

NetUp32 – documentation

<i>NetUp32 – documentation</i>	1
Information about NetUp32 version 7.1.0.299	2
The NetUp32 packaged	2
NetUp32 installation / implementation	2
NetUp32 directory structure	3
NetUp32 will monitor McAfee VirusScan	3
Monitor installation process	3
Monitor DAT update process	3
Monitor VirusScan services	4
VirusScan installation	4
Update DAT, engine, configuration, Extra.dat ex.	4
Update Extra.dat the NetUp32 way	5
AutoUpdate management	5
VirusScan configuration	5
Use central Alert manager	6
Password protect VirusScan configuration	7
Automatic update (every hour or whenever you want)	7
Configuration by McAfee Install Designer - MID	7
Support for Windows 9x and VirusScan 4.5.1	8
Log information	8

Information about NetUp32 version 7.1.0.299

This document is going to give a short introduction of the NetUp32 concept. NetUp32 is build on best practices and has been expanded over several years. This document should give you information about how NetUp32 can be implemented, purpose for each component, how NetUp32 works ex.

This document is not complete yet. There will be added more information in the near future.

Documentation for the NetUp32.ini: <http://mcafee.dk/manuals/eterra/netup32/>

The NetUp32 packaged

Short description of the different products included in the NetUp32 packaged.

http://mcafee.dk/products/E-Produktblad_Ementor_McAfee_Management_Vers_1.5.pdf

NetUp32

Distribution, installation and maintenance of McAfee VirusScan Enterprise on all the workstation and server.

Product description: <http://www.mcafee.dk/products/product.php3?prodid=netup32>

FTPUpdate

Download updated for VirusScan – DAT, extra.dat and engines. Notify when updates has been downloaded.

Product description: <http://www.mcafee.dk/products/product.php3?prodid=ftpupdate>

Remote Update

Monitor and maintain all the McAfee products from a single console.

Product description: <http://www.mcafee.dk/products/product.php3?prodid=remoteupdate>

Log Viewer

Easy access to the log files and detailed report about virus alerts.

Product description: <http://www.mcafee.dk/products/product.php3?prodid=netup32>

Log Monitor

Automatically monitor the log files and alert on problems.

