

FRISK Software

F-PROT Antivirus for Windows
Corporate Edition

Setup Guide

US-WINC-0704-05

Table of Contents

Introduction	3
Updating the virus signature file and settings	4
To update the virus signature file for the LAN Update package	4
To update the settings files for the LAN Update package	4
Upgrading the software.....	5
Creating a script to automate the copying of files	5
Password Protection	7
Security and Access	8
Technical Support	8

Introduction

Version 6 of F-PROT Antivirus for Windows Corporate is a new, significantly enhanced version that incorporates many changes and improvements, including new user interface, enhanced features such as automatic e-mail protection, automatic ActiveX protection, a quarantine, exclusion lists, backup files, improved automatic file system protection and automated virus signature file updates and software upgrades. In addition to these very significant improvements, version 6 of F-PROT Antivirus for Windows Corporate has maintained its competitive advantage as a reliable and easy-to-use antivirus product that consumes an absolute minimum of system resources.

F-PROT Antivirus for Windows Corporate updates through the local network, Internet and a proxy server. Version 6 of F-PROT Antivirus for Windows Corporate is comprised of two packages:

- LAN Update
- Internet Update

The LAN Update package of F-PROT Antivirus for Windows Corporate differs from the Internet Update package of F-PROT Antivirus for Windows Corporate mainly in two ways.

- First, the LAN Update package offers automatic virus signature file and settings updates on the local network. The Internet Update package offers automatic virus signature file updates and software upgrades from online FRISK Software download servers.
- Second, the LAN Update package does not need a Subscription Key as it only updates over the local network. The Internet Update package updates via the Internet and the proxy server and therefore requires a Subscription Key (displayed in Customer Zone).

It is recommended to only use the Internet Update package for Small Office/Home Office (SOHO) networks. For medium and large domain based networks, the recommended setup is installing the LAN Update package in combination with the Internet Update package. Please note that both the Internet Update package and LAN Update package cannot be installed on the same computer.

Updating the virus signature file and settings

The LAN Update package will be installed on all client workstations and then there has to be at least one computer (server) on the network with F-PROT Antivirus for Windows, Internet Update package, installed (see Image 1).

On the client workstations, specify the shared update location. This can be done either during or after the installation. If this is done after the installation, do one of the following:

- From the application. Run the program. Click **Updates** and then click **Settings**.
- From the registry. Edit the registry key "HKLM\SOFTWARE\FRISK Software\F-PROT Antivirus for Windows\LAN Updates".

Make sure that the F-PROT Antivirus service on the client machine (running in system account) has access to the shared update location (see [Security and Access](#)).

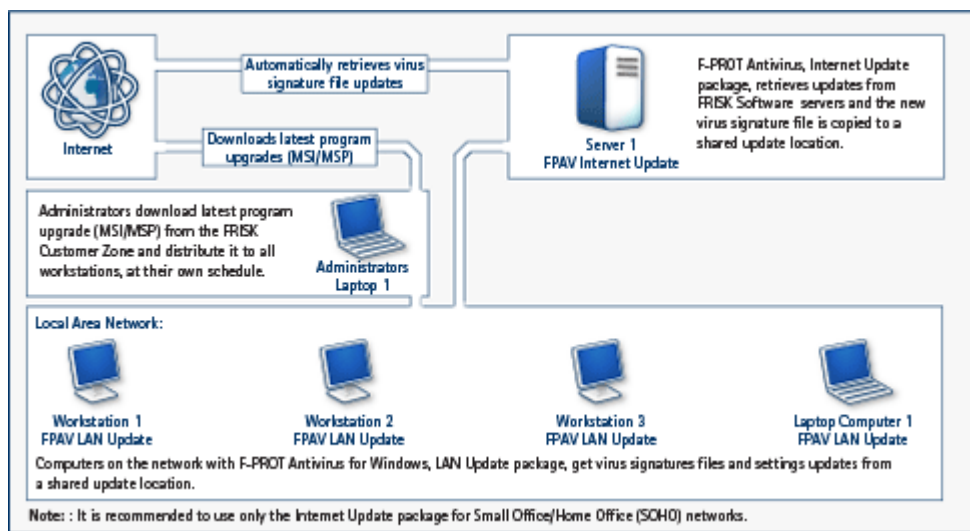


Image 1: F-PROT Antivirus for Windows Corporate: Software Upgrades and Virus Signature File and Settings Updates

To update the virus signature file for the LAN Update package

An administrator must copy the latest virus signature file (antivir.def) from the Internet Update package to the shared update location from where the client computers can update their local copies.

