Faronics™
Simplifying Computer Management

FARONICS
ANTI-VIRUS™

ADVANCED
System Integrity

User Guide

www.faronics.com

Last modified: January 2023

Contents

Preface

This user guide explains how to install and use Faronics Anti-Virus.

Topics

Important Information

This section contains important information about your Faronics Product.

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, health care facilities, libraries, government organizations, and corporations.

Product Documentation

The following documents form the Faronics Anti-Virus documentation set:

- Faronics Anti-Virus User Guide – This document guides you how to use the product.
- Faronics Anti-Virus Release Notes – This document lists the new features, known issues, and closed issues.

Technical Support

Every effort has been made to design this software for ease of use and to be problem free. If problems are encountered, contact Technical Support.

Email: support@faronics.com

Phone: 1-800-943-6422 or 1-604-637-3333

Hours: Monday to Friday 7:00am to 5:00pm (Pacific Time)

Contact Information

- Web: www.faronics.com
- Email: sales@faronics.com
- Phone: 1-800-943-6422 or 1-604-637-3333
- Fax: 1-800-943-6488 or 1-604-637-8188
- Hours: Monday to Friday 7:00am to 5:00pm (Pacific Time)
- Address:

  Faronics Technologies USA Inc.
  5506 Sunol Blvd, Suite 202
  Pleasanton, CA, 94566
  USA

  Faronics Corporation (Canada and International)
  609 Granville Street, Suite 1400
  Vancouver, BC V7Y 1G5
  Canada

  Faronics Corporation (Europe)
  8 The Courtyard, Eastern Road,
  Bracknell, Berkshire,
  RG12 2XB, United Kingdom

Definition of Terms

Term	Definition
Active Protection	Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system.
Adware	Adware, also known as advertising software, is often contextually or behaviorally based and tracks browsing habits in order to display third-party ads that are meant to be relevant to the user. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results.
Firewall	A Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. A Firewall protects your network from unauthorized intrusion.
Quarantine	The Quarantine is a safe place on your computer that Faronics Anti-Virus uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review the details of a risk and research it further and remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove the risks from Quarantine.
Rogue security program	A rogue security program is software of unknown or questionable origin, or doubtful value. A rogue security program usually shows up on web sites or spam emails as intrusive warnings that claim that your computer is infected and offer to scan and clean it. These should never be trusted. Reputable antivirus or antispyware companies will never use this way of *notifying* you. A rogue security program may appear like an ordinary antivirus or antimalware program, but will instead attempt to dupe or badger you into purchasing the program. While some rogue security programs are the equivalent to *snake oil* salesman resulting in no good, others may actually result in harm by installing malware or even stealing the credit information that you enter and possibly resulting in identity theft. Further, you need to be cautious about closing or deleting these alerts, even when you know they're fake.

Term	Definition
Rootkits	A rootkit is software that cloaks the presence of files and data to evade detection, while allowing an attacker to take control of the machine without the user's knowledge. Rootkits are typically used by malware including viruses, spyware, trojans, and backdoors, to conceal themselves from the user and malware detection software such as anti-virus and anti-spyware applications. Rootkits are also used by some adware applications and DRM (Digital Rights Management) programs to thwart the removal of that unwanted software by users.
Spyware	Spyware is software that transmits information to a third party without notifying you. It is also referred to as trackware, hijackware, scumware, snoopware, and thiefware. Some privacy advocates even call legitimate access control, filtering, Internet monitoring, password recovery, security, and surveillance software *spyware* because those could be used without notifying you.
Trojan	A trojan is installed under false or deceptive pretenses and often without the user's full knowledge and consent. In other words, what may appear to be completely harmless to a user is in fact harmful by containing malicious code. Most trojans exhibit some form of malicious, hostile, or harmful functionality or behavior.
Virus	A computer virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as CD-ROMs or flash drives. Viruses can also spread via email through infected attachments and files. Most viruses include a *payload* that can be anywhere from annoying and disruptive to harmful and damaging; viruses can cause system damage, loss of valuable data, or can be used to install other malware.
Worm	A worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike viruses, however, worms spread without attaching to or infecting other programs and files. A worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through email by sending copies of itself to everyone in the user's address book. A worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some worms may be used to compromise infected machines and download additional malicious software.

Introduction

Faronics Anti-Virus provides protection from security threats without slowing down computers due to slow scan times and large footprints. Built with next-generation technology, Faronics Anti-Virus gives you powerful anti-virus, anti-rootkit and anti-spyware software in-one that protects you against today's highly complex malware threats while providing seamless integration with Faronics Deep Freeze and Faronics Anti-Executable to form a complete layered security solution.

Topics

Faronics Anti-Virus Overview

Faronics Anti-Virus protects workstations from the following threats:

- Adware
- Rogue Security Programs
- Rootkits
- Spyware
- Trojan
- Worms

Faronics Anti-Virus can be deployed on multiple workstations via Faronics Core. For information on Faronics Core, refer to Faronics Core User Guide. The latest user guide is available at http://www.faronics.com/library.

When installed with Deep Freeze, the Anti-Virus definitions can be updated on managed workstations without requiring to *Reboot Thawed* or rebooting in *Maintenance Mode*. For more information, refer to Deep Freeze Enterprise User Guide. The latest user guide is available at http://www.faronics.com/library.

System Requirements

Faronics Anti-Virus Requirements

The Faronics Anti-Virus Loadin requires the following:

- Faronics Core 3.7 or higher

Faronics Anti-Virus Client on the workstation requires any of the following operating systems:

- Windows XP SP3 (32-bit) or Windows XP SP2 (64-bit)
- Windows 7 (32-bit or 64 bit)
- Windows 8.1 (32-bit or 64 bit)
- Windows 10 up to version 22H2 (32-bit or 64 bit)
- Windows 11 up to version 22H2
- Windows Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2022 (64-bit)

It is highly recommended that all components be installed using a Windows Administrator account.

Faronics Core Requirements

Information on Faronics Core system requirements can be found in the Faronics Core User Guide. The latest user guide is available at http://www.faronics.com/library.

Deep Freeze Requirements

Information on Deep Freeze system requirements can be found in the Deep Freeze Enterprise User Guide. The latest user guide is available at http://www.faronics.com/library.

To run Faronics Anti-Virus on workstations managed by Deep Freeze, Deep Freeze Enterprise 7.0 or higher is required.

Faronics Anti-Virus Licensing

Faronics Anti-Virus License can be applied via Faronics Core Console. Complete the following steps to apply Faronics Anti-Virus License:

1. Launch Faronics Core Console.
2. Right-click the *Core Server* and select *Properties*.
3. Click the *Anti-Virus* tab. The *Anti-Virus* tab displays the *Version*, *License Key* (if it is a Licensed Version), and *License Expiry*.
4. Click *Edit* and enter the *License Key* in the *License Key* field.
5. Click *Apply*. Click *OK*.

Faronics Anti-Virus Licensing works as follows:

- The Core Server (a component of Faronics Core) automatically pushes the License Key to the workstations where Faronics Anti-Virus Client is installed (if the computers are offline, the License Key is applied once the computers are back online).

If the Faronics Anti-Virus License Key was entered while installing the Loadin, it is not necessary to enter it again in the *Properties* tab.

Virus definitions cannot be downloaded if Faronics Anti-Virus License Key has expired.

Installing Faronics Anti-Virus

This chapter describes how to install Faronics Anti-Virus.

Topics

Installation Overview

Faronics Anti-Virus consists of two components:

- Faronics Anti-Virus Loadin – to be installed on a computer that has Faronics Core.
- Faronics Anti-Virus Client – to be deployed on workstation(s) that will be managed by the Faronics Anti-Virus Loadin.

Installation and configuration of Faronics Anti-Virus involves the following stages:

- Installing Faronics Core and generating/deploying the Core Agent
- Installing the Faronics Anti-Virus Loadin
- Deploying Faronics Anti-Virus Client

Installing Faronics Core

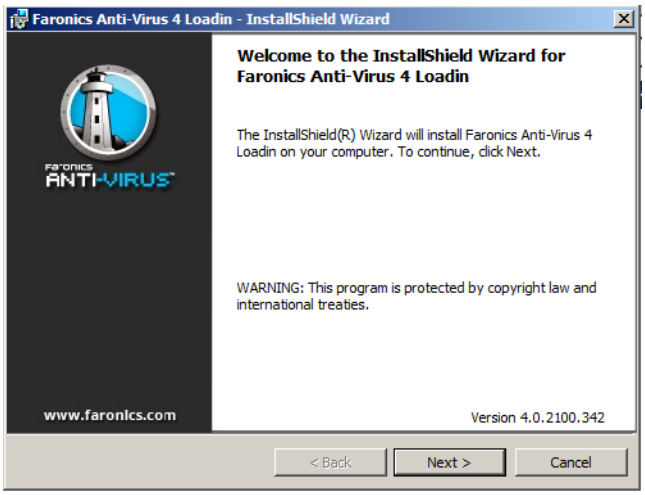
For information on installing Faronics Core and generating and deploying the Core Agent, refer to the Faronics Core user guide. The latest user guide is available at http://www.faronics.com/library.

Installing Faronics Anti-Virus Loadin

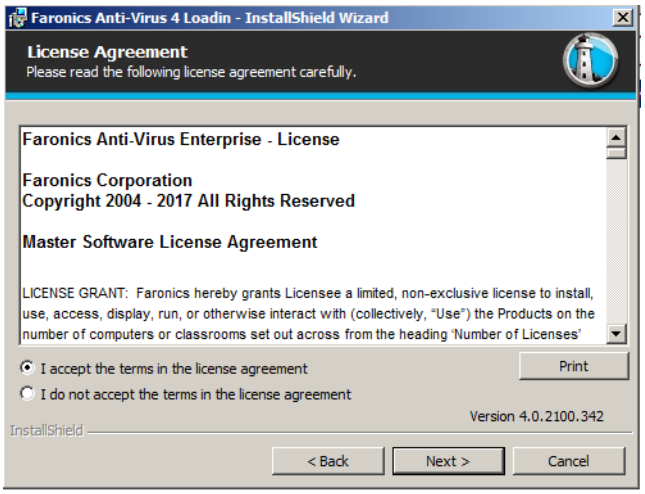
Complete the following steps to install Faronics Anti-Virus Loadin:

The Anti-Virus Loadin cannot be installed on a computer that does not have Faronics Core Console (or Faronics Core Server) installed.

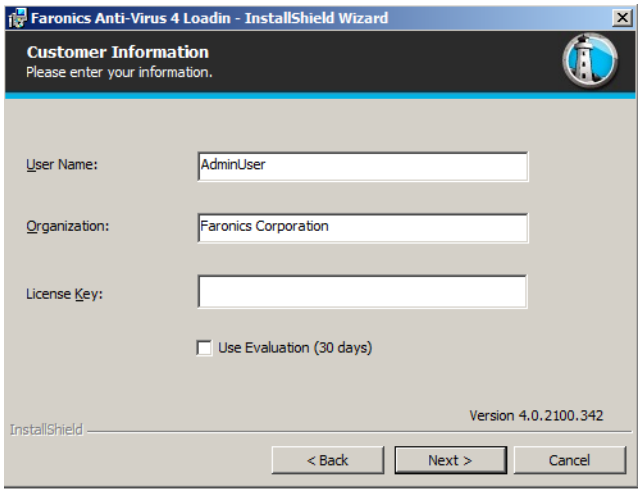
1. Double-click *Anti-VirusLoadinInstaller.exe*. Click *Next*.



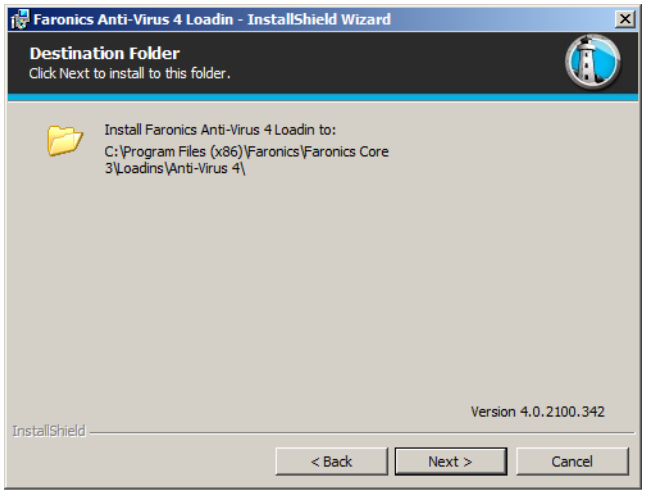
2. Read and accept the License Agreement. Click *Next*.



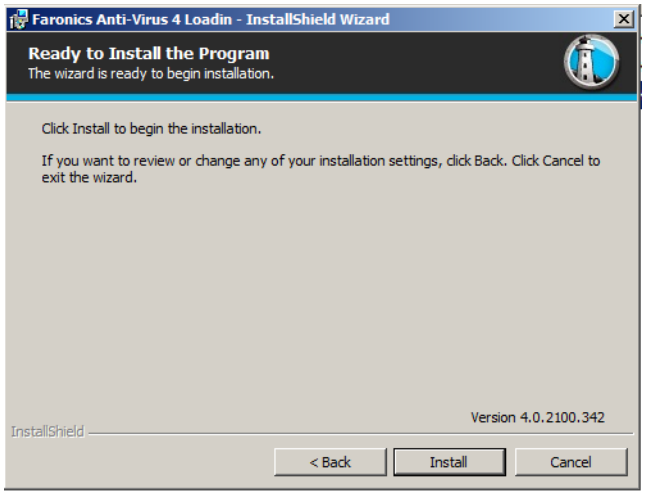
3. Enter the *User Name*, *Organization* and the *License Key*. Alternatively, select the *Use Evaluation* checkbox. Faronics Anti-Virus expires after 30 days of evaluation. Click *Next*.



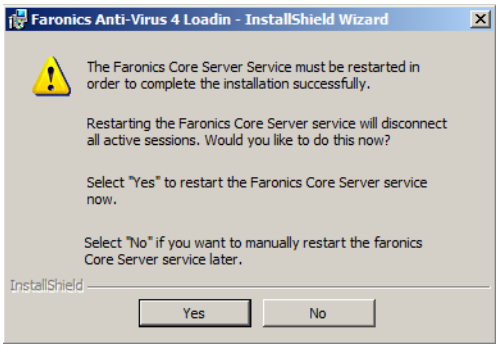
4. The default location is *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus*.



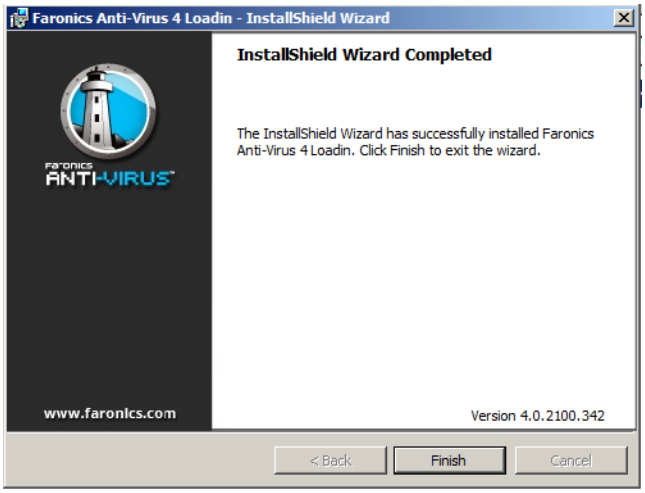
5. Click *Install* to install Faronics Anti-Virus Loadin.



6. The following message is displayed. Click *Yes* to restart the Faronics Core Server service. Click *No* to manually restart the Faronics Core Server service later.



