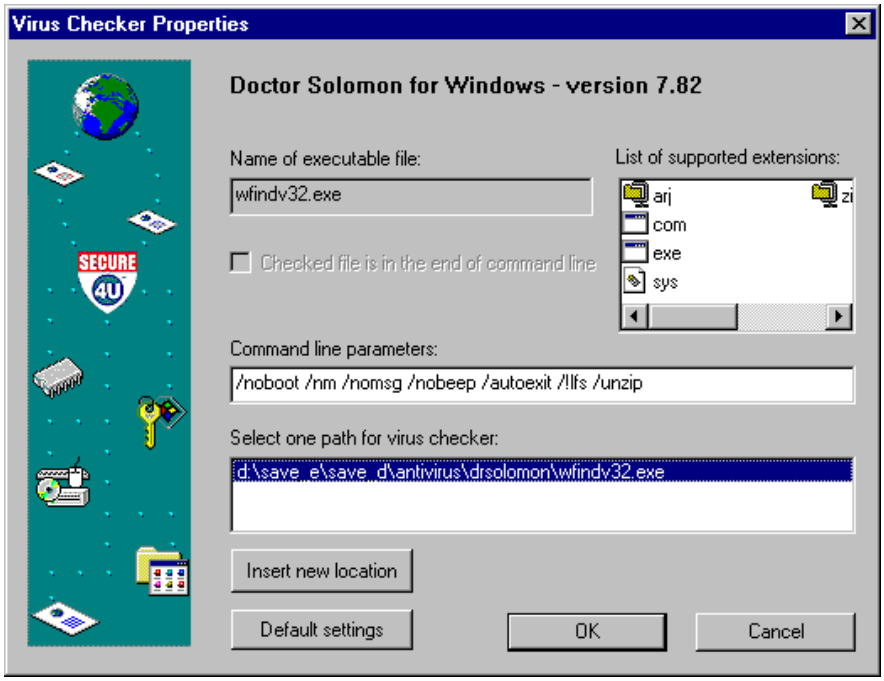
By default, virus scanning is set to [No virus checker]. You should always select a virus scanner within this list, as *Secure4U* will otherwise not scan incoming executables, cab files or other archives for viruses.

When you right-click one of the items in the list of virus scanners, *Secure4U* will display the following Popup menu:

Add new Virus Checker
Delete selected configuration
Properties
Test running

Configuring a virus scanner

When you select the [Properties] command from the Popup menu, *Secure4U* displays dialog similar to the following one (depending on the selected virus scanner):



[Virus Scanner Properties] dialog

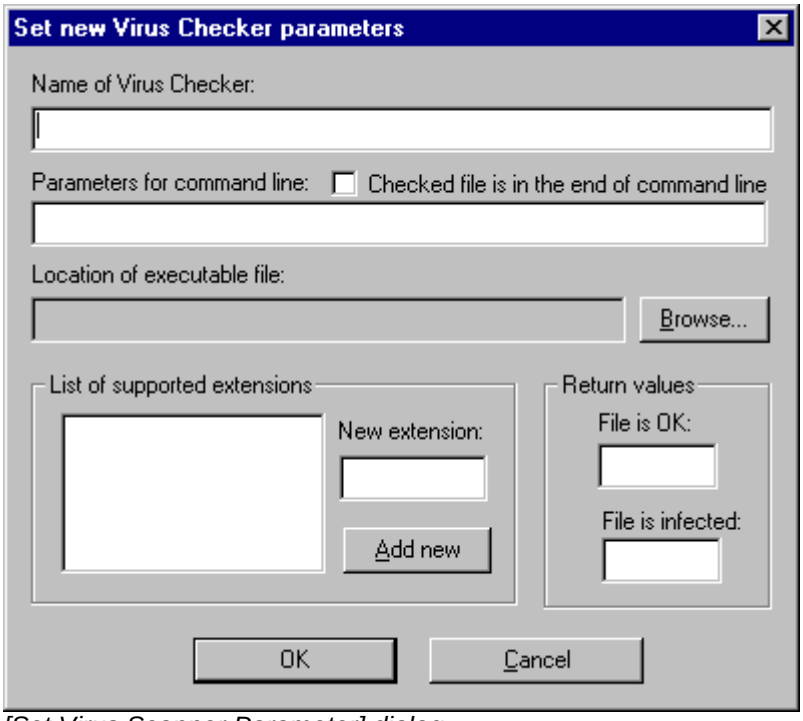
Within this dialog you can review the parameters *Secure4U* uses to call the selected virus scanner.

Creating a custom virus scanner

If you want *Secure4U* to call your virus scanner with different parameters or want to add a new virus scanner, select [Add new Virus Checker] in the Popup menu.

Note: For custom configuration in Secure4U you can only use virus scanners, which can be called with command line parameter. The virus scanner must also provide a return value to tell Secure4U the status of the checked file(s).

In the following displayed dialog you can add the parameters used by your virus scanner. To find out the parameters used by your virus scanner please contact the developer or reseller of your virus scanner.



[Set Virus Scanner Parameter] dialog

Activation of changes / settings

All changes for this *Secure4U* configuration component become active when the *Secure4U Agent* is restarted.

Cookie Management

How does the Cookie-Manager work?

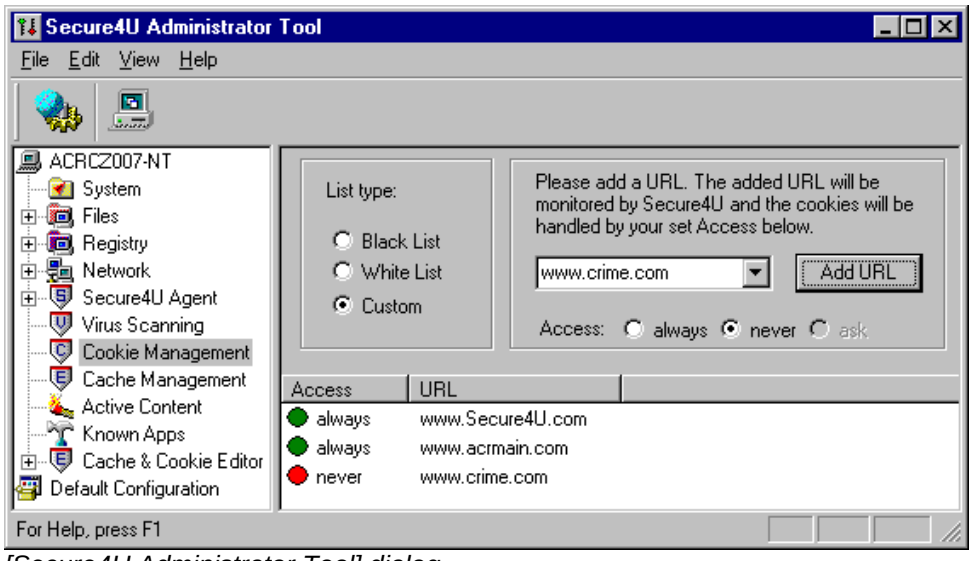
When a cookie tries to install on your computer, the *Secure4U* Cookie-Manager checks its configured cookie list if the URL/site the cookie was received from is registered or not. Depending on the set policy the Cookie-Manager undertakes the action set for this site. The following actions can be set up for the Cookie-Manager for each entry in the list:

- **Never save**
  If a cookie from this URL/site is received it will automatically be blocked. No cookies from this URL/site are allowed
- **Always ask**
  If a cookie from this URL/site is received the Cookie-Manager will display a dialog to set actions for this cookie and URL/site.
- **Always save**
  If a cookie from this URL/site is received it will be automatically saved on your computer. You will see an entry in the *Secure4U Activity Window* that the saving of the cookie was granted.

