

NetUp32 version 7 - News and updates

Support: Ementor Network Associates support 80 81 56 60 / +45 87 40 72 30 - www.mcafee.dk
Email: support@mcafee.dk
Online manual: <http://mcafee.dk/support/onlinemanualer.php>
Remember to quote version and attach NETUP32.INI

Copyright Ementor Denmark 2004

NETUP32.EXE version 7.1.0.352 (2004-04-23)

NetUp32 did not always correctly identify the user as administrator

Even if the setting bcheck_user_access=0 NetUp32 would still check for administrator rights. This has now been corrected.

NetUp32 can now upgrade old ePO agents

In the [ePO_agent] section bCheck_epo_agent_ver=1 controls if a newer ePO agent (FramePkg.exe) from the NetUp32 ePO directory should be installed. bEnable_Install_ePO=1 has to be enabled before bCheck_epo_agent_ver=1 has any function.

NetUp32 can now upgrade Common Framework - CMA

A new section in NetUp32.ini has been added:

```
[CMA]
bEnable_Update_CMA=1
szInstall_path_CMA=
szRun_setup_CMA=FRAMEPKG.EXE /FORCEINSTALL /INSTALL=UPDATER /SILENT
```

And a new directory called CMA which contains new Common Framework installation packaged installation file.

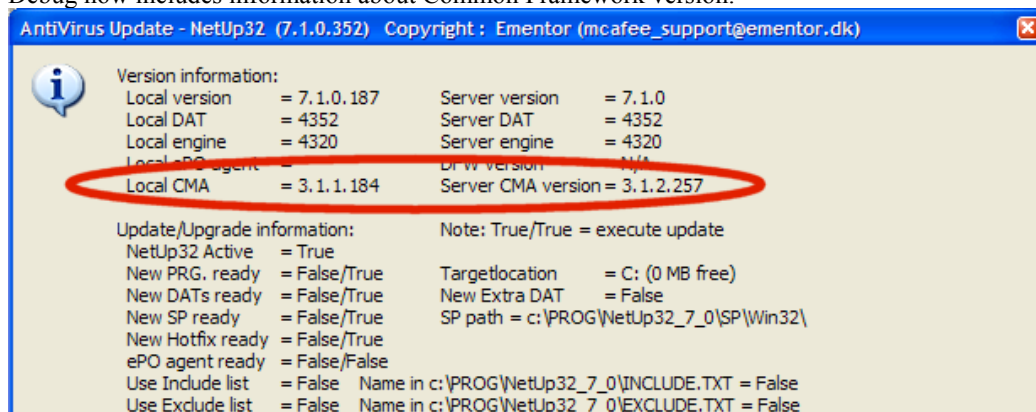
Common Framework version 3.1.2.257 has been included in the NetUp32 7.1.0.352 packaged in the \CMA\FramePkg.exe file.

VirusScan Enterprise 7.1.0 is installed with Common Framework version 3.1.1.184.

Please note that FTPUpdate has been replaced by CURT (Common Updater Replication Tool)

CURT will now handle the download of updates through HTTP and extra.dat through FTP.

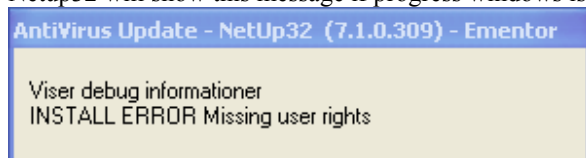
Debug now includes information about Common Framework version.



NETUP32.EXE version 7.1.0.338 (2004-03-18)

NetUp32 will only start installation if the user running NetUp32 is local administrator

Netup32 will show this message if progress windows is enabled.