7. Click *Finish* to complete installation.



Installing or Upgrading Faronics Anti-Virus on a Workstation via Faronics Core

The Core Agent, which is part of Faronics Core, must be installed on each workstation that will be managed by Faronics Anti-Virus. For more information on installing the Core Agent, refer to the Faronics Core user guide. The latest user guide is available at http://www.faronics.com/library.

Once the Core Agent is installed, the workstations are detected on the network and visible in Core Console.

To install or upgrade Faronics Anti-Virus, select a single workstation or multiple workstations:

1. Click Configure Workstations in the right pane and select *Advanced*>*Install/Upgrade Faronics Anti-Virus Client*.
2. Select the following options if you have another Anti-Virus program installed:
   - > Remove any incompatible Anti-Virus products before installing Faronics Anti-Virus Enterprise Workstation.
   - > Install Faronics Anti-Virus even if another Anti-Virus product is present or its removal failed.

The workstation reboots after a successful install or upgrade.

If there is more than one Loadin installed, the right-click contextual menu for Faronics Anti-Virus can be accessed by right-clicking a workstation, selecting *Anti-Virus* and then selecting the particular action.

Installing Faronics Anti-Virus on a Workstation Manually

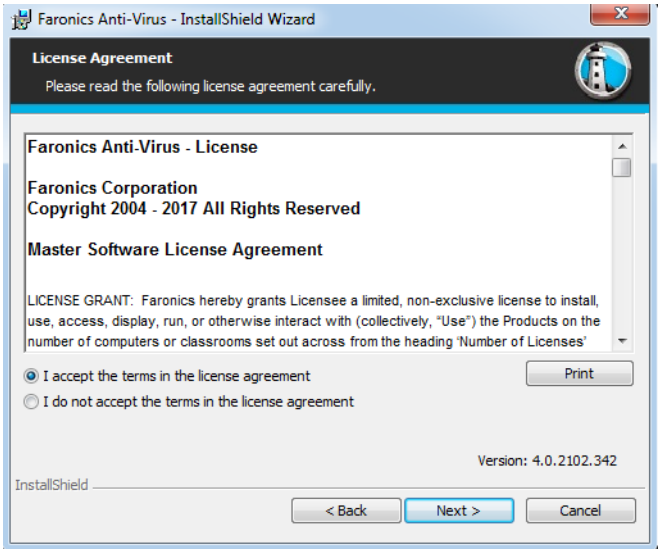
Before installing Faronics Anti-Virus Client on a workstation, copy the appropriate *.msi* file from the path *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers* on the computer where the Anti-Virus Loadin is installed to one or more workstations.

Repeat the process for each workstation that will be protected with Faronics Anti-Virus.

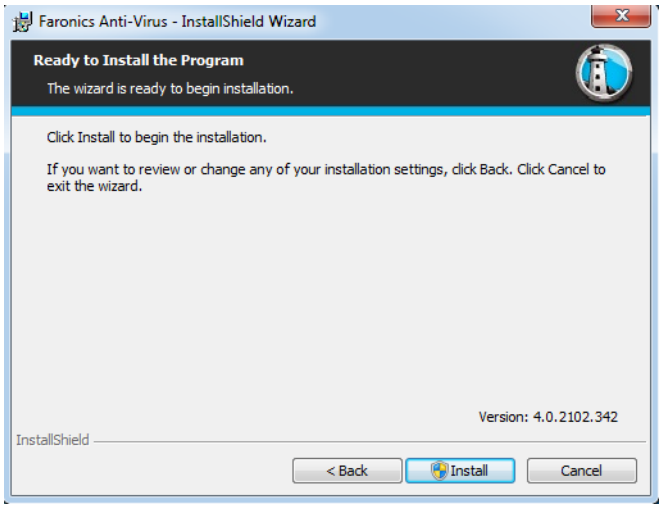
Complete the following steps to install Faronics Anti-Virus on the workstation:

1. Double-click *AntiVirus_Ent_32-bit.msi* on a 32-bit operating system and *AntiVirus_Ent_64-bit.msi* on a 64-bit operating system. Click *Next*.

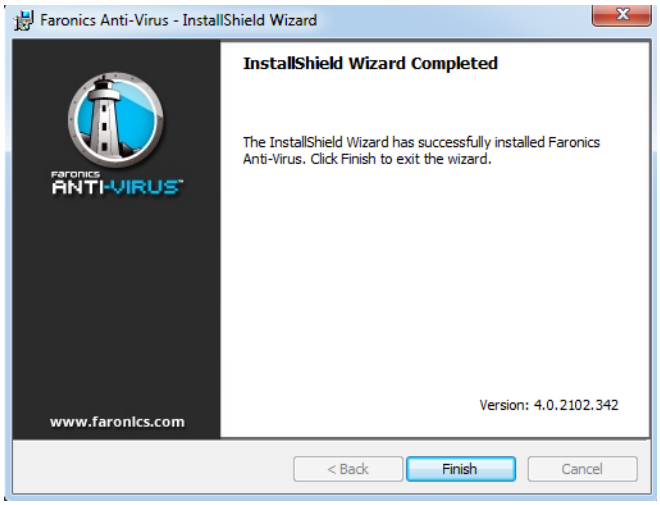
2. Read and accept the License Agreement. Click *Next*.



3. Click *Install* to install Faronics Anti-Virus.



4. Click *Finish* to complete installation.



An immediate restart is recommended after installing the Anti-Virus Client on the workstation.

Using Faronics Anti-Virus

This chapter explains how to use Faronics Anti-Virus.

Topics

Faronics Anti-Virus Overview

Faronics Anti-Virus can be used in the following ways:

Managing Faronics Anti-Virus via Faronics Core Console:

- Install Faronics Anti-Virus Loadin (for more information, refer to Installing Faronics Anti-Virus Loadin)
- Deploy Faronics Anti-Virus Client on the workstation(s)
- Create, Edit, Delete and Apply an Anti-Virus Policy
- Scan Workstation(s) via Faronics Core Console
- Enable/Disable the Firewall
- View Scanning History
- Viewing and Taking Action on Quarantined Files
- Updating Anti-Virus Definitions via Faronics Core Console
- Generating Reports
- Enable/Disable Active Protection
- View Logs

Using Faronics Anti-Virus on the Workstation

- Launching Faronics Anti-Virus on the workstation
- Scanning the workstation
- Updating Anti-Virus Definitions on the workstation
- Enable/Disable Active Protection
- Enable/Disable Firewall
- View Scanning History
- Quarantined

Managing Faronics Anti-Virus via Faronics Core Console

Once the Faronics Anti-Virus Loadin is installed, the workstations can be managed via Faronics Core Console. Various aspects of managing Faronics Anti-Virus via Faronics Core Console are explained in the subsequent sections.

Deploying Faronics Anti-Virus Client on the workstation(s)

Complete the following steps to deploy Faronics Anti-Virus Client on the workstation(s):

1. Launch Faronics Core Console.
2. In the Console Tree pane, go to *Faronics Core Console>[Core Server Name]>Workstations>Managed Workstations*.
3. Right-click on one or more workstations and select *Anti-Virus>Install/Upgrade Anti-Virus Client*.

Faronics Anti-Virus Client is installed on the workstation(s).

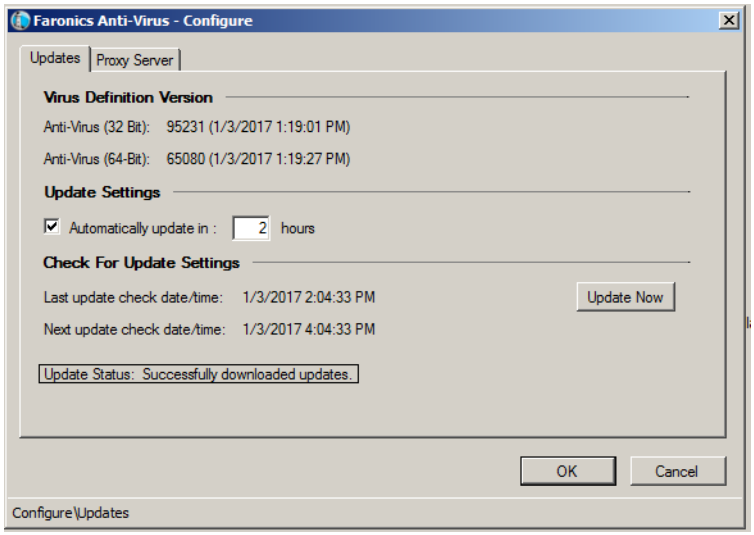
After a successful deployment the workstation has the Default policy and the latest virus definitions.

Configuring Faronics Anti-Virus

Complete the following steps to configure Faronics Anti-Virus:

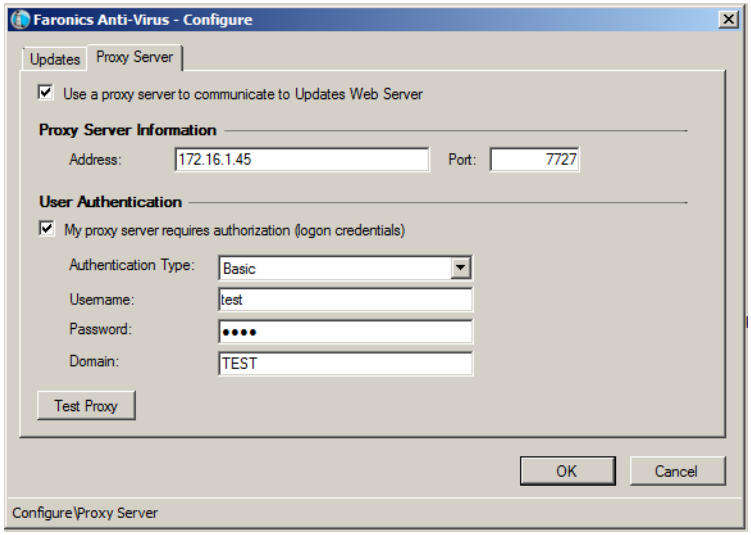
1. Launch Faronics Core Console.
2. In the Console Tree pane, go to *Faronics Core Console>[Core Server Name]>Workstations>Managed Workstations>Anti-Virus*.
3. Right-click on Anti-Virus and select *Configure Anti-Virus*.
4. The *Updates* tab in the *Configure Faronics Anti-Virus* dialog is displayed.

5. The *Updates* tab displays the Scan Engine version and Virus Definition version. Specify the following options:



   > Automatically update (in hours) – select the checkbox to automatically update virus definitions.
   > Hours – specify a value between 1 to 72 hours.
   > Update Now – click this button to update Anti-Virus definitions.

6. Click the *Proxy Server* tab and specify values for the following options:



7. Select Use a proxy server to communicate to Updates Web Server and specify the following information:

   > Address – specify the IP address or URL.
   > Port – specify the port.

8. Select the User a proxy server to communicate to Updates Web Server and specify the following settings:
   - > Authentication Type
   - > Username
   - > Password
   - > Domain
9. Click *Test* to test the connection. Click *OK* to save proxy settings.

Refreshing Faronics Anti-Virus

To retrieve settings from a single workstation running Faronics Anti-Virus, complete the following steps:

1. Launch Faronics Core Console.
2. In the Console Tree pane, go to *Faronics Core Console>[Core Server Name]>Workstations>Managed Workstations*.
3. Right-click on a workstation and select *Refresh Anti-Virus*.
4. Faronics Anti-Virus is refreshed and the following columns are updated:
   - > Policy Name
   - > Status
   - > % Scan Complete
   - > Definitions version
   - > Date of Last Update
   - > Date of Last Scan
   - > Date of Last Threat Detected
   - > Version

Faronics Anti-Virus Policy

An Anti-Virus Policy contains all the configuration settings on how Faronics Anti-Virus runs on the workstation(s). A policy contains the action taken by the program, schedule, proxy servers, error reporting and the functionality allowed to the user on the workstation(s). The following sections explain how an Anti-Virus policy is created and applied.

If you are using the Legacy Anti-Virus, complete the following steps to migrate to the new Anti-Virus:

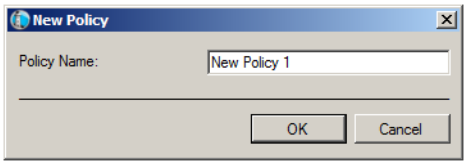
1. Uninstall the Legacy Anti-Virus from the managed workstations.
2. Configure the new Anti-Virus Policy.
3. Install the new Anti-Virus on the managed workstations.

Faronics Anti-Virus contains a *Default* policy. The Default policy contains the most optimum configuration settings for managing Faronics Anti-Virus.

Creating Anti-Virus Policies

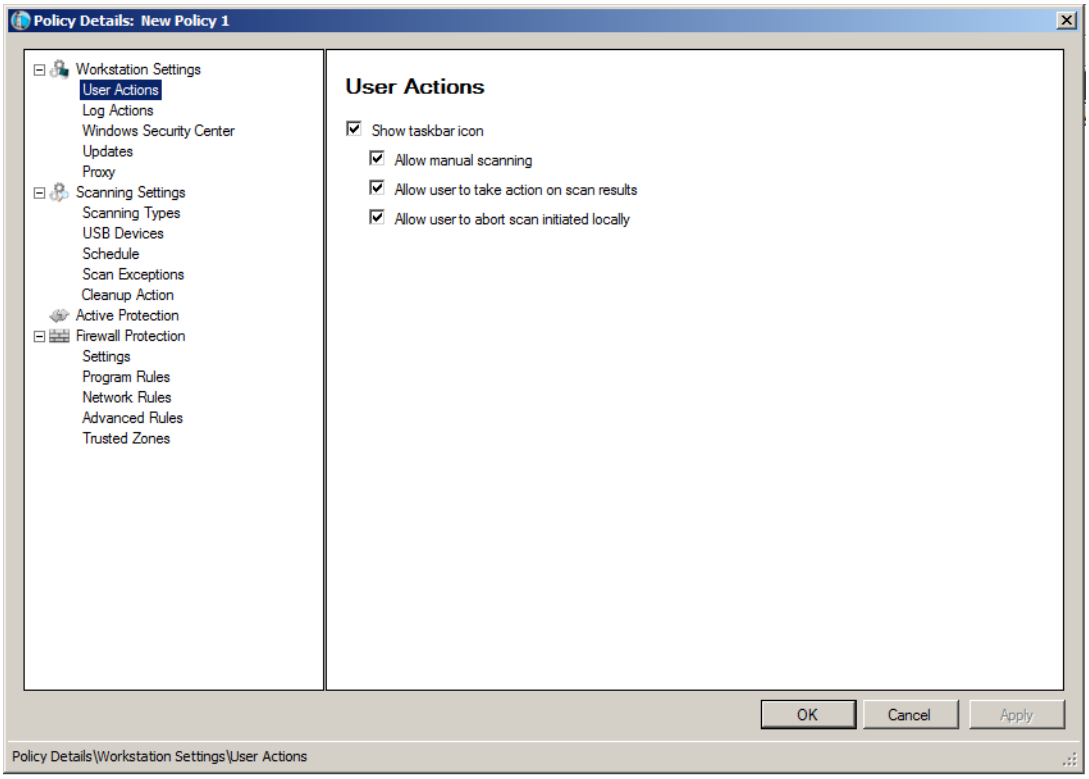
Complete the following steps create a new Anti-Virus Policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server Name]>Workstations>Managed Workstations>Anti-Virus*.
3. Right-click on the *Anti-Virus* and select *New Policy*.
4. Specify a name for the policy in the *New Policy* dialog. Click *OK*. A new policy is created under the *Anti-Virus* node policy. For example, you can name the new policy as *New Policy 1*.



5. Right-click on *New Policy 1* and select *Policy Details*. The *Policy Details* dialog is displayed.
6. Specify settings in the *Workstation Settings* node.