Setting up the Cookie-Manager

The following outlines the procedure to setup the *Secure4U* Cookie Manager:

1. **Select the type of list you want to use (Black list, White list, Custom list)**
2. **Add Site/URLs to the list**
3. **Remove existing cookies from your computer**



[Secure4U Administrator Tool] dialog

1. Select the type of list you want to use (Black list, White list, Custom list)

Secure4U allows you to set up the Cookie-Manager in a way that best fits your needs. Each type of list fulfills different run time requirements and approaches to stop unwanted cookies. You might choose or change to a different list type after adding Sites/URLs to a list. All your entries will remain within the list of the new type while related actions might change to the corresponding type within the new list.

Black list: If this list type is chosen, all cookies from the Sites/URLs included in the list, will automatically be blocked from being installed on the computer. The cookies from all other Sites/URLs will be allowed to install on the computer. For each entry in the list you can set the *Secure4U* action to:

- Never save (Always block)
- Always ask

White list: If this list type is chosen, only the cookies from the Sites/URLs included in the list will be saved. All other will automatically be blocked. For each entry in the list you can set the *Secure4U* action to:

- Always save
- Always ask

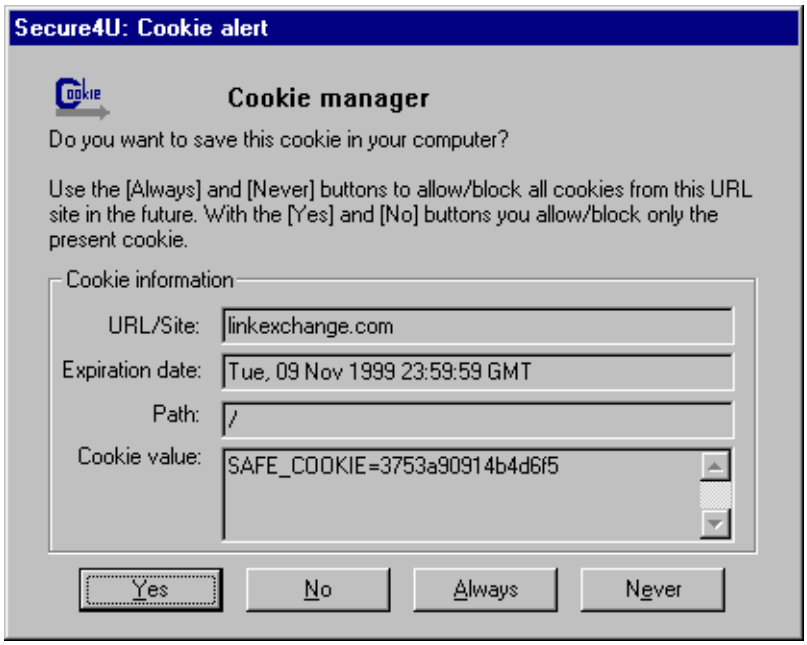
Custom list: With this type of the cookie list, *Secure4U* will ask you when a cookie arrives from all Sites/URLs which are not included in the list. You can then decide if you want to block/allow this or all cookies from the current URL. For each entry in the list you can set the *Secure4U* action to:

- Always save
- Never save (Always block)

We recommend using the Custom list, at least for some time as many sites on the Internet use different URLs for the cookie placement (i.e. excite.com / preferences.com). Also the URL resolving mechanism within this version of the *Secure4U* cookie manager needs the precise address to be able to properly block all cookies from a site.

TIP! The Custom list can also be used as a self-learning mode for the other two list types.

Within **self-learning mode** *Secure4U* presents the following alert window when a new site want to place a cookie on the computer.

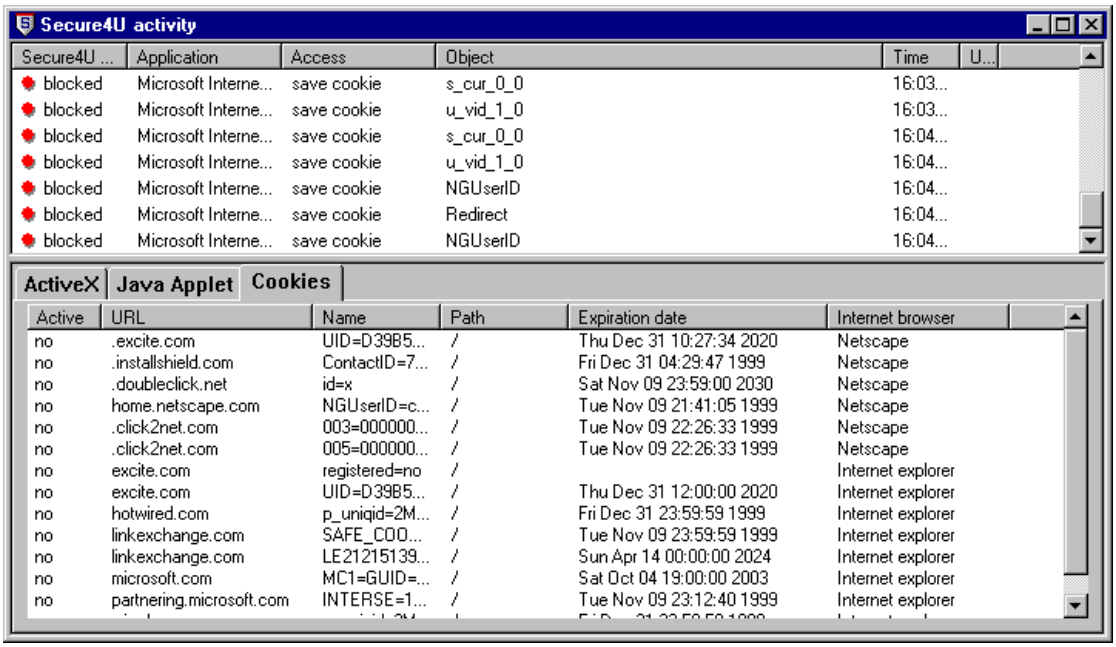


[Cookie Manager] Alert window

If you use the [Always] or [Never] buttons the settings will be added to the Cookie manager list.

If you use the [Yes] or [No] buttons the settings are only used for the current session. We recommend using the [Yes] or [No] buttons, when sites save passwords or user-ID's within the cookie.

When *Secure4U* blocks a cookie placement or the creation of a cookie is granted automatically / by the user it will inform you in the *Secure4U* Activity window about each of these actions.



[Secure4U Activity Window] dialog

In the lower part of the activity window all currently existing cookies on your computer are displayed.

By right clicking any of the entries in this list you can remove this cookie or display additional information about it.