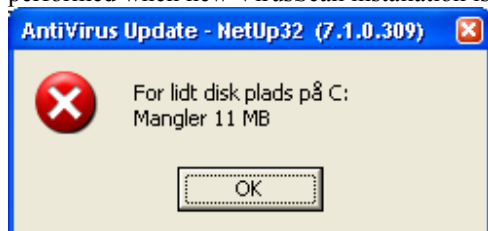
An error is written to INSTALL log if the user is not local administrator. The line starts with "Missing user rights"

Expand environment variables from NetUp32.INI and parameters

NetUp32 will now expand environment variables from every string parameter or any string key in NetUp32.INI. F.x. szRun_setup=setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS="" RUNAUTOUPDATE="" RUNONDEMANDSCAN="" LOCKDOWNVIRUSSCANSHORTCUTS="" VIRUSSCANICONLOCKDOWN=NORMAL REBOOT=R /li "%SystemDrive%\vscan.txt" /q /i

It is now possible to change the amount of free disk space need for an installation to proceed

A new option is added to the [Workstation] and [Server] section in NetUp32.INI: uFree_DiskSpace=50. The check is performed on the %SystemDrive%. There will be no check on disk space if this is set to 0 or empty. The check is only performed when new VirusScan installation is ready.



Netup32 will no longer use bcheck_free_diskSpace=1

Control the installation time-out

It is now possible to control the time-out for the setup to complete. Default uSetup_timeout=30

Enhanced logging in the Audit file

NetUp32 has now added 4 new entries to the Audit log file log. This is Desktop Firewall service status, Desktop Firewall version, IP address and NetUp32 version.

The Netup32 path will now convert mapped networkdrives to the UNC path.

With this new feature it is possible with DMEA to locate windows system not running NetUp32.

To support this feature NetUp32 Logviewer and NetUp32 Log Monitor needs to be updated.

It is recommended to remove old audit and install log files before implemented this new NetUp32 version.

Updated the configuration handling

If the directory defined by szConfig_cab_path= does not exist it will use the default directory MID\.

This can be useful if running with many different configuration directories and they are named as the computername.

Fx. NetUp32.EXE szConfig_cab_path=%COMPUTERNAME%\

Improved VShield and VirusScan central log update

The update to the central log files _VSH.TXT and _SCN.TXT are now improved to avoid mix up of different log files written at the same time.

Improved AUDIT and INSTALL central log update

Add support for file lock, write, release and wait, for support of multiple writes at the same time.

VirusScan installation errors are now reported in a separate directory

If NetUp32 detects an installation error the log file will now be copied to

`\LOG\Install_ERROR\<computername>.vscan.txt`

Previously the installation log was appended to the `\LOG\INSTALL_ERROR.TXT`

Enhanced VirusScan installation log check

NetUp32 will now perform a better check of the VirusScan installation log. NetUp32 will now resolve the installation log files from the `szRun_setup=setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS=""`

`RUNAUTOUPDATE="" RUNONDEMANDSCAN="" LOCKDOWNVIRUSSCANSHORTCUTS=""`

`VIRUSSCANICLOCKDOWN=NORMAL REBOOT=R /li "%SystemDrive%\vscan.txt" /q /i`

By reading the path and file name of the `/li` parameter.



Updated handling of registration files.

NetUp32 has now expanded the support for registry files. CONFIG.REG has been split into 5 separate .REG files. This is done to make it easy to enable, disable configurations features and also to add new configuration settings in new .REG files

`\CONFIG\REG`

```
enable_action_on_unwanted.reg
enable_and_name_alert_manager.reg.disable
enable_remove_splashscreen.reg
enable_password.reg
enable_detect_unwanted.reg
```

NetUp32 will apply all the .REG files in the `\CONFIG\REG` directory. All other files will be ignored. By default only one configuration file is disabled. This is the `enable_and_name_alert_manager.reg.disable` file. Before you delete the .disable extension change the Alert Manager Server name in the file.

The CONFIG.REG is still supported if this file exists.

The configuration and registration files will be applied in the following order:

- `\CONFIG\MID\VSECFG.CAB`
- `\CONFIG\CONFIG.REG`
- All the .REG files in the directory `\CONFIG\REG\`
- `\CONFIG\<computername>.REG`

NOTE:

Remember to remove/disable the .REG files if configurations are handled by a VSECFG.CAB file in the `\MID` directory.