- *User Actions* pane



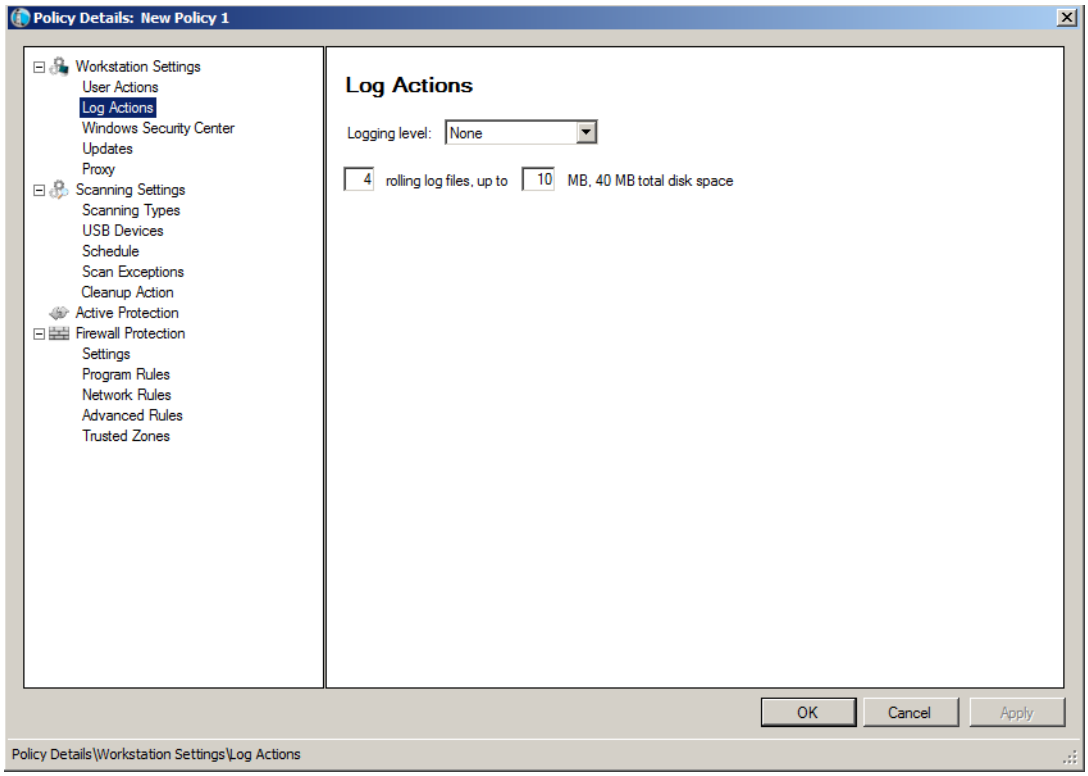
> Show taskbar icon – Select the checkbox to display Faronics Anti-Virus icon on the taskbar at the workstation(s). If this checkbox is not selected, Faronics Anti-Virus will be hidden to the user.

~ Allow manual scanning – Select the checkbox to allow users to manually initiate Faronics Anti-Virus scanning at the workstation(s).

~ Allow user to take action on scan results – Select the checkbox to allow the workstation user to take action on the scan results.

~ Allow user to abort a scan initiated locally – Select the checkbox to allow users to abort the scan initiated locally at the workstation.

- *Log Actions* pane

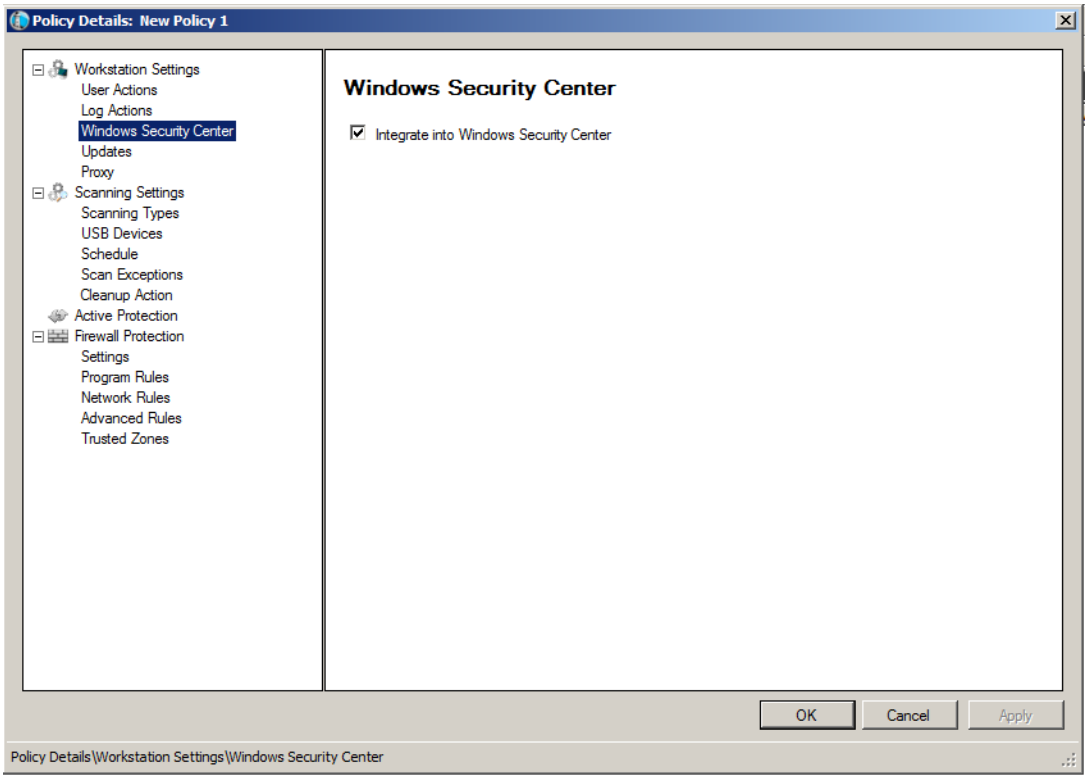


> Logging Level – Select the logging level. Select *None* for no logging. Select *Error* to log the error message. Select *Trace* for trace. Select *Verbose* for detailed logging.

> Number of logging files – Specify the number of logging files. The logging information is stored in the files serially. For example, if there are 3 files A, B and C, Faronics Anti-Virus first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.

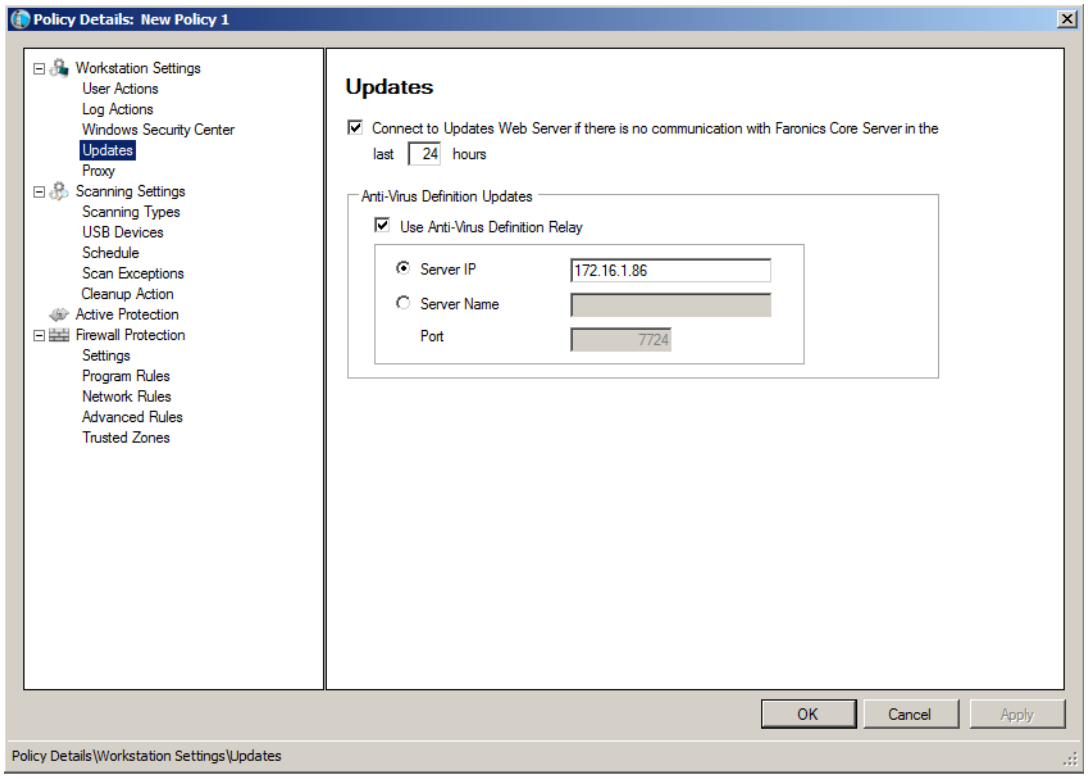
> File size – Select the size of each file in MB.

- *Windows Security Center* pane



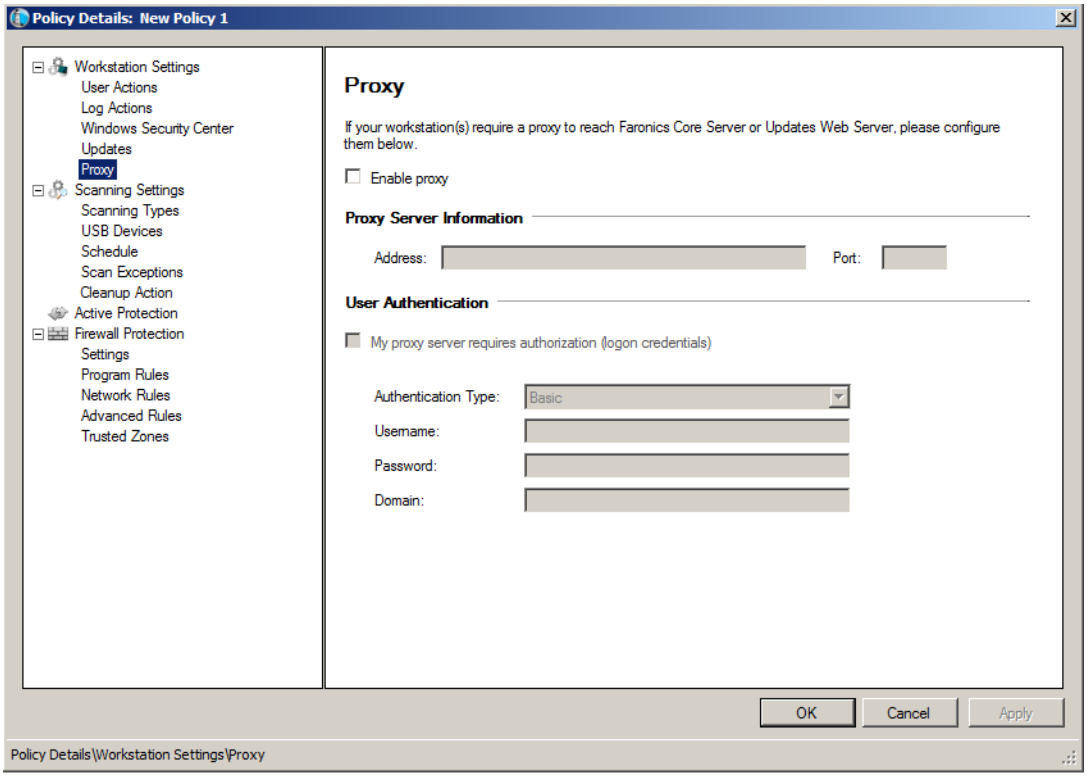
> Integrate into Windows Security Center – Select the checkbox to integrate Faronics Anti-Virus into the Windows Security Center. Windows Security Center will notify you via the System Tray if Faronics Anti-Virus is active or inactive.

- *Updates* pane



> Connect to Updates Web Server if there is no communication with Faronics Core Server in the last x hours – Select the checkbox to connect to the Updates Web Server and download Virus Definitions if the workstation loses contact with Faronics Core Server. If you do not select this checkbox, the Virus Definitions will not be updated if the workstation loses the connection with the Faronics Core Server.

- *Proxy* pane



> Enable Proxy – Select the checkbox if the workstation(s) require a proxy to reach Faronics Core Server or Updates Web Server.

> Proxy Server Information – Specify the *Address* and *Port*.

> User Authentication

  My proxy server requires authorization (logon credentials) – If the server requires authentication, specify values for the following fields:

  ~ Authentication Type – Select the authentication type.

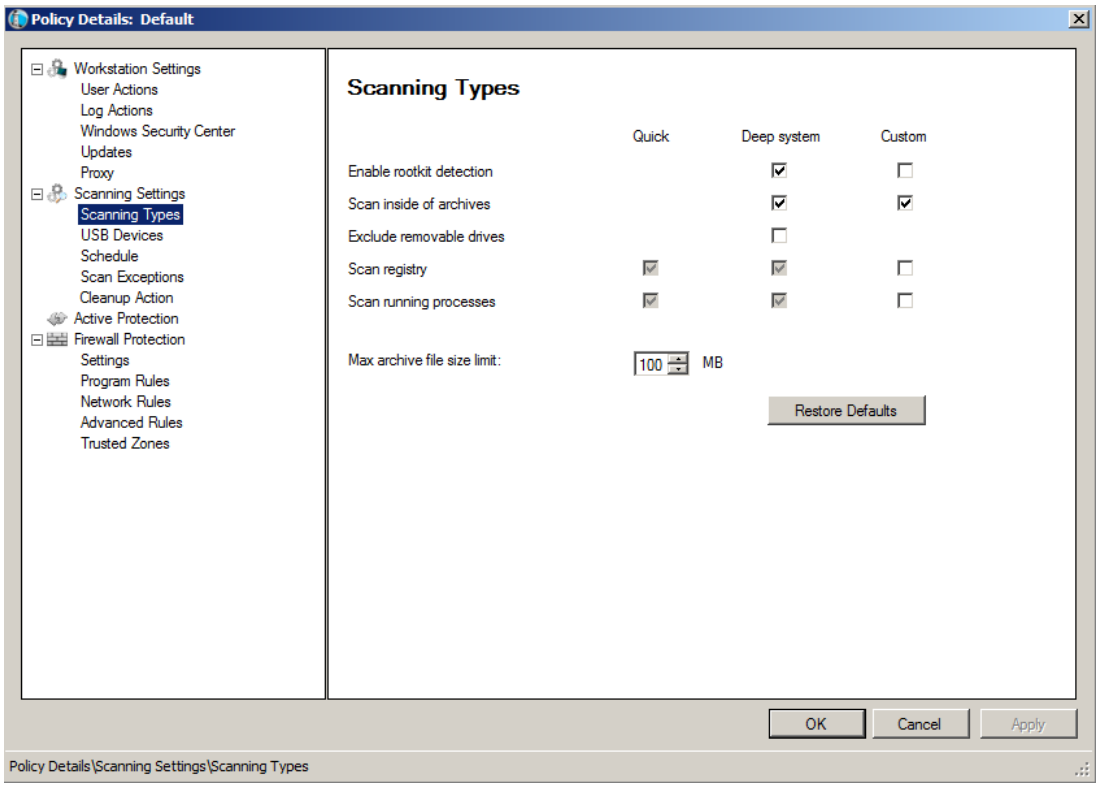
  ~ Username – Specify the username.

  ~ Password – Specify the password.

  ~ Domain – Specify the domain.

7. Specify settings in the *Scanning* Settings node.

- *Scanning Types* pane



Faronics Anti-Virus provides three types of scans:

> Quick Scan – Scans the commonly affected areas of your computer. This is shorter in duration than the Deep System Scan. Quick Scan also uses less memory than the Deep System Scan.