Product description: <http://www.mcafee.dk/products/product.php3?prodid=netup32>

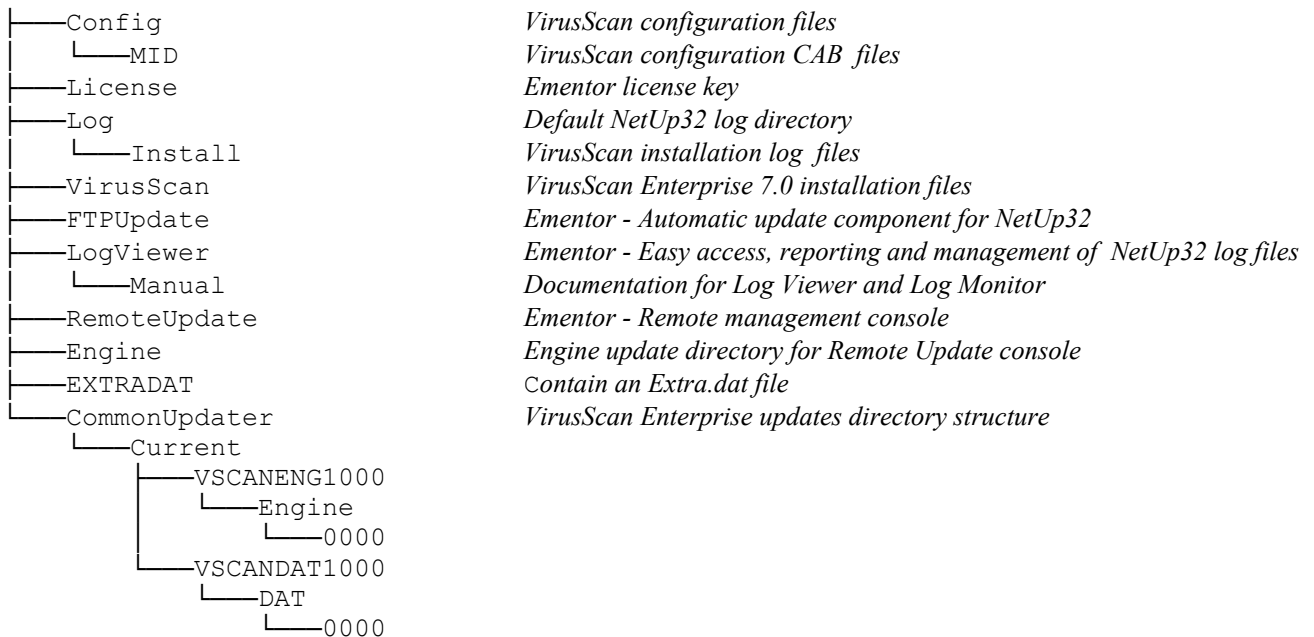
NetUp32 installation / implementation

It is possible to implement NetUp32 a number of ways. The most common one is very simple.

1. Copy the NetUp32 directory structure (all the files and directory) to a server share.
2. Activate Netup32.exe on all the workstation and servers to get VirusScan Enterprise installed and updated. Normally the workstation activate NetUp32 through the login script and the servers activate NetUp32 as a scheduled task. Remember to test NetUp32 on some workstations and servers before activation it on every system and remember to set bDebug=0 in NetUp32.ini to remove the debug screen.
3. Activate FTPUpdate on the “master” server to download updated. The “master” server is the server where the NetUp32 files is located. Create a schedules job for FTPUpdate and schedule the job to run at least once a day. We recommend checking for updates in the period from 2:00 to 7:00 in the morning. Don’t use 2:00, 3:00 Instead use 2:37 or 3:12 because the can be much traffic to the server every hour on the hour.

NetUp32 directory structure

The directory structure is a bit different compared to the previous NetUp32 (4.5.1). Here is a short overview.



NetUp32 will monitor McAfee VirusScan

NetUp32 has got several functions for checking that VirusScan is installed, updated and active.

Monitor installation process

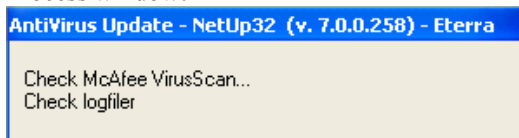
NetUp32 will check the local installation log file C:\VSCAN.TXT if it exists. The log file should include the word "INSTALL. Return value 1". An error "INSTALL ERROR" is written to the NetUp32 INSTALL log if the word "INSTALL. Return value 1" is not found in the log file. C:\VSCAN.TXT will be appended to the \Log\INSTALL_ERROR.TXT file with a header and footer so it can be investigated centralized why it failed.

This install log check is performed by NetUp32.ini in the [Log] section

bCheck_install_log=1

The local C:\VSCAN.TXT will be deleted after this.

Process window:



Monitor DAT update process

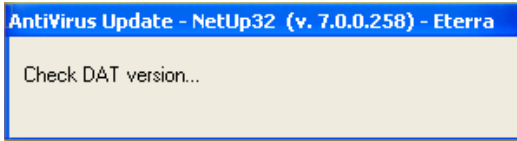
Just before NetUp32 is finish it will verify if the local DAT files is the same version as the DAT files on the server. If the version do not match NetUp32 will append the local AutoUpdate log (c:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\UpdateLog.txt) to the server \Log\ AutoUpdate.TXT with a header and footer so it can be investigated centralized why it failed.

This AutoUpdate log check is performed by NetUp32.ini in the [DAT] section

bCheck_DAT=1

The local UpdateLog.txt will be deleted after this.

Process window:



Monitor VirusScan services

It is possible for NetUp32 to verify that the correct VirusScan services are running (McShield and McTaskManager), NetUp32 will also verify that the SHSTAT process is running on the workstation. NetUp32 will try to start the services and process if they are not running. If they are not running and can not be started it will be reported in the AUDIT log and can be picked up by Log Monitor and Log Viewer which can generate an email alert.

NetUp32 service monitor is activated by netup32.ini

[Workstation] and [Server] section

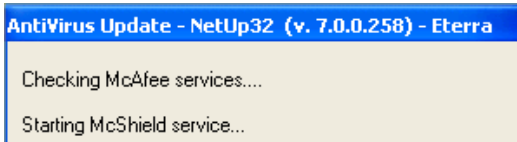
bCheck_service=1

(verify services and processes)

bStart_service=1

(try to start services and processes if they are not active)

Process window:



VirusScan installation

VirusScan will be installed from the files which is places in \VirusScan directory. The DAT files (SCAN.DAT, NAMES.DAT and CLEAN.DAT) in the \VirusScan directory will be used with the installation. This makes it possible to install VirusScan without any need to update the DAT files right after installation.