New information on the information screen

AntiVirus Update - NetUp32 (7.1.0.338) Copyright : Ementor (mcafee_support@ementor.dk)

Version information:

Local version	= 7.1.0.187	Server version	= 7.1.0
Local DAT	= 4339	Server DAT	= 4333
Local engine	= 4320	Server engine	= 4320
Local ePO agent	=	DFW version	= 8.0.465

Update/Upgrade information:

NetUp32 Active	= True	Note: True/True = execute update	
New PRG. ready	= False/True	Targetlocation	= C: (0 KB free)
New DATs ready	= False/True	New Extra DAT	= True
New SP ready	= False/True	SP path	= C:\PROG\NetUp32_7_0\SP\Win32\
New Hotfix ready	= False/True		
ePO agent ready	= False/False		
Use Include list	= False	Name in C:\PROG\NetUp32_7_0\INCLUDE.TXT	= False
Use Exclude list	= False	Name in C:\PROG\NetUp32_7_0\EXCLUDE.TXT	= False

System information:

OS	= Windows NT/2000/XP	RAS con.	= 0
User	= test	LangID	= 6
IP Addr	= 10.41.22.34	LocalAdm	= False
Date	= 18-03-2004	Time	= 09:25:41
		Licensedate	= 29-09-2006

Configuration information:

Netupdat source = C:\PROG\NetUp32_7_0\
Setup string = setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS="" RUNAUTOUPDATE=""
RUNONDEMANDSCAN="" LOCKDOWNVIRUSSCANSHORTCUTS="" VIRUSSCANICONLOCKDOWN=NORMAL
REBOOT=R /li "C:\vscan.txt" /q /i
INI file = C:\PROG\NetUp32_7_0\NETUP32.INI
Logpath = C:\PROG\NetUp32_7_0\LOG
TEMP = C:\DOCUME~1\test\LOCALS~1\Temp\NETUP32\
VShieldLog = C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\OnAccessScanLog.txt
Scan32Log = C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\OnDemandScanLog.txt
CMD_line = netup32

NOTE: To remove this message, set bDebug=0 in C:\PROG\NetUp32_7_0\NETUP32.INI

OK Cancel

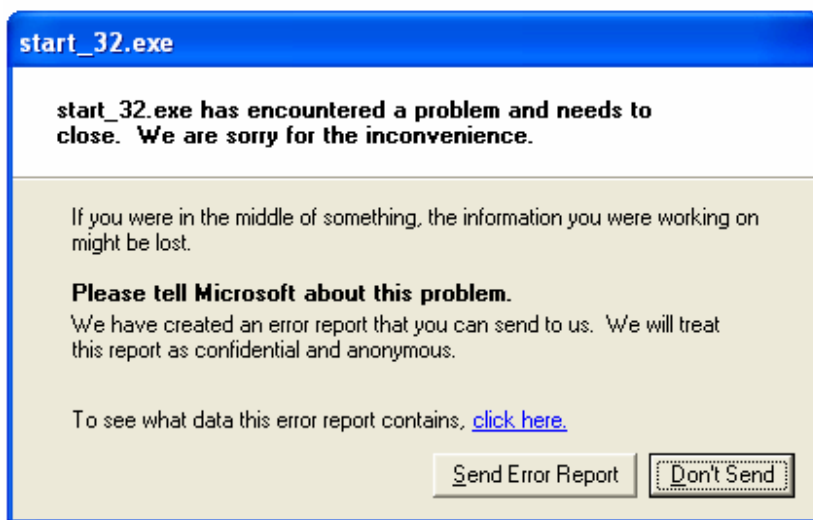
In the System information section LocalAdm will show false if the user account running NetUp32 is not local administrator.

Enhanced ePO agent check

NetUp32 can now check for both ePO agent version numbers in registry and verify that the local SiteList.XML also include a SpipeSite. The SpipeSite check can be disabled by setting bCheck_for_Spipesite=0 in NetUp32.INI.