> Deep System Scan – Performs a through scan of all areas of the computer. The time taken for the scan depends on the size of your hard drive.

> Custom Scan – Performs a scan based on the selections made in the *Policy Details* dialog.

For each type of scan, select the following options (some options may be grayed out depending on the type of scan):

> Enable rootkit detection – Detects if the computer is infected with a rootkit.

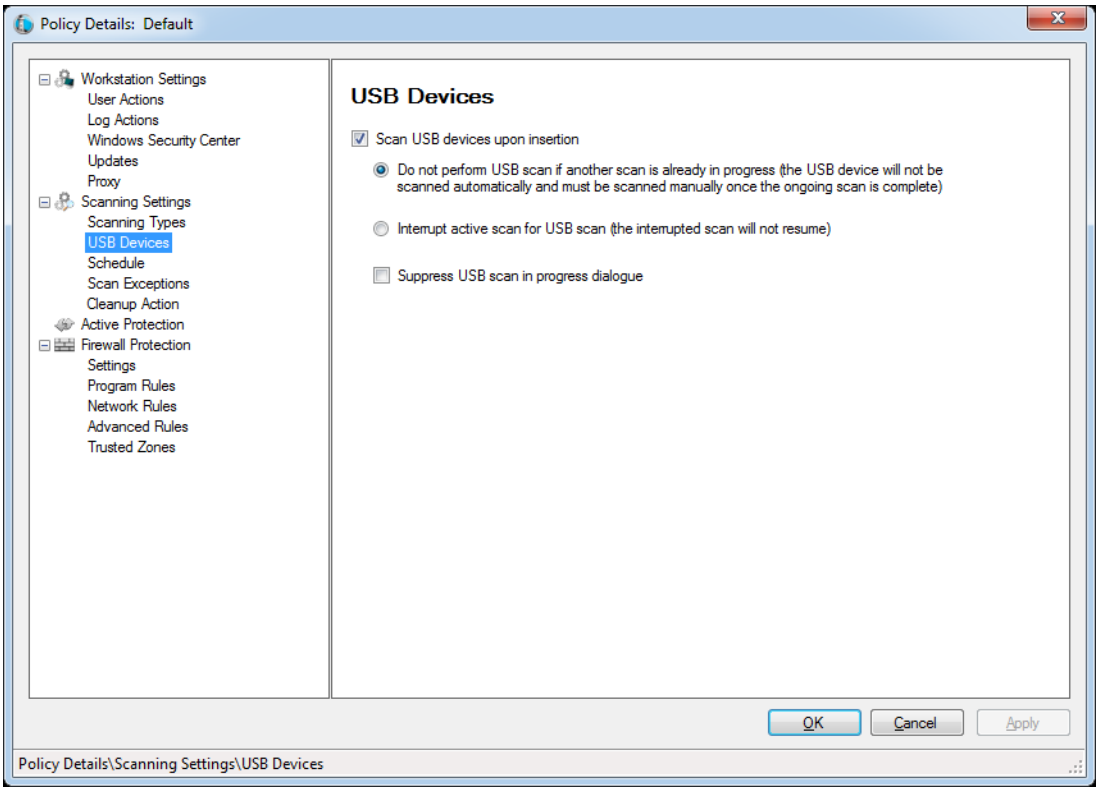
> Scan inside of archives – Scans the contents of a zip file. Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined. Specify the *File Size Limit*.

> Exclude removable drives (e.g USB) – Excludes the removable drives from the scan process. Any external hard disks, USB drives etc will not be scanned.

> Scan the registry – Scans the registry.

> Scan running process – Scans all running processes.

- *USB Devices* pane



Select the checkbox to scan USB drives upon insertion and select one of the following options:

> Do not perform USB scan if another scan is already in progress – Select this option to ensure that an active scan is not interrupted when a USB drive is inserted. The USB drive must be manually scanned once the active scan is complete.

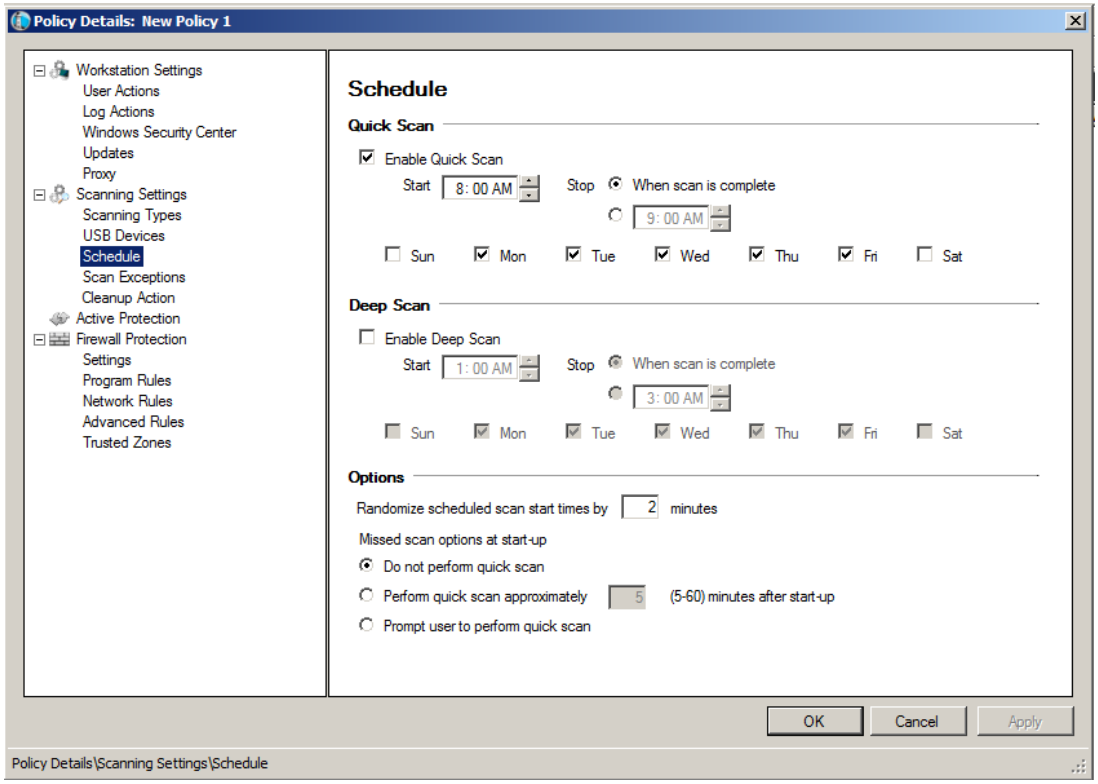
> Interrupt active scan for USB scan – Select this option to interrupt an active scan to scan the USB drive when it is inserted. Once the active scan is interrupted, it will not resume automatically and must be restarted manually.

> Suppress USB scan in progress dialogue – Select this option to hide indications that Anti-Virus is scanning USB drives when they are inserted; no Anti-Virus interface will open, and the system tray icon will not display tooltips indicating a scan in progress. Users will be notified at the end of a scan if a virus was found, but if no viruses were detected there will be no notification that the scan occurred.

  Note that if the Scan USB drives upon insertion option is not selected, this option is ignored.

If the *Allow Manual Scanning* checkbox is selected in the *Workstation Settings* tab>*User Actions* pane, the USB device is scanned automatically. If the *Allow Manual Scanning* checkbox is not selected, the USB device is not scanned automatically.

- *Schedule* pane



Quick Scan:

> Enable Quick Scan – Select the checkbox to enable Quick Scan.

> Start – Specify the start time.

> Stop – Specify the end time. The maximum duration between the *Start* time and *Stop* time is *23.59* hours. The scan ends if all the files are scanned before the *Stop* time. If the scan is not complete before the *Stop* time, it is aborted at the *Stop* time. Alternatively, select *When scan is complete* to ensure that scan is completed.

> Days – Select the days when the scheduled Quick Scan will take place.

Deep Scan:

> Enable Deep scan – Select the checkbox to enable Deep Scan.

> Start – Specify the start time.

> Stop – Specify the end time. The maximum duration between the *Start* time and *Stop* time is 23.59 hours. The scan ends if all the files are scanned before the *Stop* time. If the scan is not complete before the *Stop* time, it is aborted at the *Stop* time. Alternatively, select *When scan is complete* to ensure that scan is completed.

> Days – Select the days when the scheduled Deep Scan will take place.

Options:

> Randomize scheduled scan start times by x minutes – Specify the number of minutes. The scheduled scan start time is randomized to reduce the impact on network traffic. Faronics Anti-Virus reports to Faronics Core when the scanning starts. This might impact the network traffic if the scan for multiple systems start at the same time.

Missed scan options at start-up – Select one of the following options on how a scan will be performed if the workstation was not *ON* during a scheduled scan:

> Do not perform quick scan – Select this option if you do not want to perform quick scan on startup.

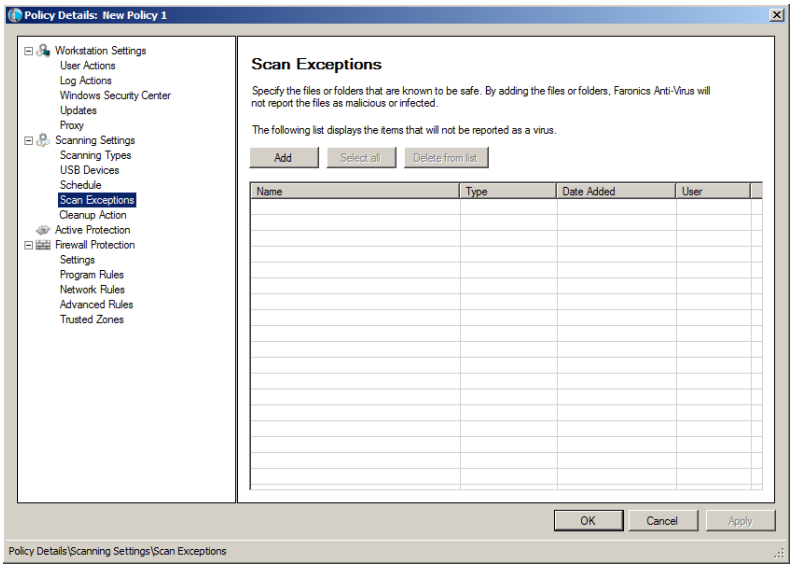
> Perform quick scan approximately x minutes after start-up – Specify the number of minutes after start-up when Faronics Anti-Virus must perform a quick scan.

> Prompt user to perform Quick Scan – Select this option to prompt the user to perform a quick scan.

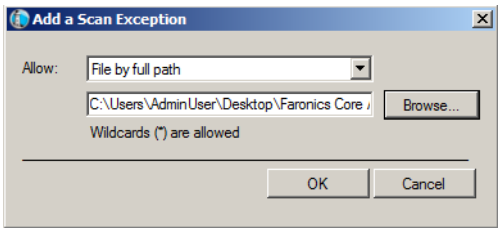
- *Scan Exceptions* pane

  Folders or files that are known to the safe and free of infections can be added to the Scan Exceptions tab. Files added to the Scan Exceptions tab will always be scanned by Faronics Anti-Virus. However, Faronics Anti-Virus will never report the files as malicious or infected. This feature is useful since files and folders that are known to be safe by the Administrator will not be reported as malicious.

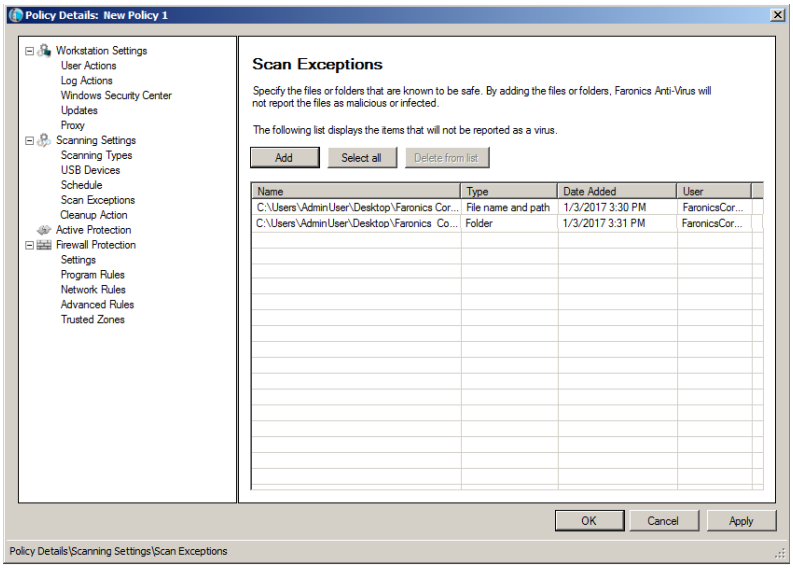
  A. Click *Add*.



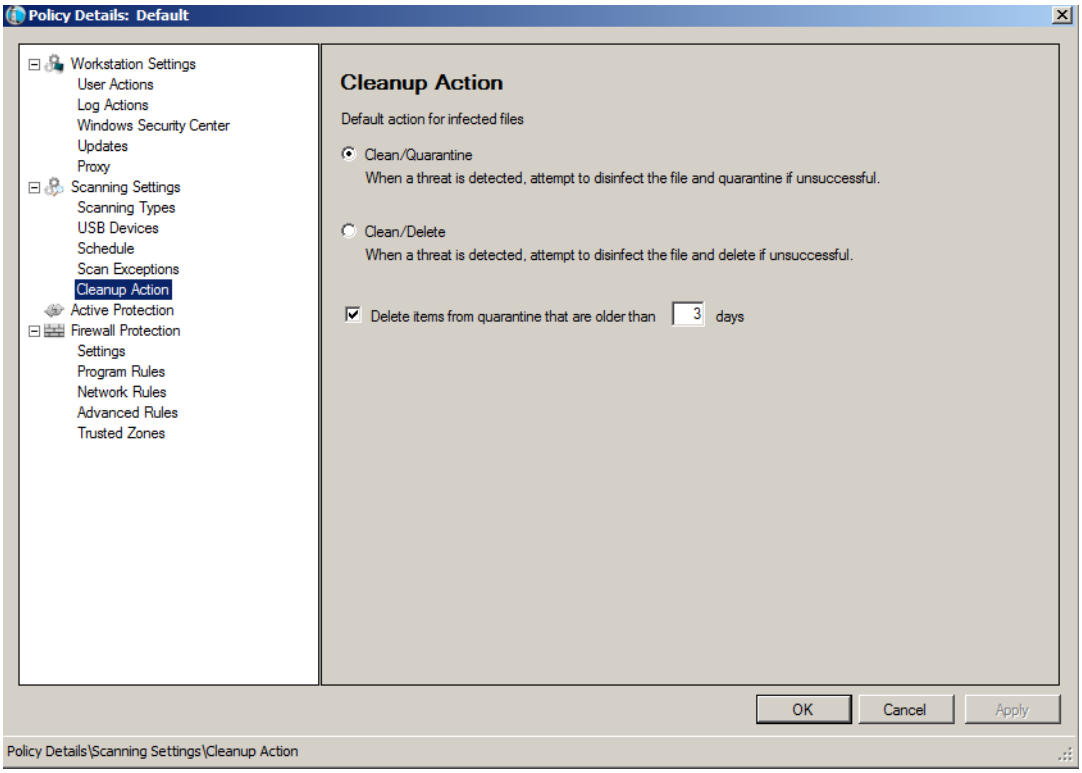
  B. In the *Add* dialog, select *File by full path* or *Entire folder*. Click *Browse* to select the file or folder and click *OK*.