[Workstation]

bNetUp32_active=1

szRun_setup=setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS="" RUNAUTOUPDATE=""

RUNONDEMANDSCAN="" LOCKDOWNVIRUSSCANSHORTCUTS=""

VIRUSSCANICONLOCKDOWN=NORMAL REBOOT=R /li "c:\vscan.txt" /q /i

[Server]

bNetUp32_active=1

szRun_setup=setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS="" RUNAUTOUPDATE=""

RUNONDEMANDSCAN="" VIRUSSCANICONLOCKDOWN=NORMAL REBOOT=R /li "c:\vscan.txt" /q /i

Update DAT, engine, configuration, Extra.dat ex.

NetUp32 use the CommonUpdater directory structure introduced with VirusScan Enterprise 7.0 when performing updates. You can use the McAfee AutoUpdate architect to maintain the <NetUp32_dir>\CommonUpdater directory, or you can use FTPUpdate. It is very easy to use FTPUpdate. If you just activate FTPUpdate it will look for new updates on ftp.nai.com. See the documentation for FTPUpdate for more information.

NetUp32 compare the DAT version found in

<NetUp32_dir>\CommonUpdater\Current\VSCANDAT1000\DAT\0000\update.ini with the local SCAN.DAT version found in <Program Files>\Common Files\Network Associates\Engine\

Update Extra.dat the NetUp32 way

NetUp32 will compare the local extra.dat (<Program Files>\Common Files\Network Associates\Engine\) with the extra.dat placed in <NetUp32_dir>\EXTRADAT. The file from the server will be copied to the local DAT dir <Program Files>\Common Files\Network Associates\Engine\. NetUp32 will delete the local extra.dat if there is no extra.dat on the server.

AutoUpdate management

NetUp32 synchronize the file \Config\SiteList.xml. This file controls where VirusScan will look for updates. As default VirusScan will try to update from the \CommonUpdater in the NetUp32 directory. VirusScan will try the next site in the list if the first fails, and then the next if the second site fails. You can disable the sites by setting Enabled="0"

```
<?xml version="1.0" encoding="UTF-8"?>
<ns:SiteLists xmlns:ns="naSiteList" GlobalVersion="20030131003110" LocalVersion="20030314085800"
Type="Server">
  <SiteList Default="1" Name="SomeGUID">
    <UNCSite Type="repository" Name="Netup32" Order="1" Server="server" Enabled="1" Local="1">
      <ShareName>share</ShareName>
      <RelativePath>netup32</RelativePath>
      <UseLoggedonUserAccount>1</UseLoggedonUserAccount>
      <DomainName></DomainName>
      <UserName></UserName>
      <Password
Encrypted="1">f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==</Password>
      </UNCSite>
      <FTPSite Type="repository" Name="NAIFtp" Order="2" Server="ftp.nai.com:21" Enabled="1" Local="1">
        <RelativePath>CommonUpdater</RelativePath>
        <UserName>anonymous</UserName>
        <Password
Encrypted="1">MQCBNesmh4xsoov8E4KA/i9ukpwRoD3RDIId9bU+InCJ/abAFPM9B3Q==</Password>
        </FTPSite>
        <HttpSite Type="repository" Name="NAIHttp" Order="3" Enabled="1" Local="1" Server="download.nai.com:80">
          <RelativePath>Products/CommonUpdater</RelativePath>
          <UseAuth>0</UseAuth>
          <UserName></UserName>
          <Password
Encrypted="1">f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==</Password>
          </HttpSite>
        </SiteList>
      </ns:SiteLists>
```

VirusScan configuration

NetUp32 will import CONFIG.REG and/or <computername>.REG from <NetUp32_dir>\Config directory if they got a different size than the ones which is places in the local <Program files>\Network Associates\VirusScan\ directory.

```
szConfig_reg=CONFIG.REG
bUpdate_config=1
uDelay_before_service=30
bStop_service_before_Config=1
```

The name of the configuration file is determined by NetUp32.ini szConfig_reg=CONFIG.REG. It's possible to have a different .REG file for workstation and servers.