Start_32 has been updated to version 7.1.0.335

In some situation Start_32 could return a Windows error when running under Windows XP as an ordinary user where the c:\program files\NetUp32 directory already existed. The problem occurred when Start_32 was trying to change the local Netup32.ini and did not have the right privileges to do so. This has now been corrected. Start_32 will now run NetUp32 from the server if it can not make changes to a local copy of NetUp32.ini.

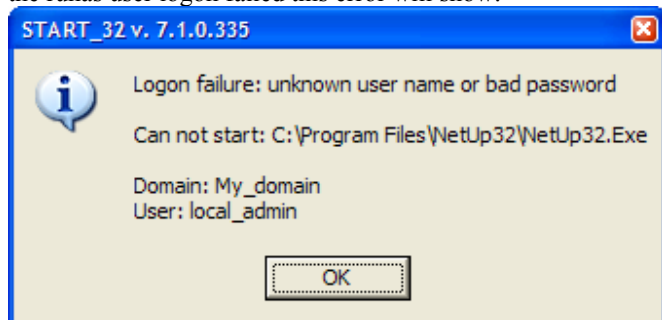


Start_32 can now point to other configuration files

Start_#2 support szinfile= parameter which now makes it possible to use a different configuration file for NetUp32
F.x. START_32 szinfile=\\server\share\my_ini_file.ini bAnswer=1 bDebug=0

Start_32 improved runas check

If the runas feature is used. Start_32 will verify that there is access to the NetUp32.exe on there server. If there is access but the runas user logon failed this error will show:



Run Start_32 from the server drive

Run START_32 with bRun_From_Server=1 as parameter will not make a local copy of NetUp32. Default in c:\Program Files\NetUp32. Fx. START_32 bRun_From_Server=1

Start_32 can now place the local copy of NetUp32 in other directories

With the szLocalPath= parameter on Start_32 it is possible to choose where START_32 places the local copy of NetUp32.exe and the configuration file.

Fx. START_32 szLocalPath=C:\NETUP32 or START_32 szLocalPath="C:\PROGRAM FILES\USE"

NETUP32.EXE version 7.1.0.302 (12/11 2003)

NetUp32 did not verify the installation log (C:\VSCAN.TXT) correctly on Windows NT 4.0

NetUp32 will now correctly identify if the log file is written in UNICODE or ANSI and then check to log file accordingly. Previously this problem could result in NetUp32 waiting 30 minutes before it would continue.

NETUP32.EXE version 7.1.0.299 (30/10 2003)

NetUp32 did not collect all the log files which contain virus alerts

NetUp32 will now correctly identify virus alerts in the local OnAccessScanLog.txt and OnDemandScanLog.txt log file. The log files are normally placed in

c:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan\

NetUp32 will only append the log file to the central log directory in the file _VSH.TXT or _SCN.TXT and delete the local log file if it contains a virus alert. If the log files had not previously been detected by NetUp32 they will be detected now.

NETUP32.EXE version 7.1.0.298 (20/10 2003)

NetUp32 can now install and maintain VirusScan Enterprise version 7.1.0

NetUp32 supports both version 7.0.0 and 7.1.0. Depending on which installation files is placed in the \VirusScan directory. NetUp32 will not and cannot downgrade version 7.1.0 to version 7.0.0. NetUp32 will upgrade version 7.0.0 to version 7.1.0.

Updated installation “completed” or “fail” verification

In some situations the installation log C:\VSCAN.TXT included special characters which made the installation completion check fail. This could cause NetUp32 to wait 30 minutes for the installation to complete. After the 30 minutes NetUp32 will stop without updating VirusScan. This has now been corrected.

Check for install errors during installation

NetUp32 will now check the install log C:\VSCAN.TXT for installation errors. Previously NetUp32 would wait 30 min. before there NetUp32 would stop waiting for the installation even if the installation had failed.

Separate directory for EXTRA.DAT

NetUp32 will now use a separate directory for the EXTRA.DAT file. Previously the EXTRA.DAT file had to be placed in the CommonUpdater directory. The new directory is named EXTRADAT. The directory name can be changed by the szExtra_DATS_dir = in the [DAT] section. Use an updated version of FTP Update for support of the EXTRADAT directory.