  C. The *File by full path* is added to the Scan Exceptions pane.



- *Cleanup Action* pane

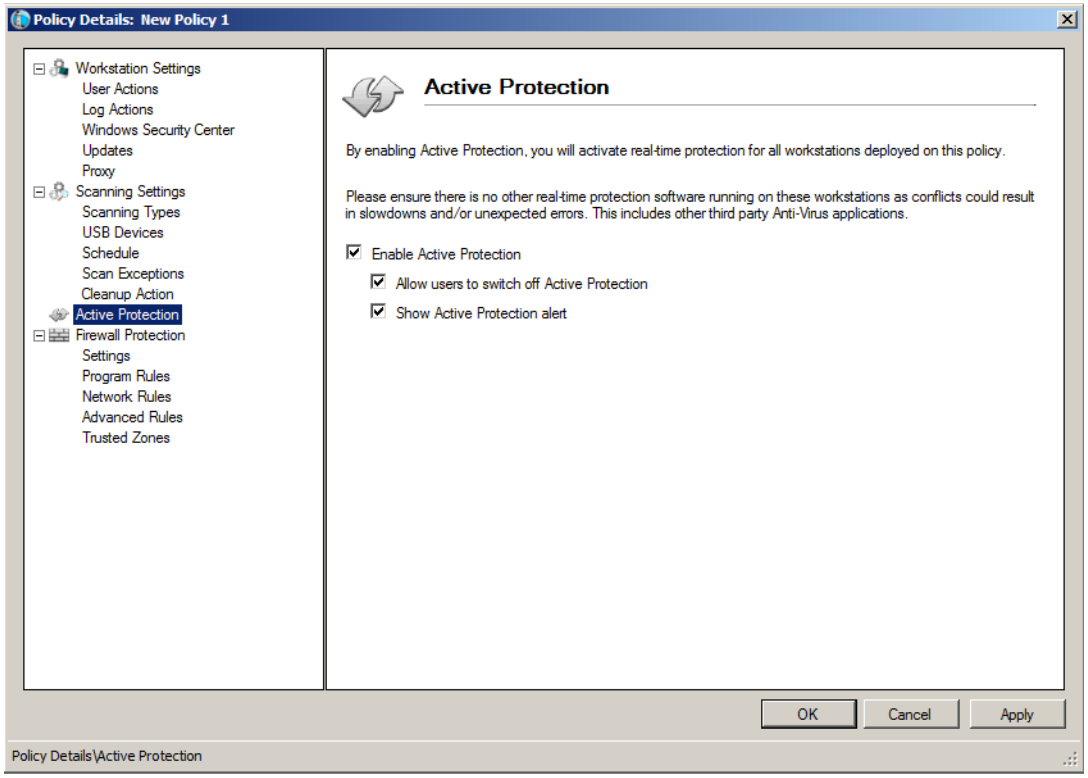


> Clean/Quarantine – When a threat is detected, attempt to disinfect the file and quarantine if unsuccessful. If the file could not be disinfected, it will be quarantined and will not be deleted.

> Clean/Delete – When a threat is detected, attempt to disinfect the file and delete if unsuccessful. If the file could not be disinfected, it will be deleted from the computer.

> Delete items from quarantine that are older than – Specify the number of days to retain items in quarantine. The default is 3 days.

8. Specify settings in the *Active Protection* pane.

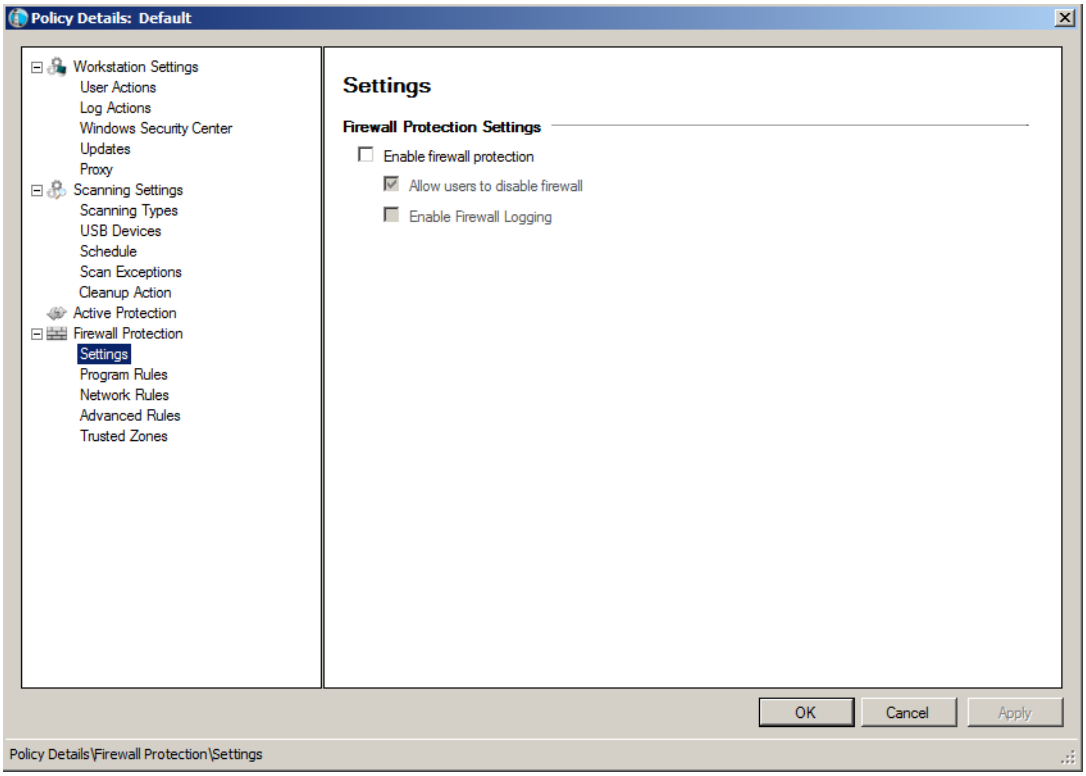


- Enable Active Protection – Select this option to enable real-time protection. Active Protection is the real-time scanning by Faronics Anti-Virus in the background without any impact on system performance. If there is a risk of real-time virus infection from the Internet, select this option.
  - > Allow users to switch off Active Protection – Select this option to allow users to switch off Active Protection. If users install or use software that might be mistaken from a virus (for example, running advanced Macros in Microsoft Office or complex batch files), select this option.
  - > Show Active Protection alert – Select this option to display an alert if a threat is detected during Active Protection. Do not select this checkbox if you do not want an alert to be displayed.

9. Specify settings in the *Firewall Protection* node.

   The Firewall Protection node provides bi-directional protection, protecting you from both incoming and outgoing traffic. You can create customized rules to protect your network. You can either *Allow* or *Block* the communication.

- *Settings* pane



Firewall Protection Settings

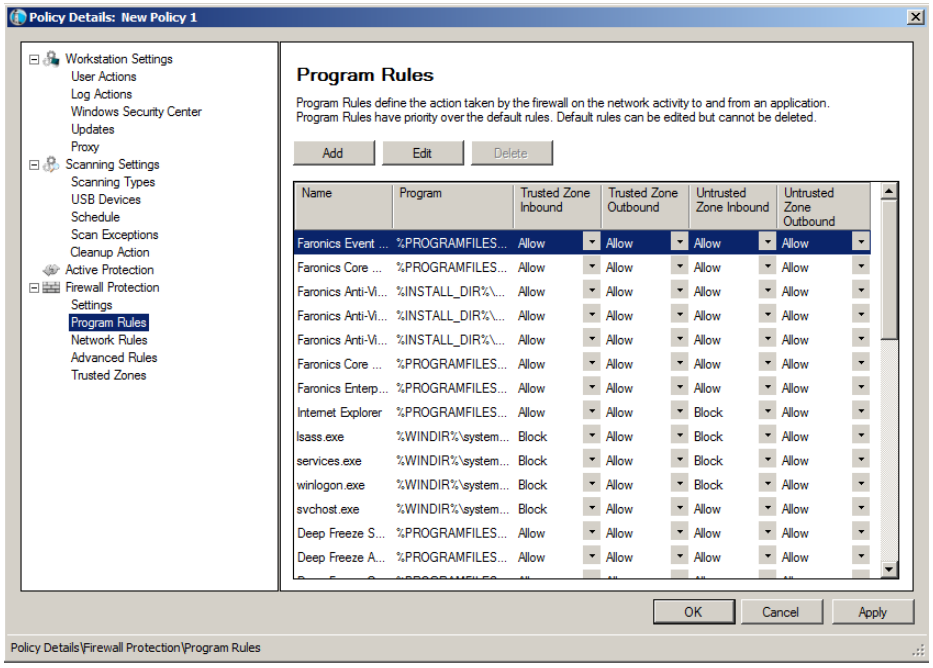
> Enable Firewall Protection – Select the checkbox to enable Firewall Protection. Firewall Protection prevents hackers or malicious software from gaining access to your computer through the Internet or the network.

  ~ Allow users to disable firewall – Select this option to allow users to disable the firewall at the computer.

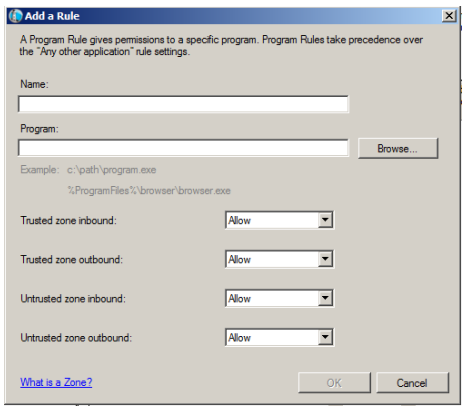
  ~ Enable Firewall Logging – Select this option to log all actions related to the Firewall.

- *Program Rules* pane

  Program Rules define the action taken by the firewall on the network activity to and from an application. Program Rules have priority over the default rules. Default rules can be edited but cannot be deleted.



Click *Add* to add a new Program Rule. Specify or select the options and click *OK*. The following parameters are displayed:



> Name – Name of the rule.

> Program – Name of the program, including full path and extension.

> Trusted Zone Inbound – The action to be taken for inbound communication to the program in a Trusted Zone (*Allow* or *Block*).

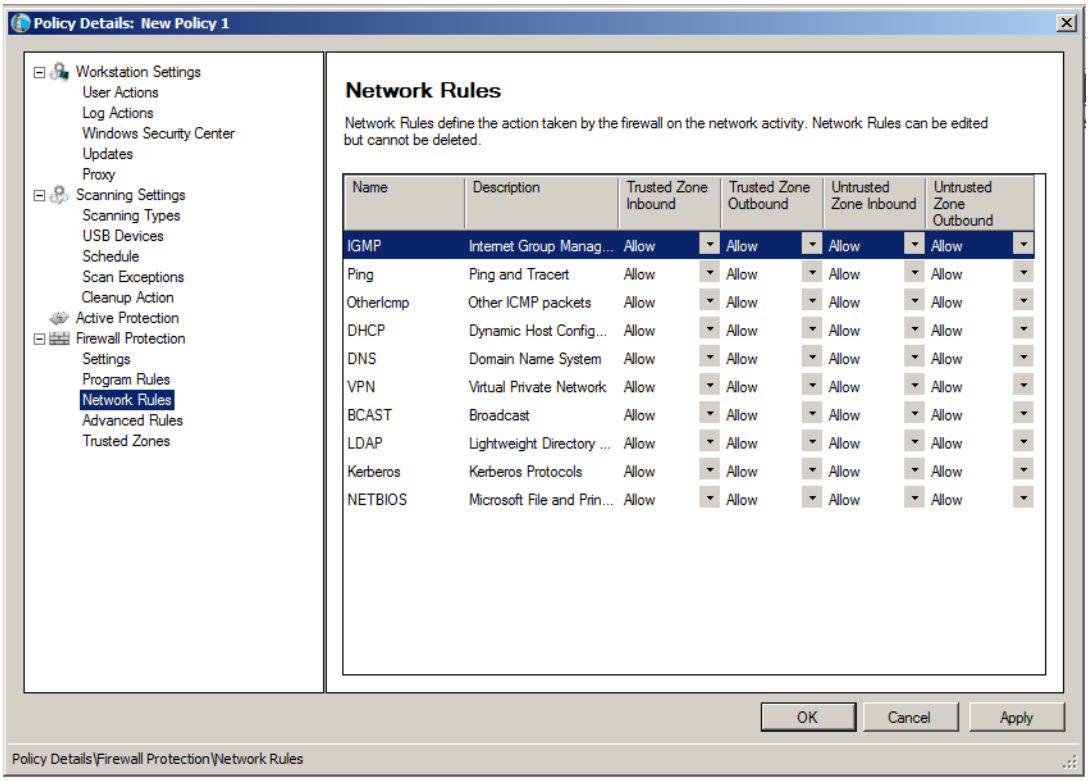
> Trusted Zone Outbound – The action to be taken for outbound communication from the program in a Trusted Zone (*Allow or Block*).

> Untrusted Zone Inbound – The action to be taken for inbound communication to the program in an Untrusted Zone (*Allow* or *Block*).

> Untrusted Zone Outbound – The action to be taken for inbound communication from the program in an Untrusted Zone (*Allow or Block*).

- *Network Rule* pane

  Network Rules define the action taken by the firewall on the network activity. Network Rules can be edited but cannot be deleted.

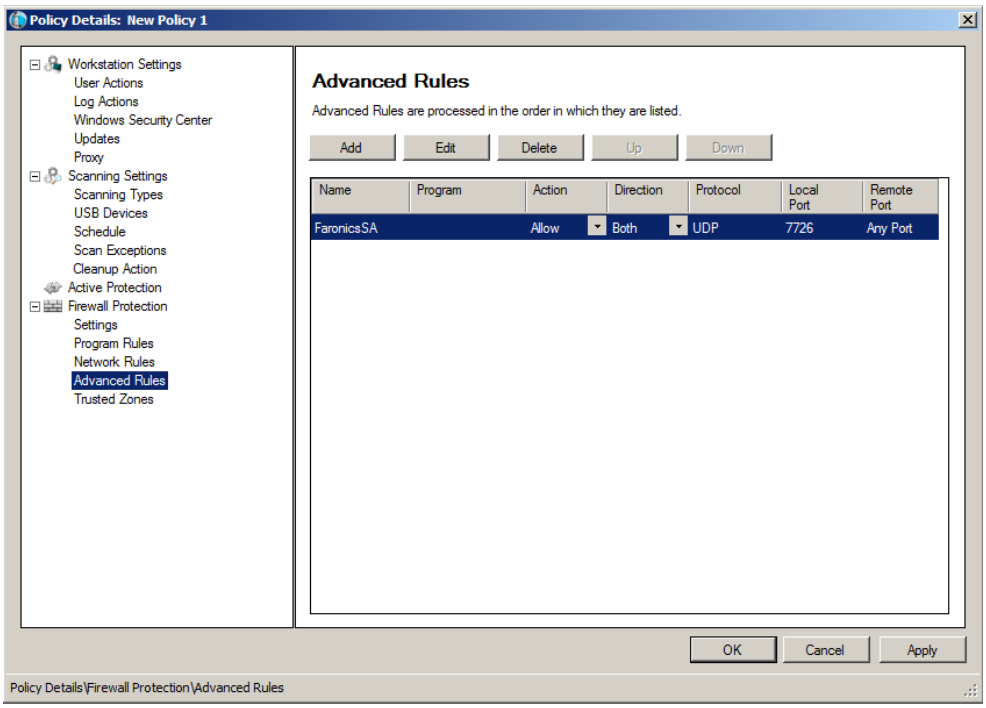


Select the Network Rules for the following:

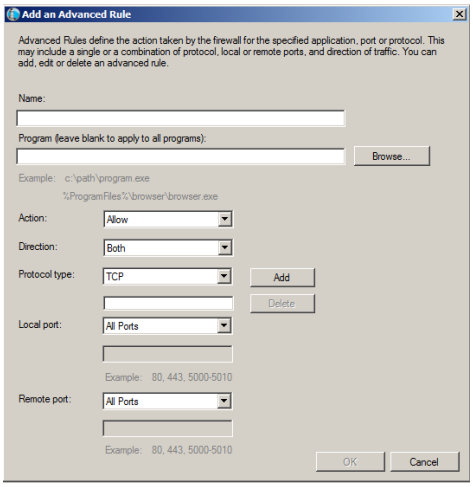
Name	Description	Trusted Zone Inbound	Trusted Zone Outbound	Untrusted Zone Inbound	Untrusted Zone Inbound
IGMP	Internet Group Management Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Ping	Ping and Tracert	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
OtherIcmp	Other ICMP packets	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DHCP	Dynamic Host Configuration Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DNS	Domain Name System	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
VPN	Virtual Private Network	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
BCAST	Broadcast	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
LDAP	Lightweight Directory Access Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Kerberos	Kerberos Protocols	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
NETBIOS	Microsoft File and Printer Sharing	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block

- *Advanced Rules* pane

  Advanced Rules define the action taken by the firewall for the specified application, port or protocol. This may include a single or a combination of protocol, local or remote ports, and direction of traffic. You can add, edit or delete an advanced rule.