2. Add sites/URLs to the Cookie list

- Enter a site in the URL field
- Set required access / action
- Click on the [Add URL] button in the Cookie-Manager dialog

3. Remove existing cookies from your computer

To remove an existing cookie from your computer select and right-click the related entry in the *Activity Window* and click on the [Remove] button. The cookie will then be physically deleted (No undo possible). You can also remove cookies in the *Cache & Cookie Editor*. Please see the *Cache & Cookie Editor* chapter in this User Manual.

Activation of changes / settings

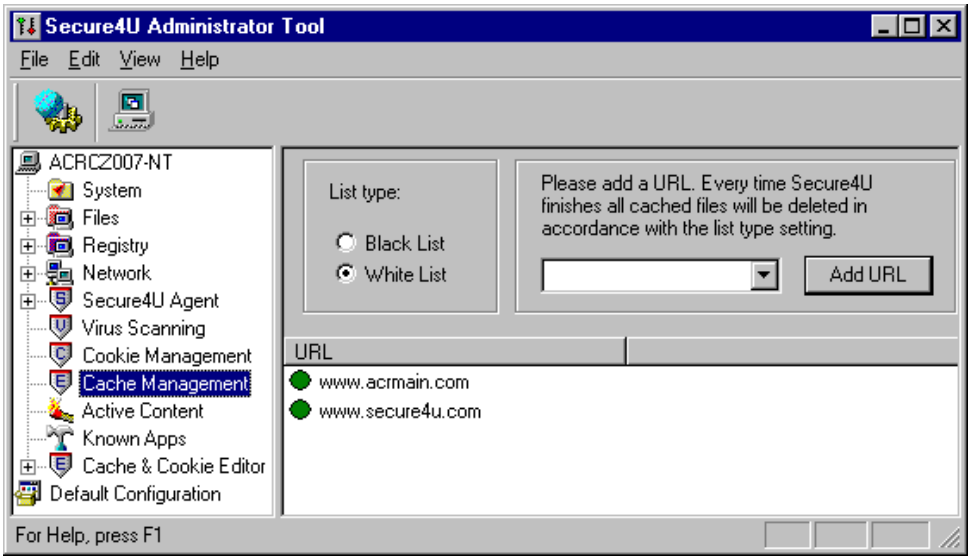
All changes for this *Secure4U* configuration component become active when the *Secure4U Agent* is restarted.

For more on Cookie Management please see the section *Cache & Cookie Editor.*

Cache Management

How does the Cache-Manager work?

When accessing the Internet, the pages shown by your browser with all their components, e.g. HTML or GIF files, will be downloaded on your computer, to the so called cache. Every file arriving on your computer is normally stored in a specific cache file. If not deleted from time to time the stored cache may take up a lot of memory space on the computer. In addition it is possible to track Internet sessions through the stored cache files and hence it might be a threat to your privacy. The *Secure4U Cache-Manager* allows the automatic removal of session information in the browser cache, registry and file system. When *Secure4U* is turned off the Cache-Manager checks if it finds the URL/site the cache was received from in its configured cache list. If the URL/site is found or not found the action undertaken by the Cache-Manager depends on the policy set by the administrator.



[Secure4U Administrator Tool] dialog

Setting up the Cache-Manager

The following outlines the procedure to setup the *Secure4U* Cache-Manager:

1. **Select the type of list you want to use (Black list, White list))**
2. **Add Site/URL to the list**

1. Select the type of list you want to use (Black list, White list)

Secure4U allows you to set up the Cache-Manager in a way that best fits your needs. The following lists can be created actions can be set:

Black list: If this list type is chosen, all cache from the Sites/URLs included in the list will automatically be removed from your computer when Secure4U is turned-off. The cache from all other Sites/URLs will be spared.

White list: If this list type is chosen, only the cache from the Sites/URLs included in the list will be spared when Secure4U is turned-off. The cache from all other Sites/URLs will automatically be removed from your computer.

2. Add sites/URLs to the Cache list

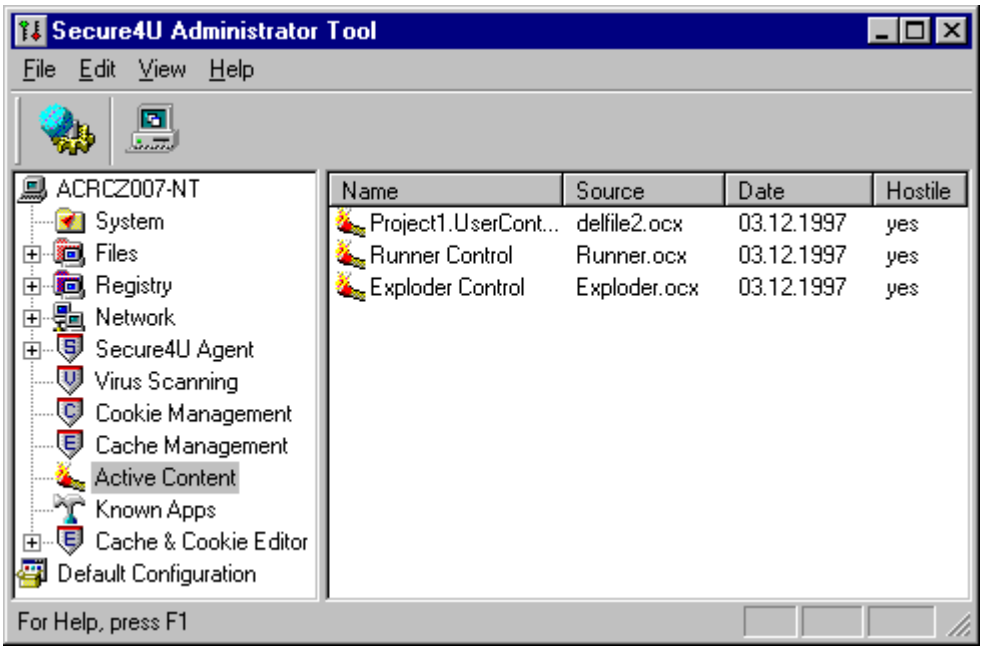
- Enter a site in the URL field
- Set required access / action
- Click on the [Add URL] button in the Cache-Manager dialog

Activation of changes / settings

All changes for this *Secure4U* configuration component become active when the *Secure4U Agent* is restarted.

Active Content

Within this configuration component you can evaluate the *Secure4U* component database and its settings.



[Secure4U Administrator Tool] dialog

Secure4U can use these settings for additional information and automatic blocking of components.

Any component flagged as hostile in the *Secure4U* component database will be automatically blocked.

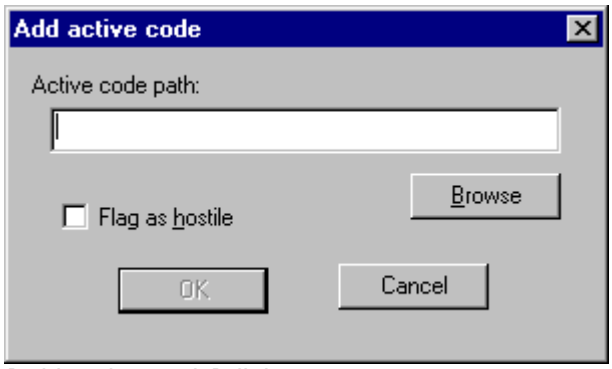
Secure4U will add all ActiveX component used on the computer to the component database.