Change in NetupTXT.6 and NetupTXT.9

Line number 59 has been added to the two languages text files in \CONFIG.

Copy the VirusScan installation log to the server log directory

NetUp32 can now make a copy of the local installation log file C:\VSCAN.TXT to the server <log directory>\Install. The log file on the server will be named <hostname>.vscan.txt. This makes it possible to get a log file from every installation which is started. If a log file with the same name already exists it will be overwritten. The size of the log file is normally 40 -160 Kb.

This is controlled by bCopy_VSCAN_log=1 in the [Log] section. By default this feature is disabled.

Delete C:\VSCAN.TXT after completed installation

NetUp32 will delete the installation log file C:\VSCAN.TXT if the installation is completed correct

Updated the handling of the ePO agent installer source directory correctly

Previously the NetUp32 used the absolute path to FramePkg.exe, now NetUp32 use a relative path from <NetUp32_Dir>. The path is changed by szInstall_path_ePO= in the [ePO_agent] section. This makes is possible to us McAfee AutoUpdate Architect to check in an ePO agent installation packaged which will be available in the CommonUpdater directory. Use this feature by changing szInstall_path_ePO=CommonUpdater\Current\EPOAGENT3000\Install\0409

Run a shell command before setup

NetUp32 now support making a ShellExecute before installing VirusScan Enterprise. The ShellExecute is started before the "szRun_before_setup=". ShellExecute can for example be used to run a .htm file or a web link without knowing which web browser is installed on the system.

This is controlled by:

szRun_Shell_before_setup= in the [Workstation] and [Server] section

Force VirusScan Enterprise installation

NetUp32 can now force the installation of VirusScan Enterprise even if it is already installed. This is done by running NetUp32 bForceInstall=1

or

Start_32 bForceInstall=1

Force ePO agent installation

NetUp32 can now force the installation of the ePO agent even if it is already installed. This is done by running

NetUp32 bForceInstall_ePO=1

Or

Start_32 bForceInstall_ePO=1

Expanded VirusScan Enterprise service check

NetUp32 will now verify that McAfee Framework service is running. If it is not running it will be try to start the service. If the service can not be started it will be reported in AUDIT70.LOG in the AVSynMgr column. The log file can be monitored by NetUp32 Log Monitor which will send an email if a McAfee VirusScan Enterprise service is not running.

NetUp32 now checks 3 services:

Network Associates McShield	-	McShield
Network Associates Task Manager	-	McTaskManager
McAfee Framework Service	-	McAfeeFramework

This check and start of services is enabled by default in the [Workstation] and [Server] section

bCheck_service=1

bStart_service=1

Verify that the user running NetUp32 has got the right access to perform VirusScan installation

NetUp32 can now before installing VirusScan verify that the user account running NetUp32 has write access to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\. This is a good indication that the user account has the sufficient right to perform a VirusScan installation.

This verification can be enabled by bcheck_user_access=1 in the [Workstation] and [Server] section.

START_32.EXE (11/08 2003) NEW VERSION

Fixed: You will not get an error when disconnecting from the network where NetUp32 is activated repeatedly by START_32 with x minute interval. START_32 will verify that there is access to the server where NetUp32 is located before running NetUp32.

New feature: Run NetUp32 from server

Start_32 will as default make a copy of NetUp32 in C:\Program Files\NetUp32. This feature can now disabled by this setting by running START_32 bRun_from_server=1

Control the settings with parameters

START_32 now support parameters which will overrule the setting from the .INI file.

Fx: START_32 bDebug=0 szlog_path="\\server1\share\log dir"

NETUP32.EXE version 7.0.0.291 (08/09 2003)

Control the settings with parameters

NetUp32 now support parameters which will overrule the setting from the .INI file.

Fx: START \\server\share\7.0.0\NetUp32.EXE bDebug=0 szlog_path="\\server1\share\log dir"

Remember to use " around values which contains spaces.