To update the settings files for the LAN Update package

If program settings for all client computers must be suitable for the network environment, the administrator may set his/her local copy of F-PROT Antivirus with the desired settings and then copy the settings files to the shared update location. The files for settings are the following:

- config.xml (program settings)
- tasks.xml (advanced scans)
- exclusions.xml

Both the settings files and antivir.def are located at:

- <CommonApplicationData>\FRISK Software\F-PROT Antivirus for Windows\

Where, CommonApplicationData, returns a path of "C:\Documents and Settings\All Users\Application Data". Please note the path can be slightly different with other language versions of Windows. See examples below:

English version:

C:\Documents and Settings\All Users\Application Data\FRISK Software\F-PROT Antivirus for Windows\

German version:

C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\FRISK Software\F-PROT Antivirus for Windows\

A script can be created to automate the copying of the virus signature file (antivir.def) and settings files to the update location and then schedule it to run regularly, e.g. hourly (see [Creating a script to automate the copying of files](#)).

Upgrading the software

The Internet Update package automatically upgrades the software without user interaction. You will be notified when you need to restart the computer to apply the latest updates. However, program upgrades for the LAN Update package must be downloaded from Customer Zone and distributed manually on the network.

Creating a script to automate the copying of files

You may create a script to automate the copying of virus signature file (antivir.def) and settings files (config.xml, tasks.xml, exclusion.xml) to the update location and then schedule it to run regularly, e.g. hourly.

To automate the copy of antivir.def and settings files to a shared update location:

The user can choose between two options:

- Change the line

```
set DEFAULT_DEST_PATH=\\server\fpav-update
```

to include the correct destination path

- Pass the destination path as the first command line parameter. If no such parameter is given, the default value from the 1st option is used.

The Script

```
@echo off
@if "%OS%"=="Windows_NT" goto :MAIN
@echo This script requires Windows 2000 or later to run properly!
goto :EOF
```

.....

```

:: Script to copy files from an existing installation of FPAV to a
:: network share or arbitrary other directory.
::
:: Usage:
:: Change the variable DEFAULT_DEST_PATH to your destination path
:: (directory) and the script should take care of the rest.
::
:: Alternatively give the destination path at the first parameter.
:::
:::
::: / MAIN subroutine
::: Receives the command line parameters
:::
:MAIN
setlocal ENABLEEXTENSIONS
set DEFAULT_DEST_PATH=\\server\fpav-update
if not "%1" == "" set DEST_PATH=%1
if not DEFINED DEST_PATH set DEST_PATH=%DEFAULT_DEST_PATH%
set DEST_PATH=%DEST_PATH:="=%
set SRC_PATH_SUFFIX=FRISK Software\F-PROT Antivirus for Windows
set FILES_TO_COPY=antivir.def config.xml tasks.xml exclusions.xml
set SRC_PATH=%APPDATA%
call :GetFilePart SRC_PATH
set SRC_PATH=%ALLUSERSPROFILE%\%SRC_PATH%\%SRC_PATH_SUFFIX%
for /D %i in (%FILES_TO_COPY%) do @(
    if exist "%SRC_PATH%\%i" @(
        echo Copying %i
        xcopy /Y /K /D "%SRC_PATH%\%i" "%DEST_PATH%"
    ) else (
        echo "%SRC_PATH%\%i" does not exist!
    )
)
)
endlocal
goto :EOF

:::
::: / GetFilePart subroutine
::: There is only one parameter, the name of the variable which
::: contains the full path and receives the last part after the last
::: backslash. The function extracts the part after the last backslash.
:::
:GetFilePart
setlocal ENABLEEXTENSIONS & set VAR_NAME=%1
set VAR_TEMPRET2=%VAR_NAME%
:GetFilePartLoop
set VAR_TEMPRET1=%VAR_TEMPRET2%
set VAR_TEMPRET2=%VAR_TEMPRET1%
for /f "tokens=1,* delims=\" %i in ('echo %VAR_TEMPRET1%') do (
    if not "%j" == "" set VAR_TEMPRET2=%j
)
if not "%VAR_TEMPRET1%" == "%VAR_TEMPRET2%" goto :GetFilePartLoop
endlocal & set %VAR_NAME%=%VAR_TEMPRET1%
goto :EOF

```

End of Script

For further explanation of the script above, please visit: <http://forum.f-prot.com/index.php?topic=243.0>

Please note that any combination of these files (antivir.def, config.xml tasks.xml exclusions.xml) can be copied to the shared update location and none of them are required, F-PROT Antivirus will update all that is available and more recent than what it has.