The administrator can easily add, remove and change the settings for each entry in the database. By right clicking one of the entries in the right window pane a popup menu with the following three commands will be displayed:

- **Add**
- **Remove**
- **Toggle**

Add

To add a component to the database click on [Add] and the following dialog will be displayed:



[Add Active Code] dialog

Then browse for the component and simply click [Enter] to add the component.

Remove

To remove a component select it, right click, select [Remove] and it is removed.

Toggle

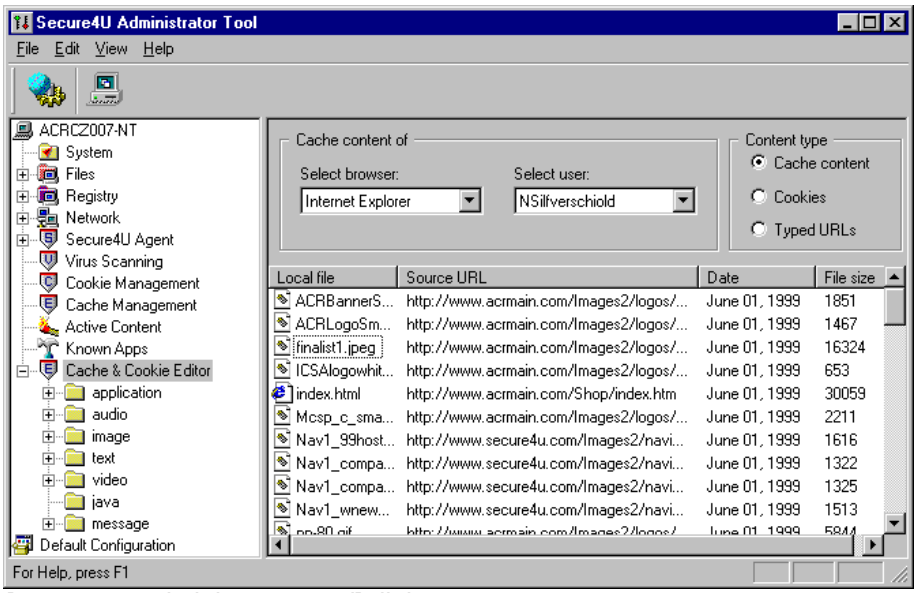
To change the state of the component from hostile to not hostile or vice versa, either double- click on the component or right-click and select [Toggle] .

Activation of changes / settings

All changes for this *Secure4U* configuration component become active when the *Secure4U Agent* is restarted.

Cache & Cookie Editor

With *Secure4U's Cache & Cookie Editor* you can manage the cache and cookies stored on the computer. When selecting the Cache & Cookie Editor the following dialog is displayed:



[Secure4U Administrator Tool] dialog

Cache Content

When the content type Cache content is selected the cache content is shown in the right window pane. You can select to view the cache content of a specific browser and also selected to view the cache content of a selected user. The browser and the user are selected from drop down lists.

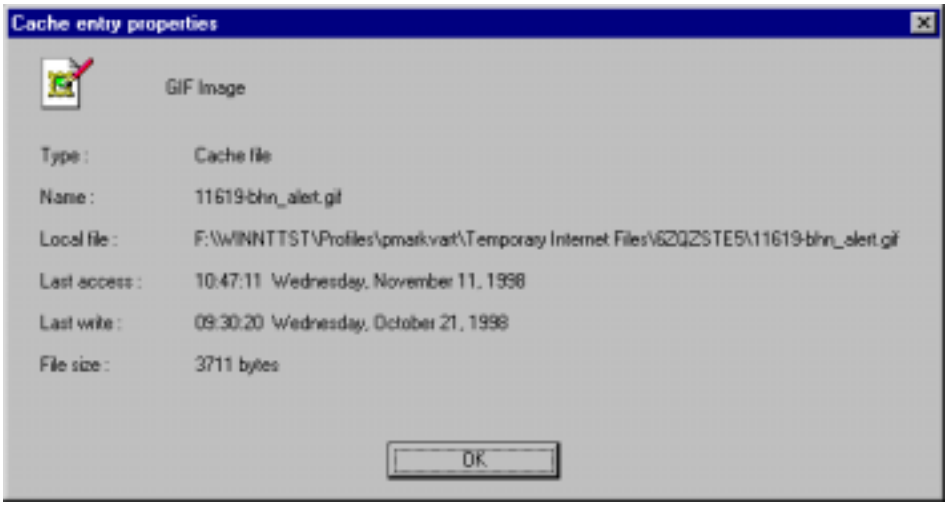
If a cached file is selected and right clicked a popup menu with three commands is shown:

- **Delete selected item(s)**
- **Delete all listed items**
- **Properties**

Delete selected item(s)
If this commands is chosen all selected item(s) will be permanently deleted.

Delete all listed items
If this commands is chosen all listed items will be permanently deleted.

Properties
If this commands is chosen a dialog showing the properties of the cached file will be shown.



[Cache Properties] dialog

Cookies

When the content type Cookies is selected all cookies are shown in the list. The cookies can be managed with the same functions as applied to the cache content.

Typed URLs

When the content type Typed URLs is selected all typed URLs are shown in the list. The typed URLs can be managed with the same functions as applied to the cache content and the cookies.

Activation of changes / settings

All changes become active after restarting the *Secure4U Agent*.

Default Configuration.

The Default Configuration contains the base configuration *Secure4U* had when it was installed on your computer.

[Secure4U Administrator Tool] dialog

The access rights for the components of the default configuration can be set similar to the above described for a single computer.

When the button [Default] is clicked in the access restriction property page the Default Configuration will apply. If the configured object, e.g., a driver, is not included in the default configuration the following restrictions will apply.

	MS Windows NT	**MS Windows 95/98**
Files	No Access	No Access
Registry	No Access	Read Only

Activation of changes / settings

All changes to specific access rights are activated immediately after a change.

Working with the Secure4U Administrator Tool

Within this chapter you will learn how to fulfil the most common tasks

The Menus

Within the local *Secure4U Administrator Tool* the following menus are currently implemented

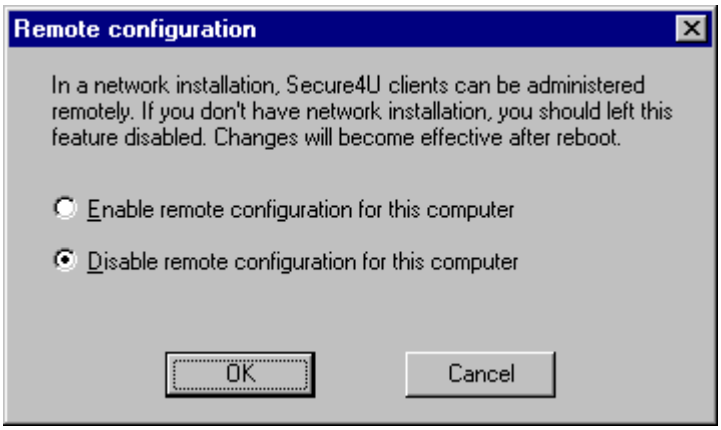
The File Menu

Within the File Menu the following commands are available:

- **Remote configuration**
- **Add remote computer**
- **Exit**

Remote configuration

Secure4U clients can be administered remotely in a network. In order to allow the client do this you need enable it. When this option is selected the following dialog will be displayed:

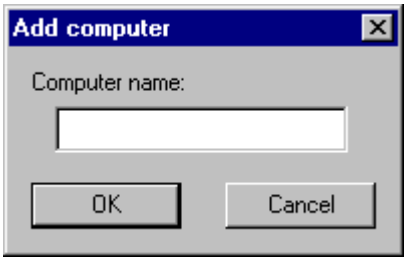


[Enable/Disable Remote Configuration] dialog

If you are not using remote configuration please disable this function since this will additionally increase security of your system.