Start NetUp32 with another .ini file use NetUp32.EXE szINIFile=new.ini here is some examples:

```
NetUp32.EXE bDebug=0 szINIFile=new.ini
NetUp32.EXE bDebug=0 \\server\share\7.0.0\new.ini
NetUp32.EXE bDebug=0 new.ini
```

[ePO_agent] section in NetUp32 has been changed

NetUp32 version 7.x only supports ePO 3.0 agent installation. The name of the keys in the [ePO_agent] section has also been changed to support the use of parameters:

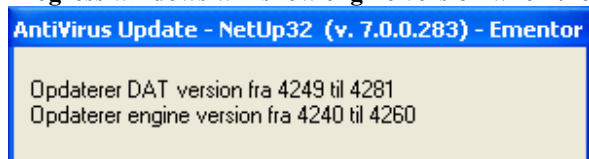
```
[ePO_agent]
bEnable_Install_ePO=0
bOnly_install_ePO=0
szInstall_path_ePO=
szRun_setup_ePO=FRAMEPKG.EXE /INSTALL=AGENT
```

[Workstation] and [Server] section

```
bChangeSitelist=0
```

NOTE: Sitelist.XML will not be changed if ePO 3.x is installed. Previous version of NetUp32 would change Sitelist.XML which will conflict with the ePO configuration of SiteList.XML.

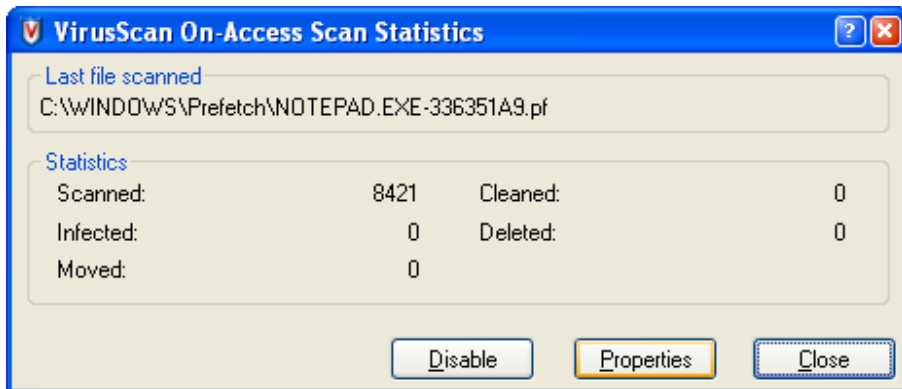
Progress windows will show engine version when the engine is being updated



Removed problem with VirusScan On-Access Scan Statistics window

The SHSTAT process (the VirusScan On-Access icon in systray) will only be started after a VirusScan installation if the process is not running. This is a know issue when upgrading from VirusScan 4.5.x to VirusScan Enterprise. There have been reported problems where the previous NetUp32 could start the "VirusScan On-Access Scan Statistics window" or started 2 icons in the systray.

Here is an example of the VirusScan On-Access Scan Statistics window



Install ePO 3.0 agent

Create an ePO directory in the NetUp32 directory and place the FramePkg.exe (agent installation file) in this directory. If bOnly_install_ePO=1 then NetUp32 will overrule the following setting and disable them.

```
bUpdate_program=0
bUpdate_DAT=0
bUpdate_SP=0;
bUpdate_config=0
bChangeSitelist=0
bUpdate_after_install=0
```

Installing ePO agent and VirusScan Enterprise

If you use ePO and NetUp32 it is important that NetUp32 do not update DAT/engine and change the configuration.

Run:

```
START_32 bdebug=0 bUpdate_DAT=0 bUpdate_config=0 bChangeSitelist=0
bUpdate_after_install=1 bEnable_Install_ePO=1
```

Or

```
NETUP32 bdebug=0 bUpdate_DAT=0 bUpdate_config=0 bChangeSitelist=0
bUpdate_after_install=1 bEnable_Install_ePO=1
```

Conflict with McAfee Autoupdate Architect solved

If McAfee Autoupdate Architect is installed NetUp32 will not change to local Sitelist. If a new DAT files is available NetUp32 will activate an update and the update sitelist will not be changed by NetUp32.