Progress window:

AntiVirus Update - NetUp32 (v. 7.0.0.258) - Eterra

Opdaterer VirusScan konfiguration

Stopper McAfee service...

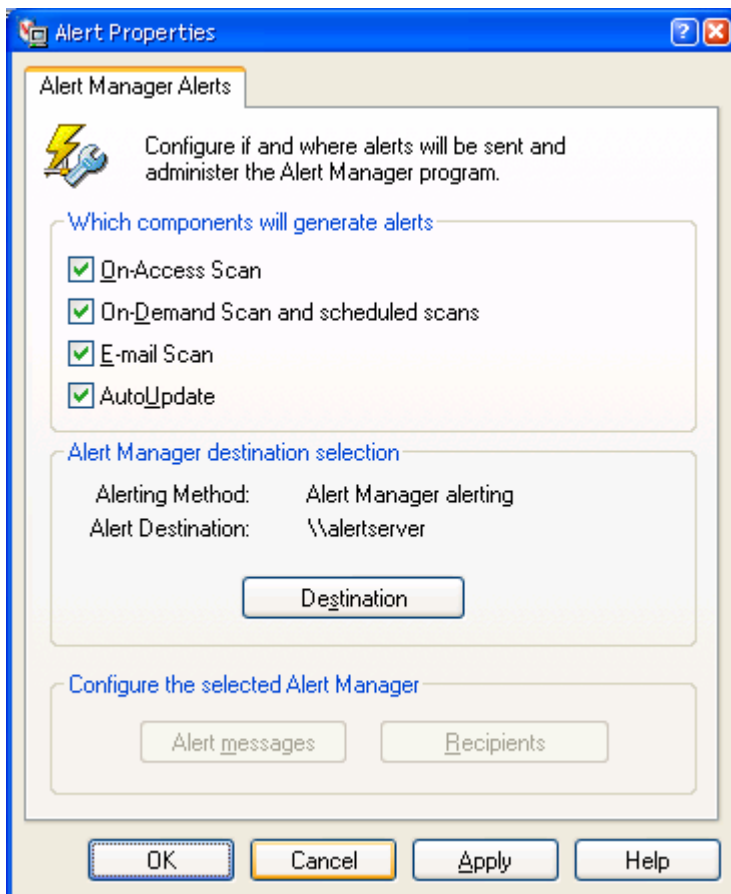
Use central Alert manager

We recommend configuring VirusScan to forward alerts to a central Alert Manager server. The server has to run Alert Manager version 4.7. This can be changed in \Config\CONFIG.REG in this section

```
;** Alert manager section - START **
[HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\Shared Components\Alert
Client\VSE]
"Alert Manager Server Path"="\\.\alertserver"
"AlertType"=dword:00000004
"Alert Manager Logical Name"=""
"Active Directory"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan
Enterprise\CurrentVersion\Alerts\CurrentVersion]
"bSendToAlertManagerUpdate"=dword:00000001
"bSendToAlertManagerOAS"=dword:00000001
"bSendToAlertManagerODS"=dword:00000001
"bSendToAlertManagerEmail"=dword:00000001
"dwLastModified"=dword:00000001
;** Alert manager section - END **
```

Change to *alertserver* to the name of you alert server. Do not remove the 4 \.



Review the alert information from the VirusScan Console menu “Tools” -> “Alerts...”

If password protected, you need to choose “Unlock User Interface” before you can access the “Alerts...” menu.

Password protect VirusScan configuration

We recommend the VirusScan configuration is protected by password. This will prevent the users from changing VirusScan configuration. By default NetUp32 will password protect every section in VirusScan configuration with the password “netup32” except On-Demand scan settings.

This can be changed in CONFIG.REG in this section

```
;** Password protection - START **
[HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan
Enterprise\CurrentVersion]
"UIPMode"=dword:00000002
"dwConsoleRefreshRate"=dword:00000003
"UIPPages"=hex:01,01,01,01,01,01,01,01,01,01,01,01,01,01,01,01,00,00,01,00,00,\
01,00,01,01,01,01,01,01,01,01,01,01,01,01,01
"UIP"="06abc5325ca037d4ed02993a54607b77"
;** Password protection - END **
```

Automatic update (every hour or whenever you want)