Add Remote Computer

To add a computer to the left window pane select this option and the following dialog will be displayed:



[Add Computer] dialog

For a computer belonging to the network and having *Secure4U* installed type the name and press [Enter} or click [OK]. The computer will then be searched for and displayed in the left window pane. Thereafter it can be configured as described in this User Manual.

Exit

Use this command to end your *Secure4U* Administrator session and save all configuration changes.

The Edit Menu

Within the Edit Menu you find the following commands:

- **Set default configuration**

Set default configuration

With this command you can reset all file and registry settings back to the installation defaults. Use this command with caution. There is no undo function available after you reset your setting.

Activation of changes / settings

All changes become active when the *Secure4U Agent* is restarted

The View Menu

Within this menu you can customize the *Secure4U* Administrator interface. The following commands are available:

- **Toolbar**
- **Statusbar**

Check these commands if you want to display/not display the Toolbar or the Statusbar.

Toolbar

In the Toolbar two symbols are displayed. With the first you can enable/disable the remote configuration of a computer . With the second symbol you can add a remote computer to the configuration tree.

Statusbar

The Stausbar is displayed in the lowest part of the window and displays the status of each command in the menus.

The Help Menu

Within this menu you can search for a help topic in the online help. For additional help we recommend you to use this User Manual or contact us directly through support@acrmain.com.

Setting program preferences of Secure4U

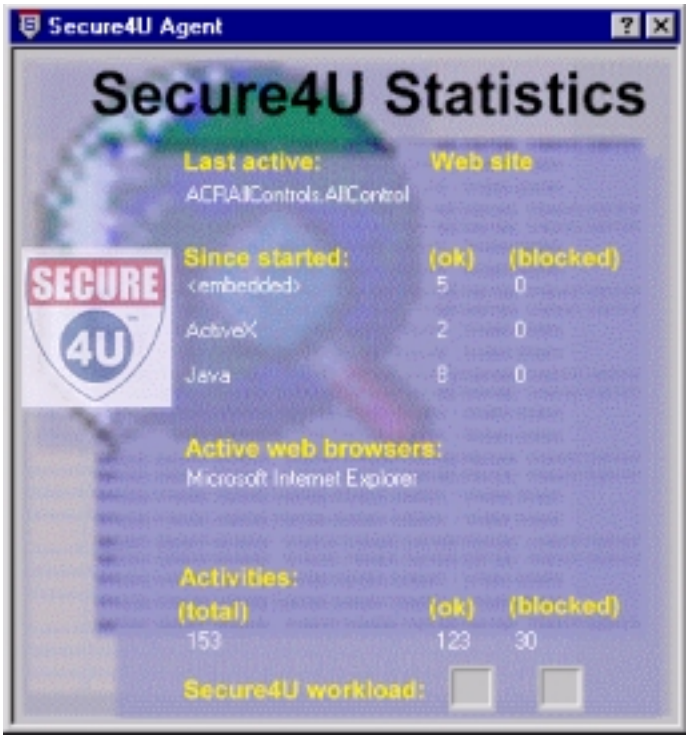
While running the *Secure4U Agent* you can change the program preferences of *Secure4U*. To change or view any of these settings right-click the *Secure4U icon* in the system tray. Within the displayed Pop-up menu you have the following options:

- **Secure4U Monitor**
- **Activity Window**
- **Properties**

Secure4U Monitor

To displaying statistic information on the current online session right-click the *Secure4U icon* in the system tray. Within the displayed Popup menu select the *[Secure4U Monitor]* command.

The following window appears:



[Secure4U monitor] window

The following information is displayed on this window:

- **Last active: / Web site:**
  These fields show you which applet was activated recently and from which web site it was received
- **Since started: / (ok) / (blocked)**
  Within these fields *Secure4U* displays statistics for the different types of active content received during the current session.

- **Active web browsers:**
  These fields list the currently running web browsers on your computer.
- **Activities:**
  These fields show you how many events have been monitored by *Secure4U* and which actions *Secure4U* has undertaken.

Secure4U workload indicators:
These two indicators display the amount of activities currently processed by *Secure4U*

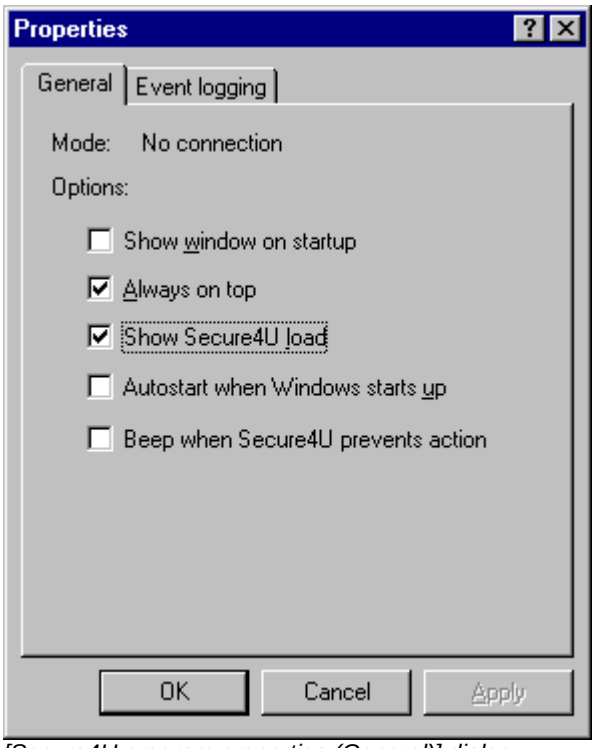
Activity Window

When you use the [Activity window] command from the above described Pop-up menu the *Secure4U Activity Window* is display.

For further information on the *Secure4U Activity Window*, please see the Chapter *Working with Secure4U: Secure4U Activity Window* within this manual.

Properties

If the [Properties] command in the above Popup menu is selected the [*Secure4U* program properties] dialog, similar to the one in the *Secure4U Administrator Tool*, is displayed.



[Secure4U program properties (General)] dialog

General properties

Within this tab page you can set or unset the following options:

- **Show window on startup**
  With this option set, *Secure4U* shows the [*Secure4U* status] dialog automatically when it starts up.

- **Always on top**
  When this option is set, [*Secure4U* status] dialog will be displayed as the topmost window.

- **Show Secure4U workload**
  When this option is set, the Indicators for the *Secure4U* workload are activated within the [Secure4U status] dialog and the system tray icon.

- **Autostart when Windows starts up**
  With this option set *Secure4U* will automatically start when *MS Windows* is started.