Click *Add* to add a new Advanced Rule. Specify or select the options and click *OK*. The following parameters are displayed in the Advanced Rules pane:



> Name – Name of the rule.

> Program – Name of the program and path.

> Action – The action taken by the Firewall for communication from the specified application, port or protocol (Allow or Block).

> Direction – The direction of communication (*Both*, *In or Out*).

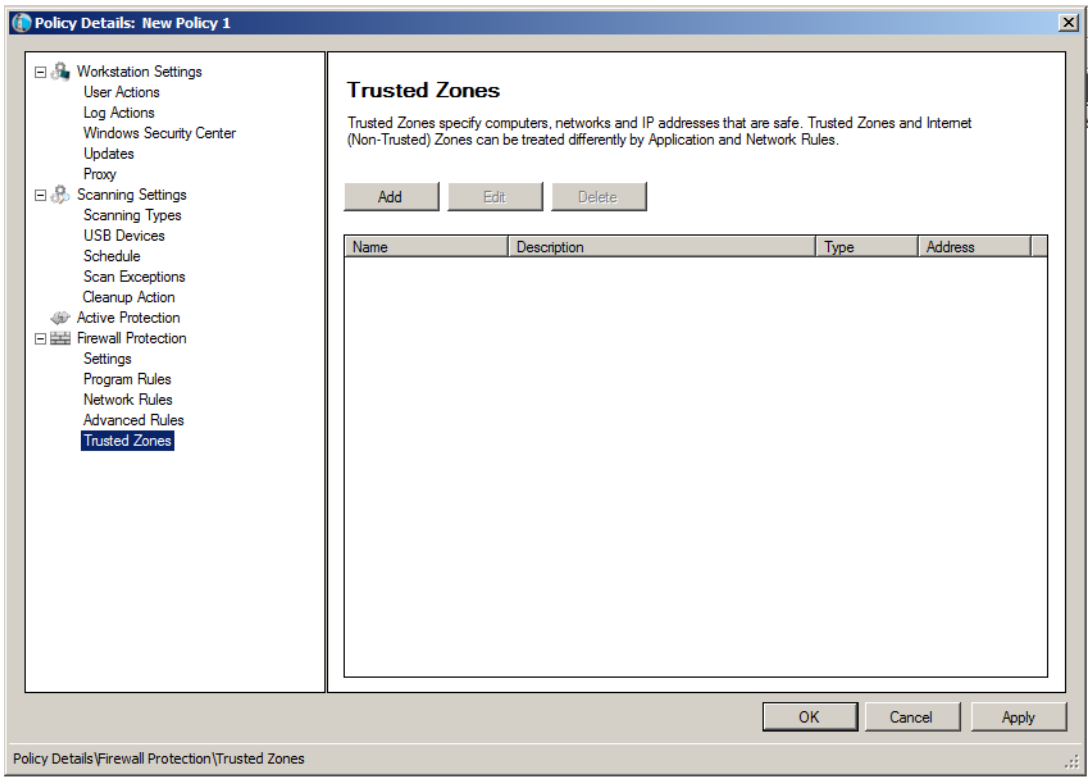
> Protocol type – The type (ICMP, IGMP, TCP, UDP) and name of the protocol.

> Local Port – Details of the local port.

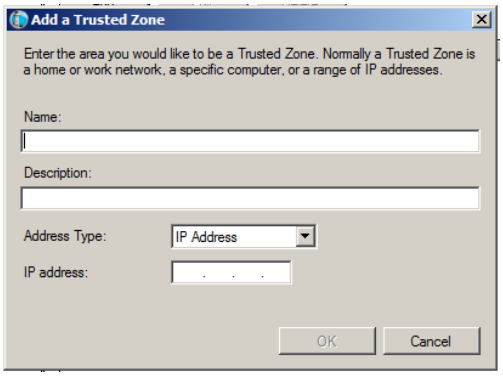
> Remote Port – Details of the remote port.

- *Trusted Zones* pane

  Trusted Zones specify computers, networks and IP addresses that are trusted. Trusted Zones and Internet (Non-Trusted) Zones can be treated differently by Program and Network Rules.



  Click *Add* to add a new Trusted Zone. Specify or select the options and click *OK*. The following parameters are displayed:



  > Name – Name of the Trusted Zone.

  > Description – Description of the Trusted Zone.

  > Type – Type of the Trusted Zone (*IP Address* or *Network*).

10. Click *OK*. The new policy, *New Policy 1* is displayed below the *Anti-Virus* node.

Applying an Anti-Virus Policy

Once the Anti-Virus policy has been created, it can be applied on one or more workstations via Faronics Core Console. Complete the following steps to apply the policy:

1. Select one or more workstations. Right-click and select *Reassign Policy*.
2. The *Reassign Workstation(s) to Policy* dialog is displayed. Select the policy from the *Assign Policy* drop-down and click *OK*.
3. The policy is applied to the selected workstation(s).

Viewing or Modifying an Anti-Virus Policy

Once the Anti-Virus policy has been created, it can be viewed or modified. Complete the following steps to view or modify a policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Policy Details*.
4. To edit the policy, modify the settings in the tabs as explained in Creating Anti-Virus Policies.
5. Click *OK* to apply the changes.
6. Changes made to a policy will be automatically applied to the workstation(s) managed by the policy.

Renaming an Anti-Virus Policy

Once the Anti-Virus policy has been created, it can be renamed. Complete the following steps to rename a policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Rename Policy*. The *Rename Policy* dialog is displayed.
4. Enter the *New policy name* and click *OK*.

Copying a Policy

An existing policy can be easily copied into a new policy. Alternatively, the data in an existing policy can be copied to another existing policy.

Complete the following steps to copy a policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Copy Policy*. The *Copy Policy* dialog is displayed.
4. Select a *Destination Policy* from the drop-down or click *New* to copy the data into a new policy. Specify a name for the New policy.
5. Click *Copy Policy Data Now*.

The data is copied into an existing policy or a new policy is created with the existing as selected in step 3.

Deleting an Anti-Virus Policy

Complete the following steps to delete an existing policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Delete Policy*. The *Delete Policy* dialog is displayed.
4. Click *Yes* to delete the policy.

If a policy assigned to a workstation is deleted, it is replaced by the Default Policy. It is not possible to delete the Default Policy.

Importing an Anti-Virus Policy

A preconfigured Anti-Virus policy can be imported into an existing policy. This feature saves time since the entire policy does not have to be reconfigured again.

Complete the following steps to import an existing policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Import Policy*. Click *Yes* to overwrite the current settings in the existing policy.
4. Browse to select the policy to be imported. Only previously exported policies in XML format can be imported.
5. Select a previously exported policy and click *Open*. The policy is imported.

Exporting an Anti-Virus Policy

A pre-configured Anti-Virus policy can be exported for reuse. This feature saves time since the entire policy does not have to be reconfigured again.

Complete the following steps to export an existing policy:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus>[Policy Name]*.
3. Right-click on the policy and select *Export Policy*.
4. Browse to select the location.
5. Specify a file name and click *Save*. The policy is exported in XML format.

Scanning via Faronics Core Console

Scanning can be done manually, as scheduled in the Anti-Virus Policy or by scheduling a task via Faronics Core Console. Complete the following steps to manually scan workstation(s) via Faronics Core Console:

1. Launch Faronics Core Console.
2. Go to *Workstation List* pane.
3. Right-click on one or more workstations.
   - > Select *Scan*>*Quick* for a quick scan.
   - > Select *Scan*>*Deep* for a deep scan.
   - > Select *Fix Now* to download the latest virus definitions and perform a scan. If Active Protection was temporarily disabled by the user, it is enabled when *Fix Now* is selected.

The scan progress (*% Scan Complete*) is displayed in the *Workstation List* pane in Faronics Core Console.

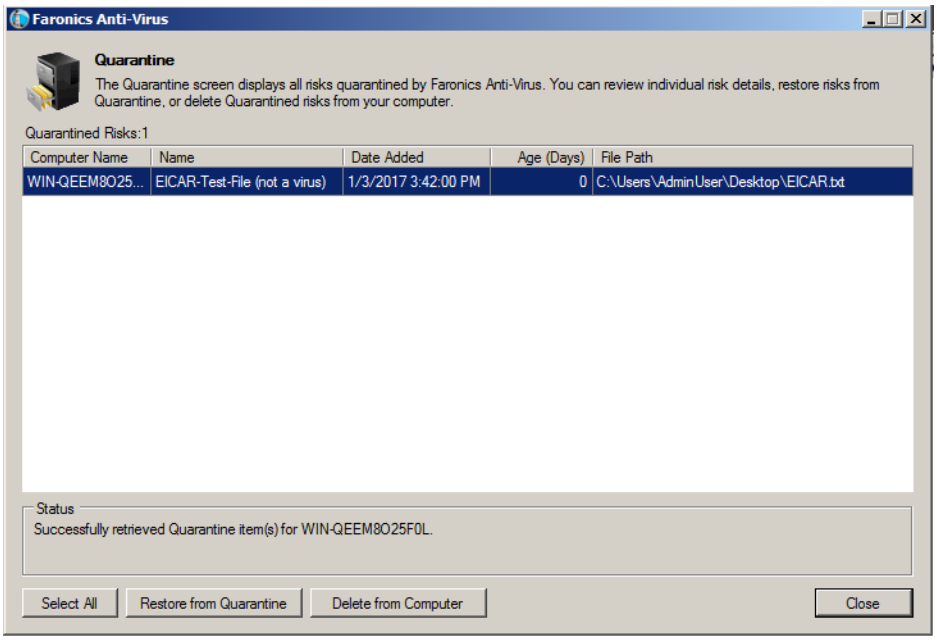
If there is more than one Loadin installed, the right-click contextual menu for Faronics Anti-Virus can be accessed by right-clicking a workstation, selecting *Faronics Anti-Virus* and then selecting the particular action.

Active Protection must be enabled for the *Fix Now* feature to work via Faronics Core Console.

Viewing and Taking Action on Quarantined Files

Complete the following steps to view the files quarantined by Faronics Anti-Virus:

1. Launch Faronics Core Console.
2. Go to *Workstation List* pane.
3. Select the workstation.
4. Right-click on the workstation and select *View Quarantine*. The list of quarantined files is displayed.



5. The following information about each infected file is displayed:
   - Risk Name
   - File Name
   - Original Location
   - Date Added
   - Age (Days)
6. Select the following actions:
   - Select All – selects all the files.
   - Delete from Computer – deletes the selected file from the computer.
   - Restore from Quarantine – restores the selected file from the computer.
   - Close – closes the dialog.

Updating Faronics Anti-Virus via Faronics Core Console

Faronics Anti-Virus definitions can be updated on the workstation(s) via Faronics Core Console. Faronics Core acts as the Anti-Virus update repository for the managed workstations. The Anti-Virus updates are automatically sent to remote workstations by Faronics Core. Additionally, the Faronics Core Administrator can manually update virus definitions as described below.

Complete the following steps to update Faronics Anti-Virus on the workstation(s):

1. Launch Faronics Core Console.
2. Go to *Workstation List* pane.
3. Right-click on one or more workstations and select *Update*.
   > Select *Update*>*Full Update* – this updates the Anti-Virus definitions.
   > Select *Update*>*Full Force Update* – this deletes the existing Anti-Virus definitions and updates the latest Anti-Virus definitions.

Schedule Action for Faronics Anti-Virus via Faronics Core Console

Faronics Anti-Virus and Faronics Core Console events can be scheduled to occur on one or more workstations at a date and time convenient to the administrator. Click on one or more workstations and select *Schedule Action*. The sub-menus which appear contain the following list of available actions:

Actions controlled by Faronics Core Console:

- Shutdown
- Restart
- Wake up

Actions controlled by Faronics Anti-Virus:

- Active Protection>Enable
- Active Protection>Disable
- Scan>Quick
- Scan>Deep
- Update>Full Update
- Update>Force Full Update
- Fix Now
- Install/Upgrade Anti-Virus Client
- Uninstall Anti-Virus Client

Selecting an action displays a *Schedule* menu that allows the administrator to specify the frequency (one-time, daily, weekly or monthly). Based on the frequency, you can select the specific time, day, date, or month.

The Scheduled Task set via an Anti-Virus Policy always takes precedence over a Scheduled Action set via Faronics Core Console.

Generating Reports

Faronics Anti-Virus provides many reports to monitor the activity on each workstation. There are two categories of reports:

- Global Reports – these reports are based on all workstations protected by Faronics Anti-Virus.
- Workstation-specific Reports – these reports are specific to the selected workstation.

Global Reports

Complete the following steps to generate a Global Report:

1. Launch Faronics Core Console.
2. In the *Console Tree* pane, go to *Faronics Core Console>[Core Server]>Managed Workstations>Anti-Virus*.
3. In the *Action* pane, click *Global Reports*.
4. Select the report and enter a date range in the displayed dialog. Click *OK*. The following reports are available:
   - > Threats by number of detections – the threats detected by the number of detections in all workstations managed by Faronics Anti-Virus is displayed.
   - > Threat Severity Summary – the threat severity summary is displayed.
   - > Top 25 Infected Machines – the top 25 infected computers are displayed.

The selected report is displayed in the *Console Tree* pane>*Reports* node.