NetUp32 will normally be activated from the loginscript. If this is the only way VirusScan is updated it can result in cases where VirusScan is not up to date. This can happen where the workstation is not logged off every day. The workstation is only locked or in standby mode. To prevent this from happening NetUp32 and VirusScan Enterprise offers several solutions:

1. By default VirusScan Enterprise will perform AutoUpdate every Friday between 17:00 and 18:00. The update will be performed from the AutoUpdate Repository List. If the first site fails AutoUpdate will use the next site in the list. This makes it possible for AutoUpdate to update even if the internal update site is not reachable. The update will then be performed from Network Associates FTP or HTTP site (they are by default included in the Repository List)
2. NetUp32 can configure VirusScan Enterprise to perform AutoUpdate whenever you want. This is done by VSECFG.CAB which is created by McAfee Install Designer. See Configuration by McAfee Install Designer section.
3. Use Windows Schedule Tasks to activate NetUp32. This is very useful on servers because NetUp32 is not activated very often through the loginscript on the server. NetUp32 will not only update VirusScan Enterprise it will also check to that every thing is running and report the status in NetUp32 log files. The schedule tasks can be created and push to the servers and workstations with Remote Update.
4. Start_32.exe can be used to activate NetUp32 with another user account which has administrators right on the system but Start_32 can also be use to automatically run NetUp32 every x minutes. This can be controlled from the [Start_32] section in NetUp32.ini where uRepeat_min= will contain the number of minutes between activation of NetUp32. Start_32 will be running all the time as a “sleeping” process.

An AutoUpdate will not generate a lot of network traffic. If there is nothing to update there will only be transferred about 2000 bytes over the network.

Configuration by McAfee Install Designer - MID

VirusScan Enterprise configuration can be completely managed by McAfee Install Designer – in short MID. NetUp32 support the distribution of these MID configuration packages to the VirusScan Enterprise directory (normally . The name of the MID configuration files are fixed:

VSECFG.CAB	— For both servers and workstations.
VSECFG_S.CAB	— For servers only.
VSECFG_W.CAB	— For workstations only.

By default NetUp32 will check for these MID configuration packages in the \CONFIG\MID directory. This can be changed in NetUp32.INI in the [Workstation] and [Server] section:

Default value:

```
szConfig_cab_path=MID\
```

For more information about McAfee Install Designer read the McAfee Install Designer Product Guide.

NetUp32 will first check for the file VSECFG_W.CAB on workstations or VSECFG_S.CAB on servers. If this configuration file is not found NetUp32 will use VSECFG.CAB which is a configuration file which can be use for both workstations and servers.

Support for Windows 9x and VirusScan 4.5.1

VirusScan Enterprise 7.0 does not support Windows 95, Windows 98 and Windows ME. With NetUp32 version 7.0.xxx it is possible to start NetUp32 version 4.5.1.xxx when a Windows 9x system start NetUp32 version 7.0.xxx. This is handled by this section in netup32.ini.

```
[Win9x]
bNetUp32_active=1
szPrevious_NetUp32=
```

szPrevious_NetUp32 has to point the UNC path and name of a NetUp32 version 4.5.1.xxx. This makes it possible for NetUp32 version 7.0.xxx to coexist with Windows 9.x, VirusScan 4.5.1 and NetUp32 4.5.1.xxx.

It is recommended to use the \SCRIPTS\TestOS.bat in the loginscript to selected the right NetUp32 version depending on the OS version.

Log information

NetUp32 will maintain several log files.

Audit log – contain information about the current state of the system which activate NetUp32.

Normal named AUDIT70.TXT

Install log – contain information about which component is being installed or updated.

Normal named INSTALL70.TXT

On-access log – contain VShield virus alert log from system which has detected virus.

Normal named _VSH.TXT

On-demand log – contain VirusScan virus alert log from system which has detected virus.

Normal named _SCN.TXT

AutoUpdate log – contain AutoUpdate log files from systems where the AutoUpdate has failed.

The log file is named AutoUpdate.TXT

Install problem log – contain VirusScan installation log (C:\VSCAN.TXT) from systems where the installation has failed. The log file is named INSTALL_ERROR.TXT.

Netup32.ini has a [Log] section.

```
[Log]
szlog_path=
szInstall_list_file=INSTALL70.TXT
bAudit=1
szAudit_list_file=AUDIT70.TXT
bShow_logfile_warning=0
szRun_at_log_warning=
bClear_logfile=1
bCheck_install_log=1
```