Event logging

For *MS Windows 9x* please consult in this manual *Secure4U Administrator Tool/Agent Configuration/Event logging.*

If the pane [Event logging] is selected in the [*Secure4U* program properties] dialog, similar to the one in the *Secure4U Administrator Tool*, the following dialog will be displayed:

[Secure4U program properties (Event logging)] dialog

For *MS Windows NT* you can select the amount of information *Secure4U* writes to the *MS Windows NT* system log within this tab page. The following options are available:

- **Log blocked/granted accesses**
  When this option is enabled, any blocking action or any access request granted will be written as one entry to the *MS Windows NT* system log.
- **Log alerts**
  With this option enabled, *Secure4U* writes an entry to the *MS Windows NT* system log for any alert message it shows.

- **Log monitored accesses**
  When enabled, *Secure4U* writes an entry to the *MS Windows NT* system log for each access request it monitored.

Note: *To use these options, event logging has to be turned on within your MS Windows NT user policy. Also consider increasing the size of the log file (System log [Application]), if using option 3 (Log monitored accesses).*

Working with Secure4U

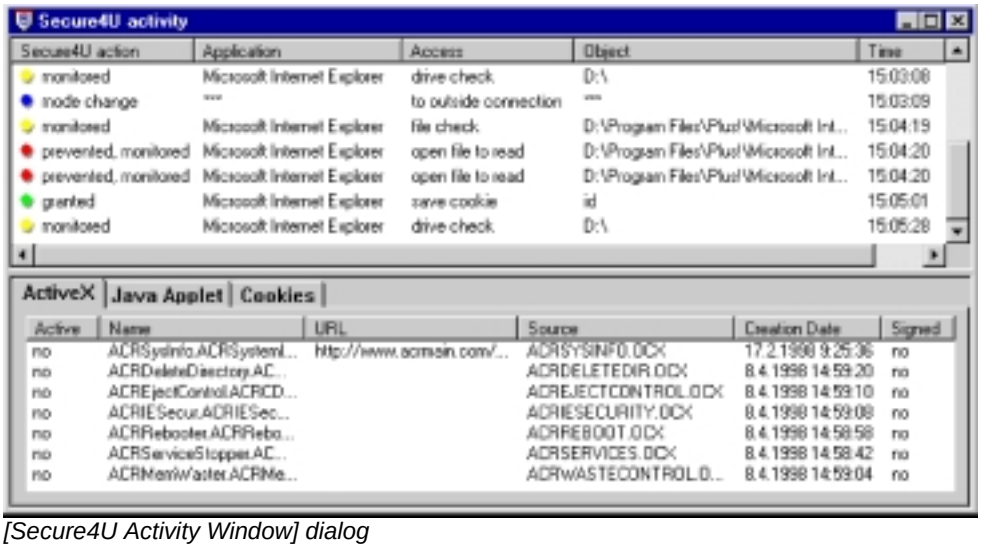
Depending on the configuration *Secure4U* will start:

- Automatically when *MS Windows NT* starts up
- Automatically when you run the monitored applications.
- Manually by the user

To manually start *Secure4U* double click on the *Secure4U icon* in the Start menu.

The Secure4U Activity Window

To see the latest action from *Secure4U* you can use the *Secure4U Activity Window*. To displaying the activity information on the current online session right-click the *Secure4U icon* in the system tray. Within the displayed Popup menu select the *[Activity Window]* command.



[Secure4U Activity Window] dialog

During the active session the *Secure4U Activity Window* displays the following information:

- **The actions undertaken by *Secure4U***
- **The applications which are requesting the accesses**
- **The type of access**
- **The object accessed (if applicable)**
- **The time of the access**

Within the lower part of the *Secure4U Activity Window* you find three panes for ActiveX, Java and cookies. You can switch from one pane to another by clicking on the header.

Within these panes the controls and applets installed by your web browsers from the Internet are displayed. The ActiveX-pane shows all ActiveX installed on your computer. The Cookie and Java-pane displays the Cookies and Java applets running on your computer during the current session. All Cookies installed on the computer can be viewed in the *Secure4U Administrator Tool.* By right clicking on

one of the items in the first column of the ActiveX-pane list a pop-up menu is displayed to manage the entry

Secure4U shows you the following information:

- The status of the applet (active / not active)
- The name of the applet
- The file name of the applet
- The date and time when it was installed on your computer
- The URL from which the applet was received*

* The URL is not always displayed correctly due to the fact that some web browsers do not support this function. In addition, if a CAB file with several components is downloaded and allowed to install only the URL for the first component will be displayed.

When you right-click an entry in the first column you can:

- Remove the applet from your computer
- Display the properties of the applet

Installing applets / controls

Any time you request pages from the Internet which contain references to active content, your web browser automatically downloads all necessary applets/ controls to your computer and installs them.

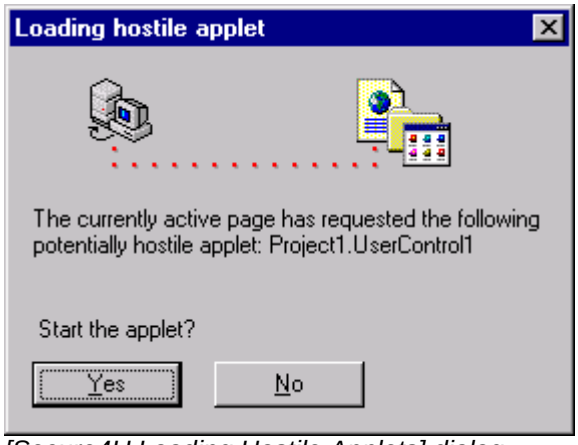
During this process and before the controls are installed / activated on your computer *Secure4U* can allow you to display the controls and to stop the installation process.

Secure4U displays the following dialog:

[Secure4U Installing Components] dialog

To continue with the installation process click on the [Yes] button. To stop the installation of the applet please select the [No] button.

If an applet arriving on your computer is flagged as hostile in the *Secure4U* Hostile applet database *Secure4U* displays the following dialog:



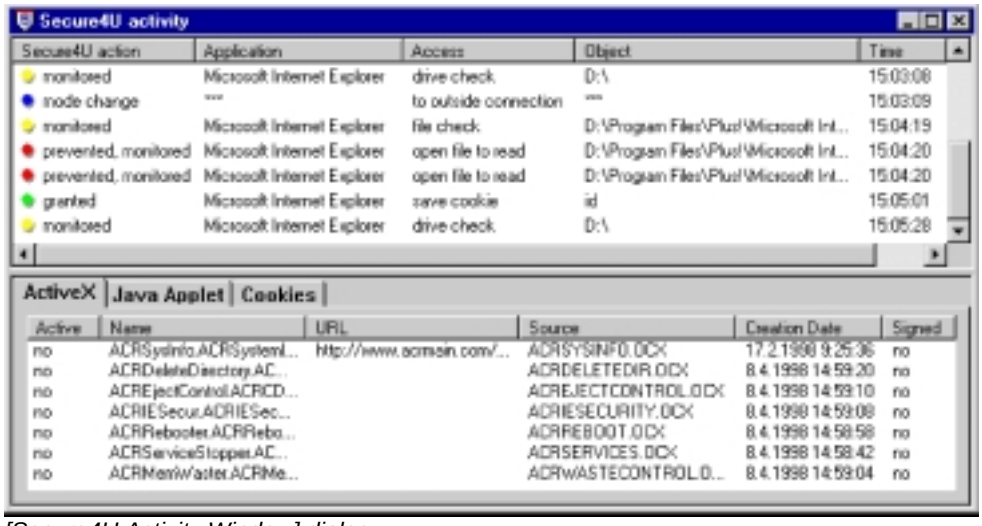
[Secure4U Loading Hostile Applets] dialog

You should normally not install applets that are flagged as hostile.