Password Protection

F-PROT Antivirus offers password protection that enables you to create a password in the program to protect your settings from being modified by unauthorized users.

To update the password protected settings in the LAN Update package

To update password protected settings on the client machines an additional file is needed in the shared update location: password.xml. The file contains the password(s) needed, encrypted, and is generated using a password tool that comes with the LAN Update package. During updates, F-PROT Antivirus will read the password in the file "password.xml" and supply it when, and if, prompted (internally).

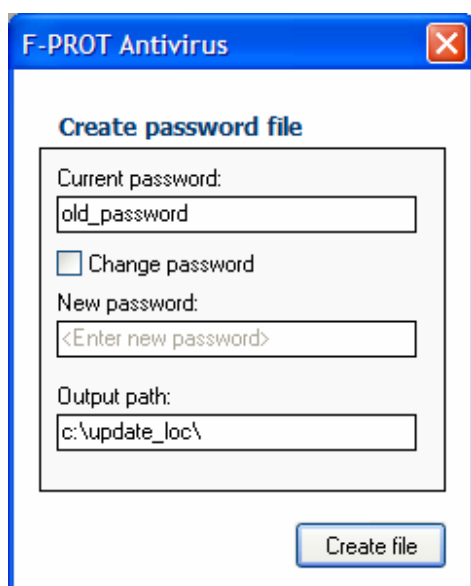


Image 2: Password protected settings. Here, it shows how the file c:\update_loc\password.xml is created for clients that have settings protected with the password "old_password".

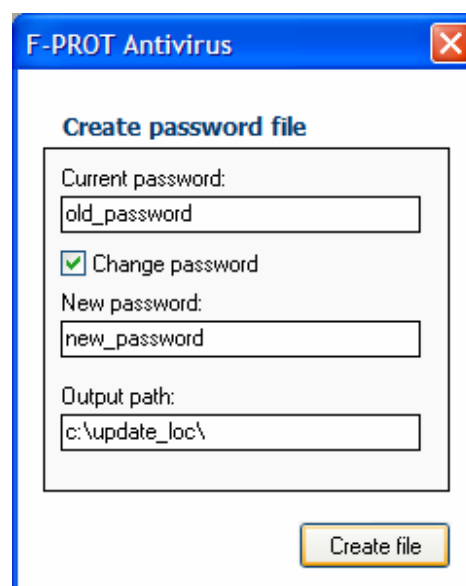


Image 3: Change a password. Here, it shows the password is being changed from "old_password" to "new_password". When the new password has been applied to the client computers, password.xml has to be re-generated with "new_password" as the current password.

Security and Access

F-PROT Antivirus for Windows uses the SYSTEM account on the local computer to access the resources and objects it needs. The system account is a predefined local account that has full access to the computer. It acts as the host computer account on the network and has access to network resources just like any other domain account. On a domain network, this account appears as <DOMAIN NAME>\<machine name>\$ and is included in the Everyone group.

To be able to update from the shared updated location on the network, each host computer account (the system accounts) must be granted read access to the share and the folder. On a domain network, this can be accomplished by giving Read access to the Everyone group. On a non-domain network this might have to be accomplished by allowing anonymous read access (null sessions) to the share and the folder. Below are a few examples on how to do this.

Client and server are on a domain

- Give "Everyone" read access to the folder **and** the share.

Client in a workgroup

- Windows XP/Windows Server 2003:
 - Give "Anonymous login" read access on the folder **and** the share or give "Everyone" read access and enable the local computer policy "Network Access: Let Everyone permission apply to anonymous users" on the server.
 - Add the share name (not the path) to the list "Network Access: Shares that can be accessed anonymously" in local computer policy on the server.
- Windows 2000:
 - Add the share name (not the path) to the NullSessionShares list in registry "HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares"

UNIX with Samba

- Set "public = yes" on the share in smb.conf

Note that it is not needed nor recommended to give write access to the folder or the share, only read access.

Technical Support

If you need assistance please [contact technical support](#).