Workstation-specific Reports

Complete the following steps to generate a Workstation-specific Report:

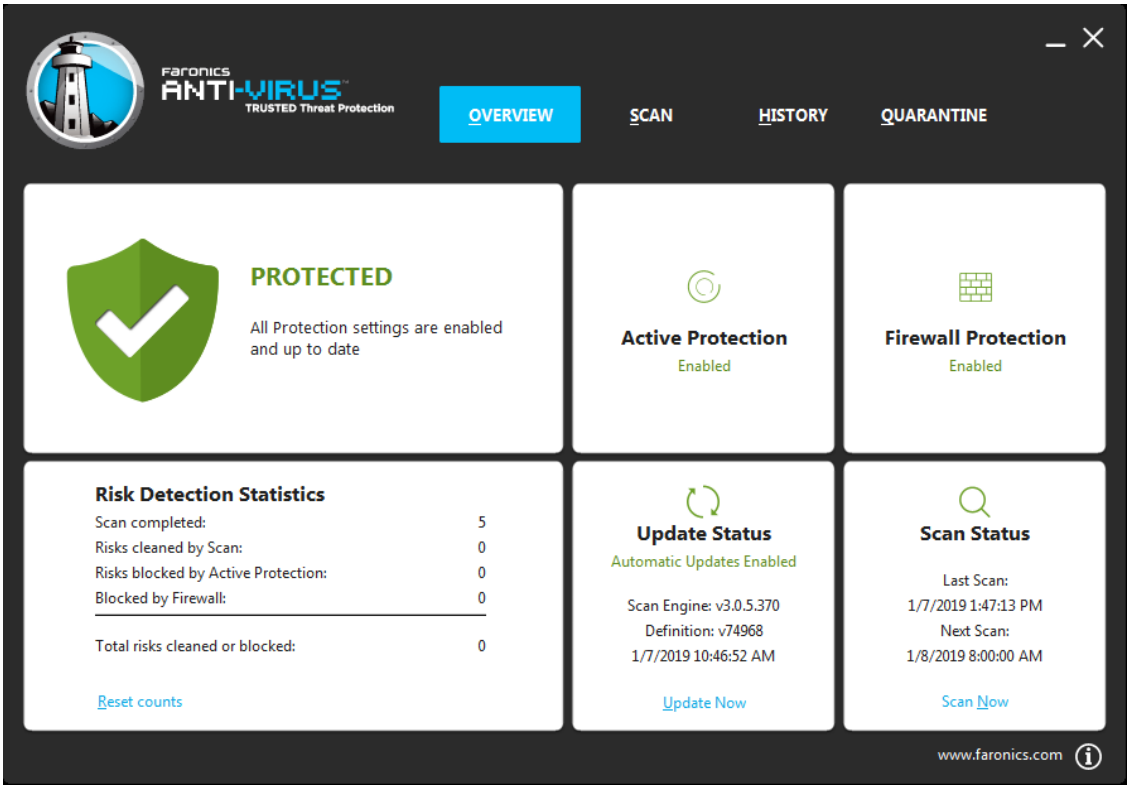
1. Launch Faronics Core Console.
2. In the *Console Tree* pane, go to *Faronics Core Console>[Core Server]>Managed Workstations*.
3. Select the workstation for which the report is to be generated.
4. Right-click on the workstation and select *Generate Report>Anti-Virus>[Report Name]*.
5. Enter a date range in the displayed dialog. Click *OK*. The following reports are available:
   - > Workstation Details
   - > Last Scan
   - > Scan History
   - > Active Protection History
   - > Quarantine
   - > Firewall Daily Network Activity
6. The selected report is displayed in the *Console Tree* pane>*Reports* node.

Using Faronics Anti-Virus on the Workstation

The features available in Faronics Anti-Virus on the workstation fully depends on the settings selected in the Anti-Virus Policy. For more information about Anti-Virus Policy, refer to Faronics Anti-Virus Policy.

Launching Faronics Anti-Virus on the Workstation

Go to *Start>Programs>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternatively, you can double-click on the Faronics Anti-Virus icon in the System Tray.



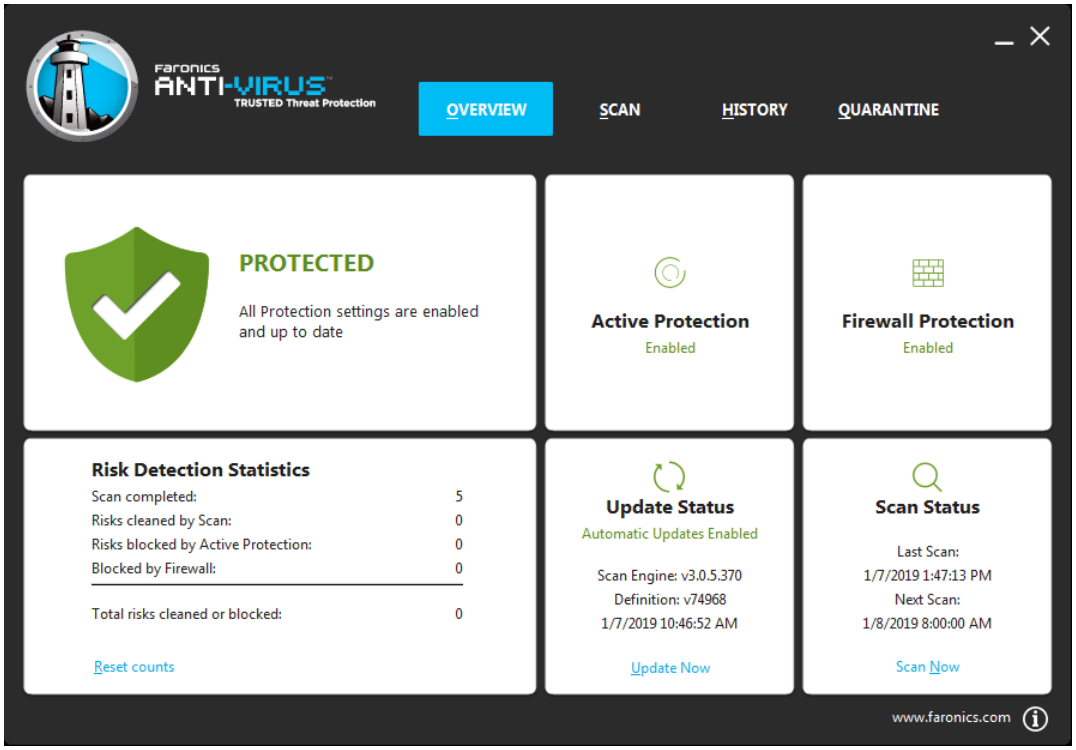
The following panes display important information to the user:

- *Protected* or *Not Protected is* displayed notifying if the computer is protected or not. If Not Protected is displayed, click the *Fix Now* button below the *Not Protected* sign.
- *Scan Status* displays when the last scan was performed. To scan now, click the *Scan Now* link.
- *Update Status* displays when the last update was performed. To update virus definitions, click the *Update All Now* link.
- *Active Protection* displays if real-time protection is enabled.
- *Firewall Protection* displays if the workstation is protected by the Firewall.
- *Risk Detection Statistics* displays the statistics for the actions taken by Faronics Anti-Virus. Click *Reset counts* to reset the counts to zero.

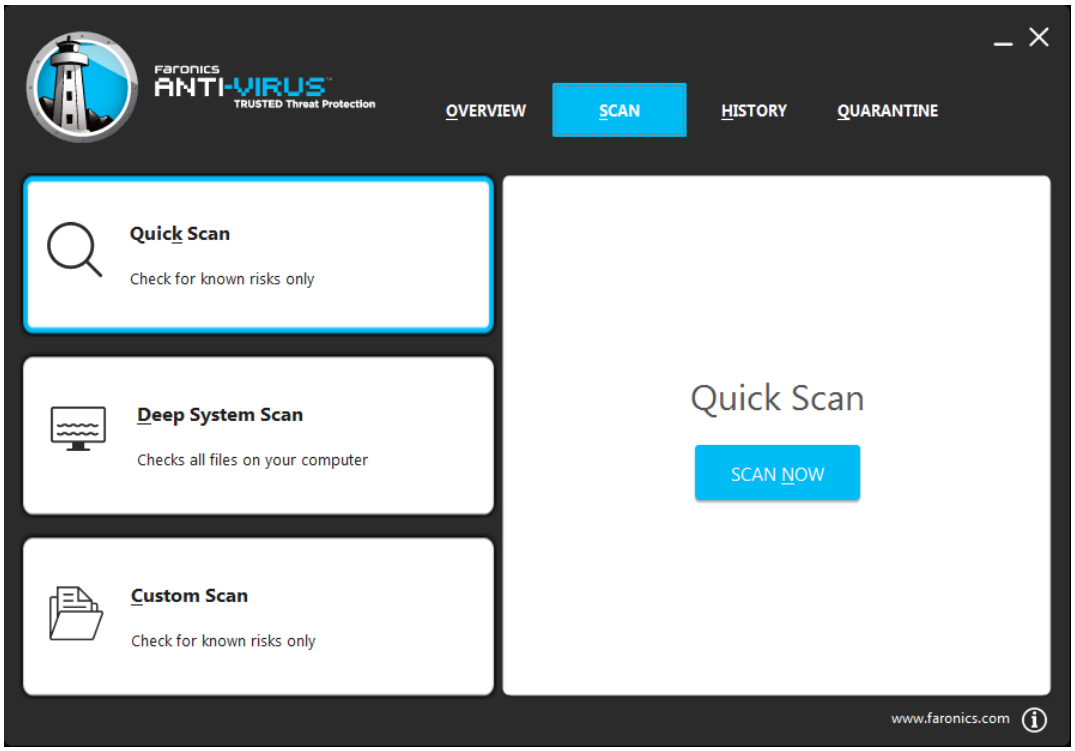
Scanning the Workstation

Complete the following steps to scan a workstation:

1. Go to *Start>Programs>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.



2. In the *Scan Status* pane, click *Scan Now*. The *Scan* tab is displayed. Alternatively, you may also click the *Scan* tab.



3. Select one of the following options:
   - > Quick Scan- scans only known threats.
   - > Deep System Scan- a detailed scan of all files on the workstation.
   - > Custom Scan (select one of the following):
     - ~ Scan Running Processes – scans the process running on the workstation.
     - ~ Scan Registry – scans the registry.
     - ~ Specify drives *and folders to scan*: Click *Browse* and select the folders.
4. Click *Scan Now*. The spinning icon indicates that a scan is in progress. The scan results are displayed after the scan is completed.
5. Select the file and the following options are available:
   - > Select *Change Clean Action*>*Recommended Action* to take the action as recommended by Faronics Anti-Virus.
   - > Select *Change Clean Action*>*Quarantine/Disinfect* to quarantine or disinfect the file.
   - > Select *Change Clean Action*>*Delete* to delete the file.
   - > Select *Change Clean Action*>*Allow* to allow the file.
   - > Click *Select All* to select all the files displayed in the *Scan Result*.
   - > Click *Details* to display details of the risk.
   - > Click *Cancel* to close the dialog without taking action.
   - > Click *Clean* to remove the file and close the dialog.

Action can also be taken via Faronics Core Console. For more information refer to Viewing and Taking Action on Quarantined Files.

Scanning a File or a Folder via Right-Click

Files or folders (single or multiple) can be easily scanned for a virus. When Faronics Anti-Virus is installed on a workstation, the Scan for Virus option is added in the right-click menu.

Complete the following steps to scan a file or a folder on the computer:

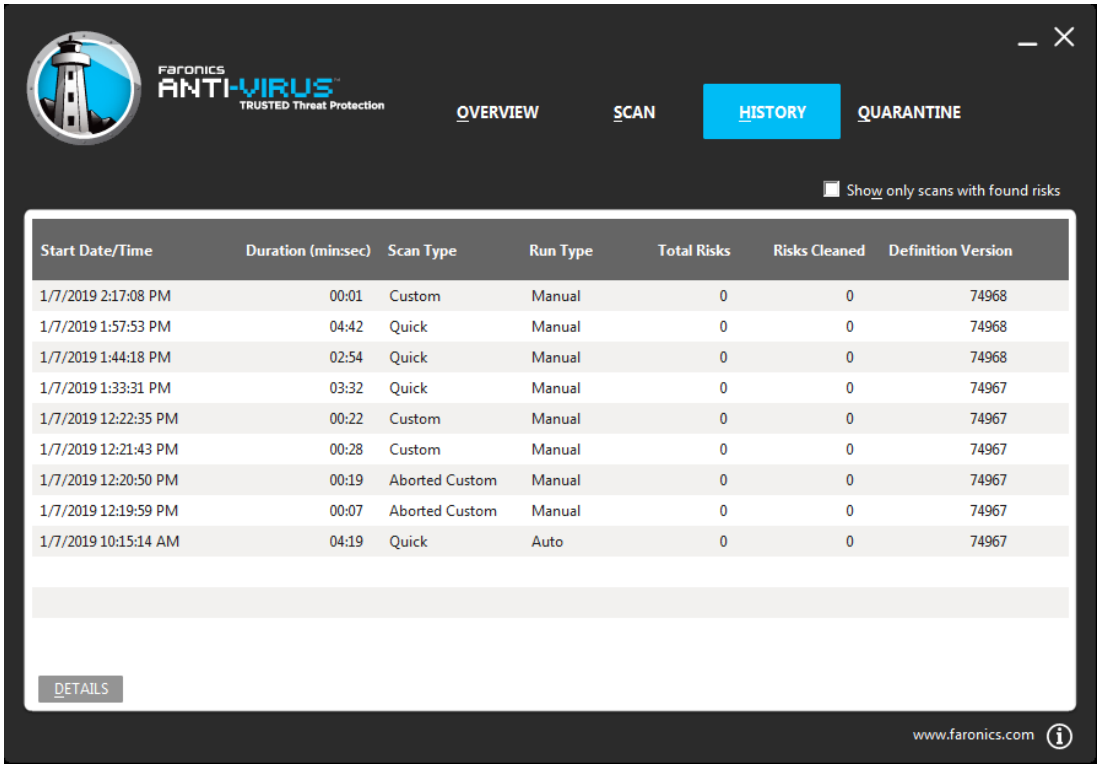
1. Right-click on the file or folder.
2. Select *Scan for viruses*.

The scan is performed and the results are displayed.

View Scanning History

Complete the following steps to view the scanning history:

1. Go to *Start>Programs>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.
2. Click the *History* tab.

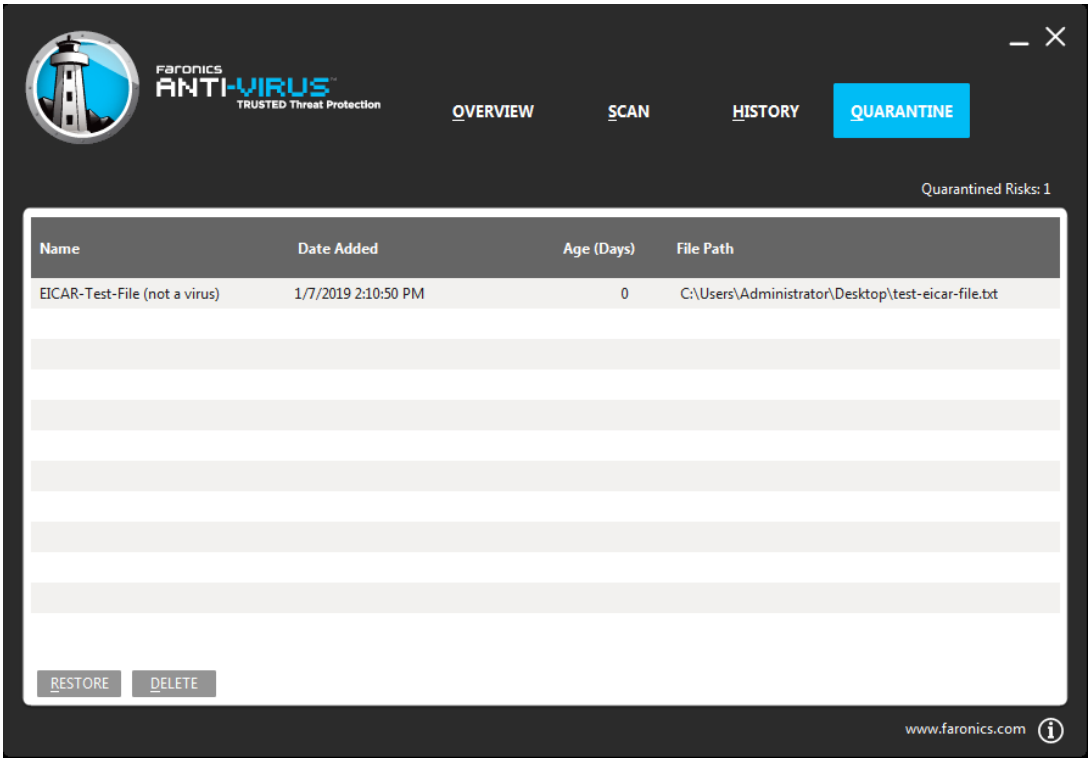


3. Select the following actions:
   - > Show only scans with found risks – select this option to view only the scans where risks were found.
   - > Details – select an entry and click details to view the details of the scan.