What shall I do when I receive a hostile applet warning from Secure4U?

It is not recommended to install applets that are flagged as hostile. However with *Secure4U* even these applets run until they requesting actions or accessing resources outside the sandbox.

To stop the installation, click the [No] button. *Secure4U* then stops the installation process.



[Secure4U Activity Window] dialog

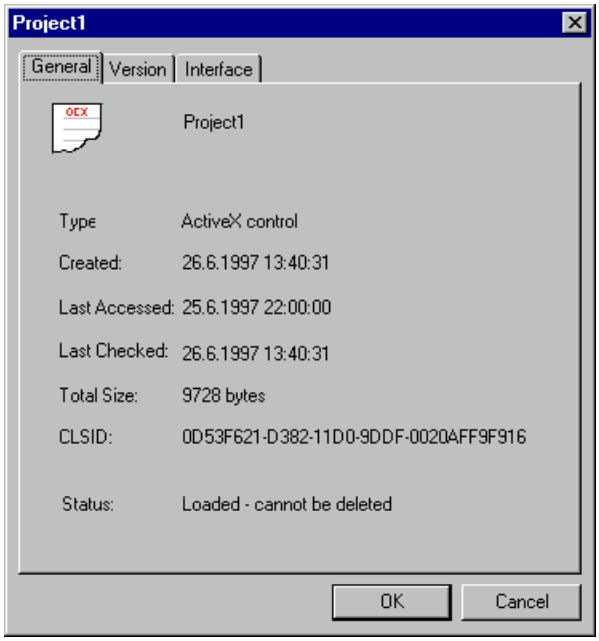
Removing an applet / control

To remove an ActiveX installed on your computer right-click its entry within the first column of the applet list on the *Secure4U Activity Window*. In the Popup menu select [Remove]. The file and its related entries in the registry database are then removed. You can also use the [Delete] button instead of the Popup menu.

The Cookies can also be removed in the *Secure4U Administrator Tool*

Displaying the properties of an applet / control

To display the properties of an applet or control installed on your computer right-click its entry within the first column of the applet list on the *Secure4U Activity Window*. In the Pop up menu select [Properties]. The following dialog appears:



[ActiveX Properties] dialog

On the three tabbed pages you find the following information:

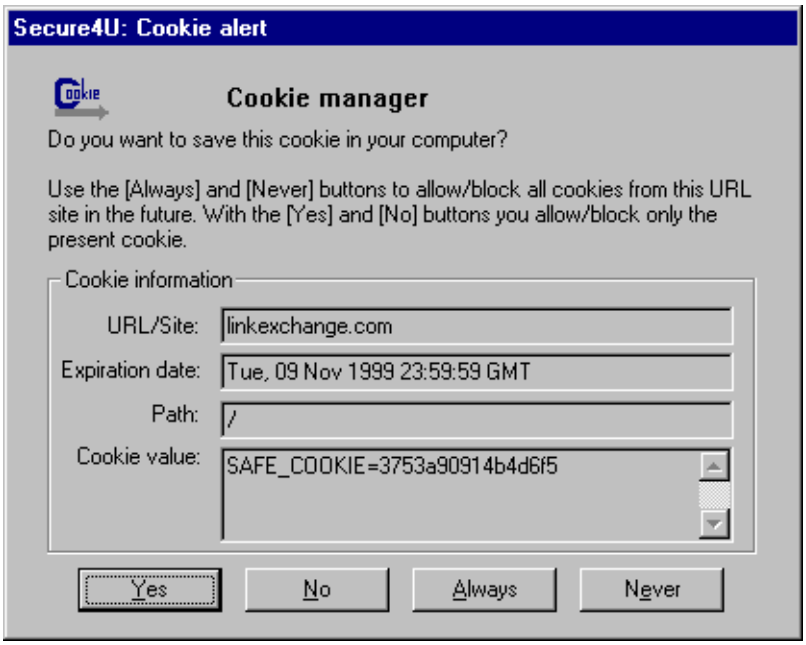
- **General**: General information like name, type, size etc.
- **Version**: Information about the version, the creator and copyright
- **Interface**: Technical information about the interface of the control i.e. properties and events

Note: *Currently only the properties of ActiveX controls can be displayed.*

Managing Cookies during Runtime of Secure4U

1. The Cookie alert dialog

This alert dialog is displayed when you have set the *Secure4U* cookie list type to Custom list and a cookie arrives from a site not included in the list.



[Cookie Manger] dialog

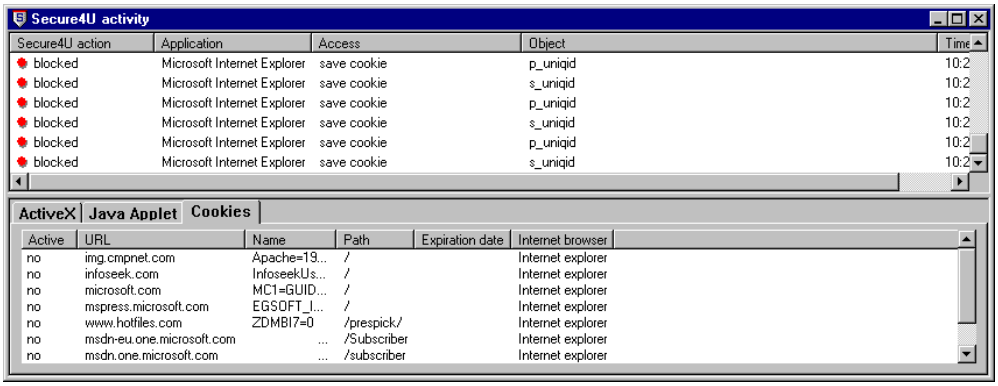
Within this dialog details of the arriving cookies are displayed and you can choose one of the following actions:

- Click [Yes], if you want this specific cookie to be placed on your computer. You will be asked for any new cookie arriving from this site
- Click [No], if you want to block this specific cookie. You will be asked for any new cookie arriving from this site.
- Click [Always], if you always want to allow cookies from this site. Any cookie from this site will then automatically be saved on your computer. The site will be added to the *Secure4U* Cookie list (see previous chapter about the *Secure4U* Cookie-Manager). You will find also an entry for these cookies within the existing cookie list (*Secure4U Activity window*).

- Click [Never], if you want to block all cookies from this site. Any cookie from this site will then automatically be blocked when arriving from the Internet. The site will be added to the *Secure4U* Cookie list (see previous chapter about the *Secure4U* Cookie-Manager).

2. Tabbed panes within the Secure4U activity window for ActiveX, Java and Cookies

Within the *Secure4U Activity Window* 3 panes for ActiveX, Java and Cookies are displayed.