Corrected bUseSuperDAT_for_update=1

Previous NetUp32 tried to start SDATxxxx from the wrong directory in the Commonupdater directory. This has now been fixed.

Progress window missing if using uDelay_sec and uRandom_Delay_min

This has been corrected and the progress window will now show correctly.

Log files were not collected from Windows NT 4.0 workstation and server

The All User Profile was not handled correctly when running Windows NT 4.0. This problem is now corrected. NT 4 - the directory is normal:

C:\WINNT\Profiles\All Users\Application Data\Network Associates\VirusScan

Windows 2000, 2003 and XP – the directory is normal:

C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan

This can change depending on the Windows installation. NetUp32 is flexible and will read the directory information from the system.

Running NetUp32 on a system with McAfee Autoupdate Architect

Run NetUp32 or Start_32 with bChangeSitelist=0

Run program or script before and/or after DAT update

The [DAT] section includes two new lines in NETUP32.INI in.

szRun_before_DAT=

szRun_after_DAT=

NetUp32 will run the program/script and wait for it to finish.

Complete control with update sites

Normally NetUp32 will change the first update site in the local Sitelist.xml which is a copy from (\Config\SiteList.xml). It is now possible to prevent NetUp32 from copying SiteList.xml from the server and changing the first update site.

[Workstation] and [Server] section

bChangeSitelist=0

Add information to information window

CMD_line = the command line which is used to activate NetUp32

AntiVirus Update - NetUp32 (v. 7.0.0.291) Copyright : Ementor - (support@mcafee.dk)

Version information:

Local version	= 7.0.0.511	Server version	= 7.0.0
Local DAT	= 4291	Server DAT	= 4291
Local engine	= 4260	Server engine	= 4260
Local ePO agent	=		

Update/Upgrade information: Note: True/True = execute update

NetUp32 Active	= True		
New PRG. ready	= False/True		
New DATs ready	= False/True	New Extra DAT	= False
New SP ready	= False/True	SP path	= c:\PROG\NetUp32_7_0\SP\Win32\
New Hotfix ready	= False/True	ePO agent ready	= False/False
Targetlocation	= (0 KB free)		
Use Include list	= False	Name in c:\PROG\NetUp32_7_0\INCLUDE.TXT	= False
Use Exclude list	= False	Name in c:\PROG\NetUp32_7_0\EXCLUDE.TXT	= False

System information:

OS	= Windows NT/2000/XP	RAS con.	= 0
User	= sp	PC	= OPA-SP-310
Date	= 08-09-2003	Time	= 14:12:44
		LangID	= 6
		Licensedate	= 29-09-2006

Configuration information:

Netupdat source = c:\PROG\NetUp32_7_0\
Setup string = setup ADDLOCAL=ALL REMOVE=EmailScan PRESERVESETTINGS="" RUNAUTOUPDATE=""
RUNONDEMANDSCAN="" LOCKDOWNVIRUSSCANSHORTCUTS="" VIRUSSCANICONLOCKDOWN=NORMAL
REBOOT=R /li "c:\vscan.txt" /q /i
INI file = c:\PROG\NetUp32_7_0\NETUP32.INI
Logpath = c:\PROG\NetUp32_7_0\LOG
TEMP = C:\DOCU...1\sp\LOCALS~1\Temp\NETUP32\
VShieldLog = C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\OnAccessScanLog.txt
Scan32Log = C:\Documents and Settings\All Users\Application Data\Network
Associates\VirusScan\OnDemandScanLog.txt
CMD_line = "c:\PROG\NetUp32_7_0\NetUp32.exe" bdebug=1 udelay_sec=0

NOTE: To remove this message, set bDebug=0 in c:\PROG\NetUp32_7_0\NETUP32.INI

OK Cancel