View and take action on Quarantined Files

Complete the following steps to view Quarantine:

1. Go to *Start>Programs>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.
2. Click the *Quarantine* tab.

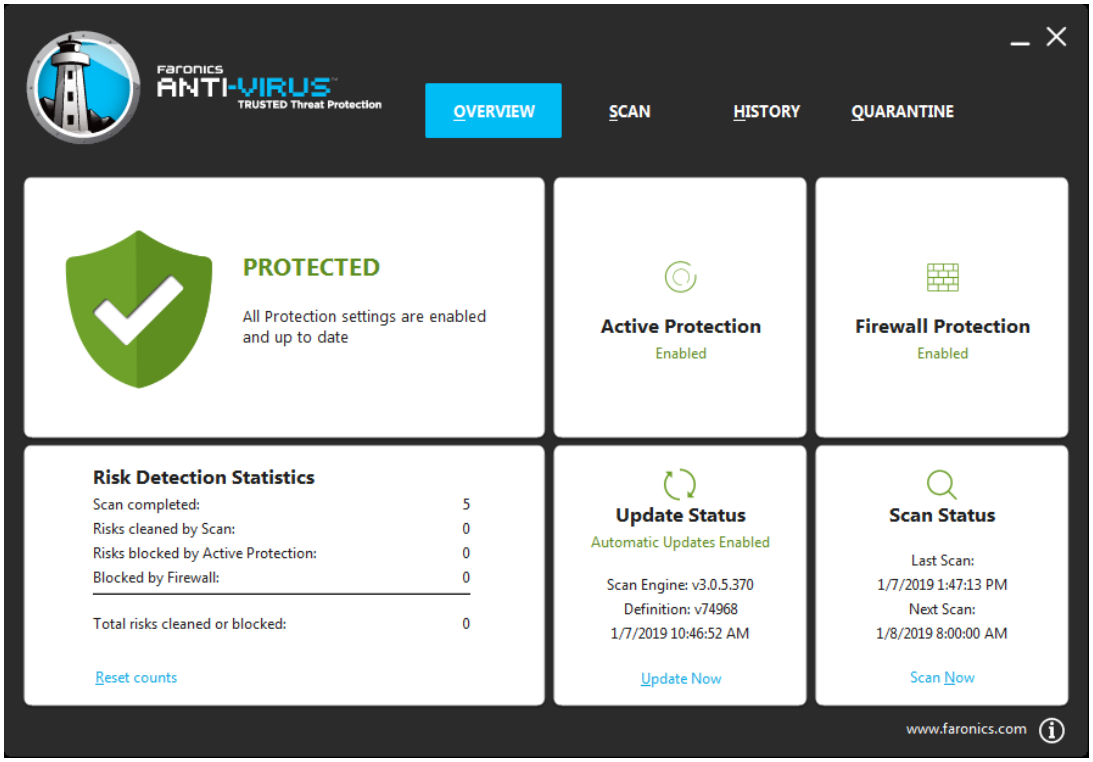


3. Click *Risk Details*. The following information about each infected file is displayed:
   - > Name
   - > Risk Category
   - > Date Added
   - > Age (Days)
   - > Quarantined By

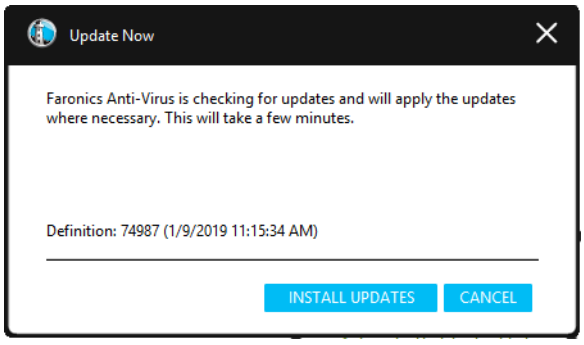
Updating Anti-Virus Definitions on the Workstation

Complete the following steps to update Anti-Virus definitions on a workstation:

1. Go to *Start>Programs>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternatively, you can double-click on the Faronics Anti-Virus icon in the System Tray.



2. In the *Update Status* pane, click *Update Now*. The *Update Now* dialog is displayed.



3. Click *Install Updates*. The virus definitions are updated on the workstation.

Managing Faronics Anti-Virus on the Workstation via the System Tray

Faronics Anti-Virus can be managed on the workstation via a menu available from the System Tray.

Right-click on the Faronics Anti-Virus icon in the System Tray. The following options are available:

- Open Faronics Anti-Virus – launches Faronics Anti-Virus on the workstation.
- Active Protection
  - > *Active Protection>Enable Active Protection* – enables Active Protection.
  - > *Active Protection>Disable Active Protection>[Select the option]* – select the duration for which Active Protection is to be disabled. Select 5 minutes, 15 minutes, 30 minutes, 1 Hour, Until Computer Restart or Permanently. This option is displayed only if it has been selected in the Anti-Virus policy.
- *Scan Now>[Select the option]* – select Cancel Scan, Pause Scan, Resume Scan, Quick Scan or Deep Scan. This option is displayed only if it has been selected in the Anti-Virus policy.
- *Firewall Protection>Enable* or *Disable*

The above options are available to the user only if it was specified in the Anti-Virus policy. For more information, refer to Creating Anti-Virus Policies.

Command Line Control

This chapter explains the various Command Line Controls available for Faronics Anti-Virus.

Topics

Command Line Control

Faronics Anti-Virus Command Line Control offers network administrators increased flexibility in managing Faronics Anti-Virus workstations by allowing for control via third-party management tools and/or central management solutions.

Complete the following steps to run the commands for Faronics Anti-Virus:

1. On the workstation, go to <*System Directory*>:*Program Files**Faronics**Faronics Anti-Virus Enterprise* via command prompt.
2. Enter `AVECLI/[Command]`

The following commands are available:

Command	Definition
`definitionversion`	Displays Virus Definition version.
`scanengineversion`	Displays Scan Engine version.
`updatedefs`	Updates and apply Virus Definitions.
`fixnow`	Downloads the latest Virus Definition. Enables Active Protection and Email Protection. Performs the default Deep Scan.
`scanquick`	Starts a QUICK scan.
`scandeep`	Starts a DEEP Scan.
`enableap`	Enables Active Protection.
`fixnow /quick`	Performs a *Quick Scan* if applicable.
`setlicense[key]`	Applies a given license key.

Syntax:

```
AVECLI/definitionversion
```

Uninstalling Faronics Anti-Virus

This chapter describes how to uninstall Faronics Anti-Virus.

Topics

Uninstallation Overview

The Faronics Anti-Virus Loadin is installed on the Faronics Core Console (or Faronics Core Server) system. The Faronics Anti-Virus Client is installed on workstations.

Uninstall Faronics Anti-Virus Client on the workstation manually or via Faronics Core Console. Once this is done, uninstall the Faronics Anti-Virus Loadin on the Faronics Core Console (or Faronics Core Server) system.

The uninstallation procedure is explained in the next sections.

Uninstalling Faronics Ant-Virus Client via Faronics Core Console

Complete the following steps to uninstall Faronics Anti-Virus Client via Faronics Core Console:

1. Launch Faronics Core Console.
2. In the *Console Tree Pane*, go to *Faronics Core Console>[Core Server]>Managed Workstations*.
3. Select the workstation(s) to uninstall Faronics Anti-Virus Client.
4. Right-click and select *Configure Workstations>Advanced>Uninstall Anti-Virus Client*.

Faronics Anti-Virus Client is uninstalled from the workstation(s).

Uninstalling Faronics Anti-Virus Client on the Workstation via Add or Remove Programs

Complete the following steps to uninstall Faronics Anti-Virus via *Add or Remove Programs* in Windows:

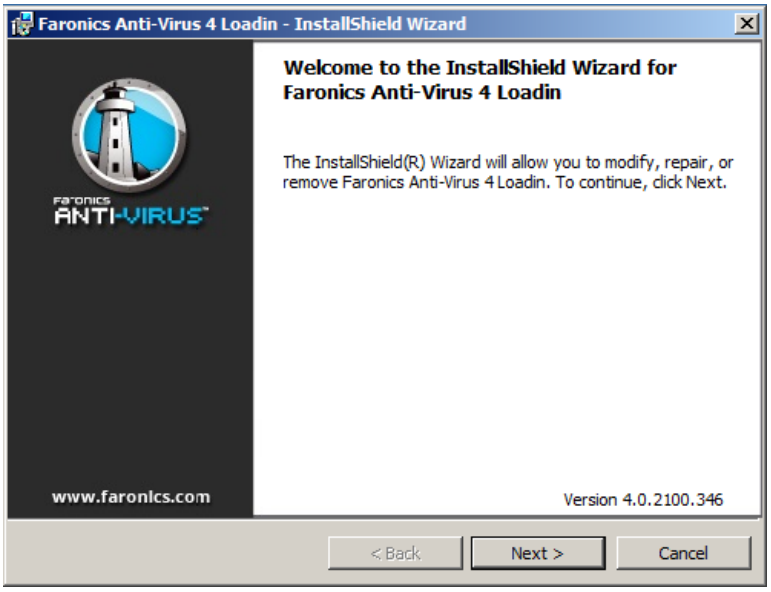
1. Click *Start>Control Panel>Add or Remove Programs*.
2. Select *Faronics Anti-Virus Enterprise Workstation*.
3. Click *Remove*.

Faronics Anti-Virus Client is uninstalled from the workstation.

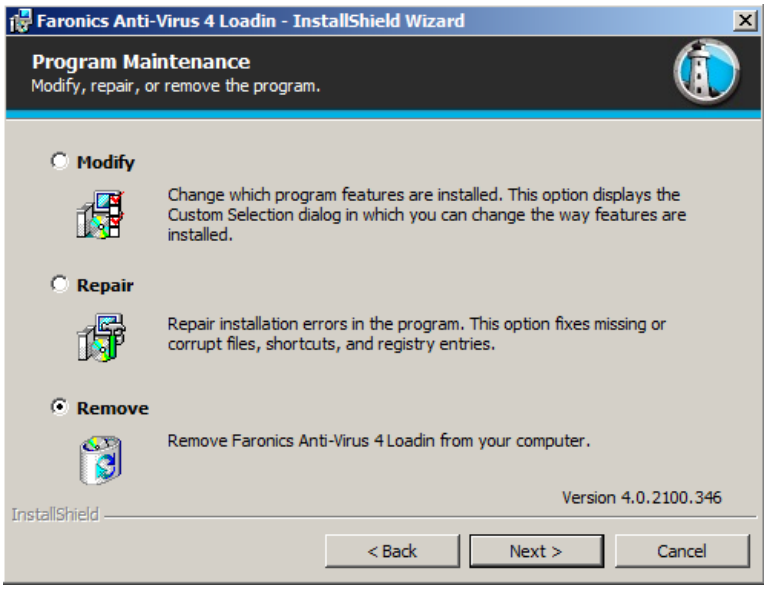
Uninstalling Faronics Anti-Virus Loadin with the Installer

Complete the following steps to uninstall Faronics Anti-Virus Loadin:

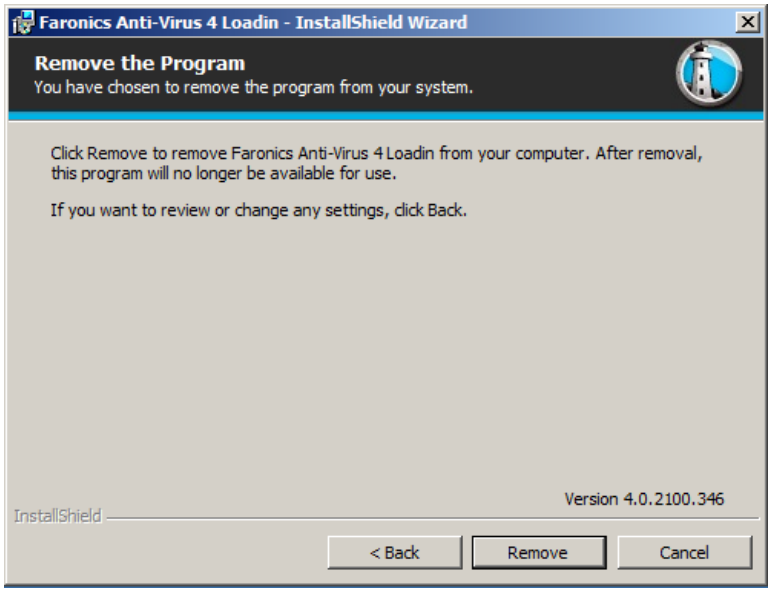
1. Double-click *Anti-VirusLoadinInstaller.exe*. Click *Next*.



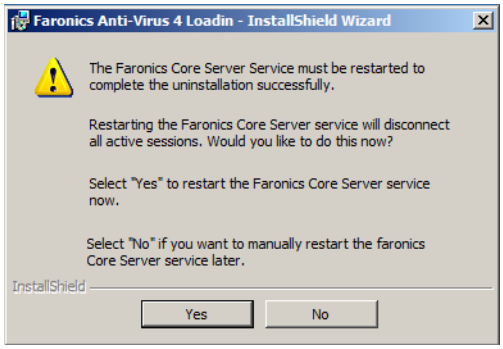
2. Select *Remove*. Click *Next*.



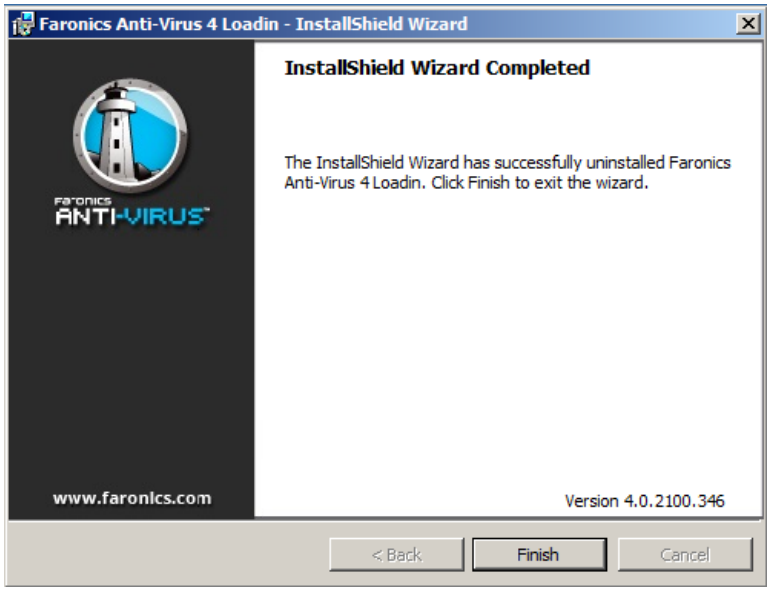
3. Click *Remove*.



4. The following message is displayed. Click *Yes* to restart *Faronics Core Server* service or *No* to manually restart the *Faronics Core Server* service later.



5. The Faronics Anti-Virus Loadin is removed from your computer. Click *Finish* to complete uninstallation.



Uninstalling Faronics Anti-Virus Loadin via Add or Remove Programs

Complete the following steps to uninstall Faronics Anti-Virus Loadin via *Add or Remove Programs* in Windows:

1. Click *Start*>*Control Panel*>*Add or Remove Programs*.
2. Select *Faronics Anti-Virus Loadin*.
3. Click *Remove*.