[Secure4U Activity Window] dialog

You can switch from one pane to another by clicking on the header. Right-click one of the items in the first column of the list displays a pop-up menu to manage the entry. For existing cookies on your computer it allows you to remove the selected cookie or display its properties/content.

Note: *You can also remove a cookie by selecting its entry and then pressing the [Del] button.*

Alert Messages for Administrator use

If set to block access interactively *Secure4U* will show the unwanted or dangerous actions that are requested. In these cases *Secure4U* sends you a message asking you to grant or block a particular event.

When you receive an alert message from *Secure4U* the application is trying to access resources outside the closed environment (sandbox). Depending on the configuration *Secure4U* blocks these accesses automatically or sends an alert message to the user.

When *Secure4U* alerts the user it halts the request for the action / event until it has received an input from the user. Because *Secure4U* is deeply integrated into the operation system it can halt almost any type of request. We created a technology called *Smooth Stopping* with which we intercept the call to the system resources by the application and reply to the system in a way that the operating system can continue running. Otherwise if you block certain actions / events automatically, your operation system might become unstable or the restricted application will not respond any more. This is also one of the reasons why you receive standard MS Windows messages if for example your web browser tries to access protected resources and *Secure4U* is set to automatic blocking.

[High Risk Access Request] dialog

Within the *Secure4U* alert messages you receive the following information:

- The risk level of the requested action
- The application which is requesting the action
- The type of request
- The object / resource on your computer which is accessed (if applicable)

If *Secure4U* is not set up to automatically block all unwanted accesses, you can grant the current access request by clicking on the [Yes] button or block the requested access by clicking on the [No] button.

To block or grant access of a particular type to one specific object use the [Grant all] and [Block all] buttons. These accesses will then be automatically granted or blocked by *Secure4U* during the whole online session.

Note: *These buttons are not available when there is no object.*

How should I react when I receive a Secure4U Alert Message?

If you receive an alert message *Secure4U* gives you all necessary information to decide which action should be taken.

The application which is requesting the action:
Within the alert message you find the name and a description of the executable which is requesting the access.

The type of request:
Within this field you see the type of access requested. Common types are e.g. reading, writing, deleting of files or configuration settings. Depending on the resources accessed an attack can consist of a series of accesses. The severity of the request is automatically shown by the risk level *Secure4U* applies for this type of request (in combination with other indicators)

The mode your computer is in:
In the MS Windows Statusbar *Secure4U* diversifies between two modes your computer can be in:

- **No connection**: There is no remote connection open via the MS Windows socket and the restricted application.
- **Outside connection**: There is a MS Windows socket connection opened via your LAN or via remote access

The object / resource on your computer which is accessed (if applicable):
Within this field you see which resource the restricted application wants to access. This is normally the best indicator in combination with the risk level for an attack. Typical unwanted accesses would e.g. be writing to an executable file or changing of system files.

With the above information and qualification of the access request you can normally decide if you should allow the access or not. If you are still not sure check the following:

- Which risk level is displayed?
- Which applets are currently running (*Secure4U* activity window)?
- Do you know the applets, their sources or have you seen these warning in the past?
- Have there been multiple other monitored requests proceeding since this applet is running?
- Was the applet flagged as hostile when received from the Internet?
- Which resource is accessed, is it part of the system or one of your documents?
- Is the resource deleted or changed by the type of access requested?
- Is your computer in outside mode?

If you are still not sure we recommend you to block the access.

Deploying and using Secure4U within LANs

Remote Configuration

Secure4U can be centrally deployed and administered within LANs. For a simple remote configuration you can install *Secure4U* on the server and add computers to the administration tool.

A more sophisticated remote configuration can be reached by installing the *Secure4U Network Console* on the server.

For more information about the *Secure4U Network Console* please see the *Secure4U Network Console* User Manual.

PLEASE OBSERVE! Both MS Windows NT and MS Windows 95/98 can be configured offline. Configure a computer online is only possible for computer running MS Windows NT.

Deployment of Secure4U via SMS

Secure4U can be deployed via SMS version 1.2. However, please be aware that the default configuration of SMS is to install the program with user rights. *Secure4U* needs administrator rights to install and this has to be made possible to the program.

Management of Secure4U via MMC

Currently the clients can be shown and managed through the *Secure4U Network Console*. Which is implemented as a snap-in for the Microsoft Management Console ("MMC").

For more information about the *Secure4U Network Console* please see the *Secure4U Network Console* User Manual.

Management of Secure4U via other Network management systems

Management and configuration of *Secure4U* via other Network management systems will be made possible in the future.

Silent Installation of Secure4U

A silent Installation can be done when installing *Secure4U* through the InstallShield standard remote network installation programs.

Limitation of user interaction

The Administrator can limit the user interaction possibilities by removing the *Secure4U Administrator Tool* and the *Secure4U Unloader Tool* from the client computer. The *Secure4U Administrator Tool* is named tuconf.exe and the *Secure4U Unloader Tool* is called unloader2.exe. Both are to be found in the installation folder selected for *Secure4U* during the installation.

Using Secure4U together with other software

Secure4U layers itself transparently into the MS Windows operating system. To restrict applications please consult the Restricted Applications chapter in this manual.

PLEASE OBSERVE! A too restrictive sandbox around a program can lead to unwanted results or malfunctions within the restricted program.

Before you set blocking activities, you should know all the necessary accesses the program need. If you don't know all the necessary accesses you can start the application and then review its access calls in the *Secure4U Activity Window.* By using the *Secure4U Activity Window* and the *Secure4U Administration Tool* you can through trial and error find the necessary accesses the application need to function. For more information about the *Secure4U Activity Window* please consult the specific chapter in this manual.

Installing other software on a computer with Secure4U

As *Secure4U* can be configured to restrict all unknown applications, it can be difficult to install new software on a remote computer. The *Secure4U Administrator Tool* gives the administrator the possibility to temporarily disable, remotely or locally, Secure4U until the new software is installed. Please remember to turn it on afterwards.

By right-clicking the computer symbol in the left hand window pane a popup menu displays the command:

- **Enable Secure4U**,
- **Disable Secure4U**,

Please select the appropriate command. The changes will be active immediately.

Grouping of computers

In the *Secure4U Network Console* the administrator can divide the computers in a LAN into different groups (i.e., Management, Marketing, etc.). It is currently possible to disable / enable *Secure4U* on remote computers for groups. In future versions of Secure4U it will be made possible to change the configuration for computers within the group at once.

For more information about the *Secure4U Network Console* please see the *Secure4U Network Console* User Manual.

Index

Contact information

If you require further information on the *Secure4U* product family or want to know more about our products and services, please contact us via the Internet at: www.acrmain.com or www.Secure4U.com

Support information request for *Secure4U*: support@acrmain.com

Please include your license number, information about your computer (operating system, processor and memory) and a brief description of your problem. You can also fill out our support form and submit it online on http://www.acrmain.com/Support/

Updates or new versions of Secure4U:
Please check the product section on
www.acrmain.com and www.Secure4U.com

If you want to write us a letter please use the following address:

Advanced Computer Research Praha s.r.o
Bretislavova 12
110 00 Prague 1
Czech Republic