



# Argon Client Management Services™ (CMS) and Virus Scanning

Using Argon  
CMS to  
perform  
centralized  
virus scanning  
can significantly  
reduce the  
Total Cost of  
Ownership

## Who should read this paper?

This paper is for system administrators who intend to use the Argon Client Management Services (CMS) to conduct centralized virus scanning in a pre-OS environment. This paper explains the advantage of running virus scans in pre-OS environments. Step-by-step instructions and sample files' content are provided in this document.

## Introduction

Using Argon CMS to perform centralized virus scanning can significantly reduce the Total Cost of Ownership (TCO) of client PCs. Computer viruses can be spread widely over networks and the Internet and are more destructive than ever before. Eradicating viruses and recovering infected systems can cost lots of time and money. It is not feasible in a corporate environment for a system administrator to visit every computer to scan/clean the virus or upgrade the virus scanning software.

CMS provides a virus-scanning solution to reduce TCO. With CMS, the administrator can conduct the virus scanning centrally, during off-hours, with the build-in Remote Wake-Up (RWU) functionality and scheduler.

## Pre-OS vs. Login Scripts

System administrators can embed virus scanning commands into system login scripts, so when the client PCs boot up and log into the server, the virus scanning commands will be executed. However, if a client PC is infected and encounters difficulties in connecting to the server or cannot even boot the operating system from its local hard drive, login script-driven virus scanning will be ineffective. With any PXE-compliant boot ROM, such as Argon's Managed PC Boot Agent (MBA), installed, the client PC can always connect to the server when it boots up, download an assigned boot image file, and execute it prior to loading the local operating system. The system administrator can assign a boot image file with virus scanning utility to a client PC, so the client PC can perform the virus scanning even when the PC cannot connect to the server via a login-script.

## Requirements


### Client PC:

- Has a boot ROM that is compatible with the Preboot Execution Environment (PXE) specification, such as Argon's Managed PC Boot Agent (MBA) v3.0 or greater.
- Has Remote Wake Up (RWU) ability and has proper power management (APM or ACPI). If the PC does not follow PCI specification v2.1 or higher, a RWU cable is needed to connect the network interface card (NIC) and the RWU socket on the PC's motherboard.

### Server:

- Microsoft Windows NT 4.0 server with Service Pack 4 or above, or Windows 2000 server
- A DHCP server
- Argon CMS — Client Boot Manager, Boot Server and TFTP Server
- DOS-based virus scanning software (such as F-Secure's F-PROT.EXE).

### Server Configuration:

- **Install Argon CMS on the server** (please refer to the Argon Client Management Services Quick Start Guide).
- **Configure and start the DHCP server.**
- **Start the Argon Boot Server and the Argon TFTP server.**
  1. On the Windows NT 4 or Windows 2000 server, click Start -> Settings -> Control Panel.
  2. On NT 4, double click on the "Services" icon in Control Panel window. On Windows 2000, double click the "Administrative Tools", and then double click on the "Services" icon.
  3. When the "Services" window displays, select "Argon Boot Server " and press the "Start" button (on NT 4) or click the  icon on the toolbar (on Windows 2000) to start the server.
  4. Start the "Argon TFTP Server".
  5. If the DHCP server is running on a different server, the Proxy DHCP should be run on the Boot Server. From the "**Control Panel**" window, double click on the "Argon Boot Server" icon, check the "Proxy DHCP" from the "Options" tab.

## Create a Virus Scanning Boot Image by using the Client Boot Manager that comes with CMS

1. On the server, create a shared directory and copy the DOS-based virus scanning utility (such as F-PROT.EXE) onto the server. For example, on the server `\\Demo`, create a directory `C:\VirusScan` and share the directory as `\\Demo\VirusScan`. Copy the virus scanning utility (the executables and all other relevant files, such as virus definition files) into this shared directory. The DOS version of F-PROT is shareware, free of charge for non-commercial use. The latest version of the software can be downloaded from [ftp://ftp.europe.datafellows.com/anti-virus/free/](http://ftp.europe.datafellows.com/anti-virus/free/).
2. Create a user account to access this shared directory, for example, user name: CMSUser, password: argon.
3. Create a virus scanning log subfolder for logging the scanning reports for each client PC. Create a subdirectory named "Log" under `C:\VirusScan`.
4. Create a batch file, named VIRUSCAN.BAT, to run the DOS-based virus scanning utility and log the report on to the server. Save this file to a directory, such as `C:\TFTPBOOT`. A sample VIRUSCAN.BAT is shown in the Appendix.
5. Launch Argon Client Boot Manager (CBM)

On the server, click Start -> Program Files -> Argon Client Management Services -> Client Boot Manager. The "Argon Client Boot Manager" window will be displayed. See Figure 1. If this is the first time running Client Boot Manager, please refer to the "Argon Client Management Services Quick Start Guide" for more information.

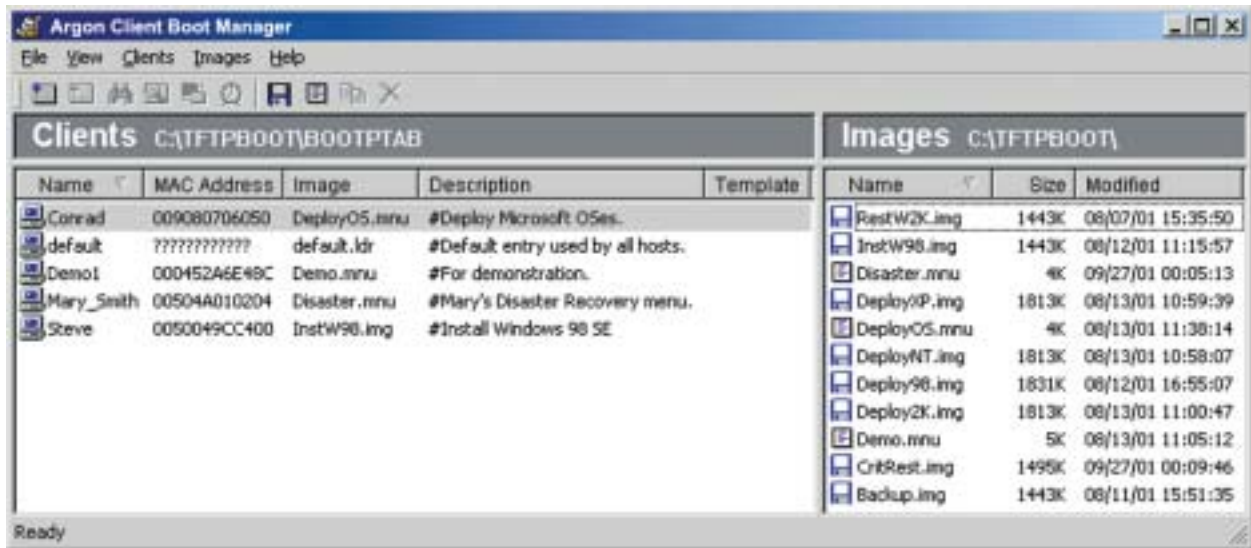



Figure 1. Client Boot Manager

6. Create a new boot image file
- 6.1 Click on the  button on the tool bar or select "New Image File..." from the "Images" menu of the CBM window. A "Create Image File" wizard appears.
- 6.2 Select the "Create a boot image using the wizard", then click "Next". See Figure 2.

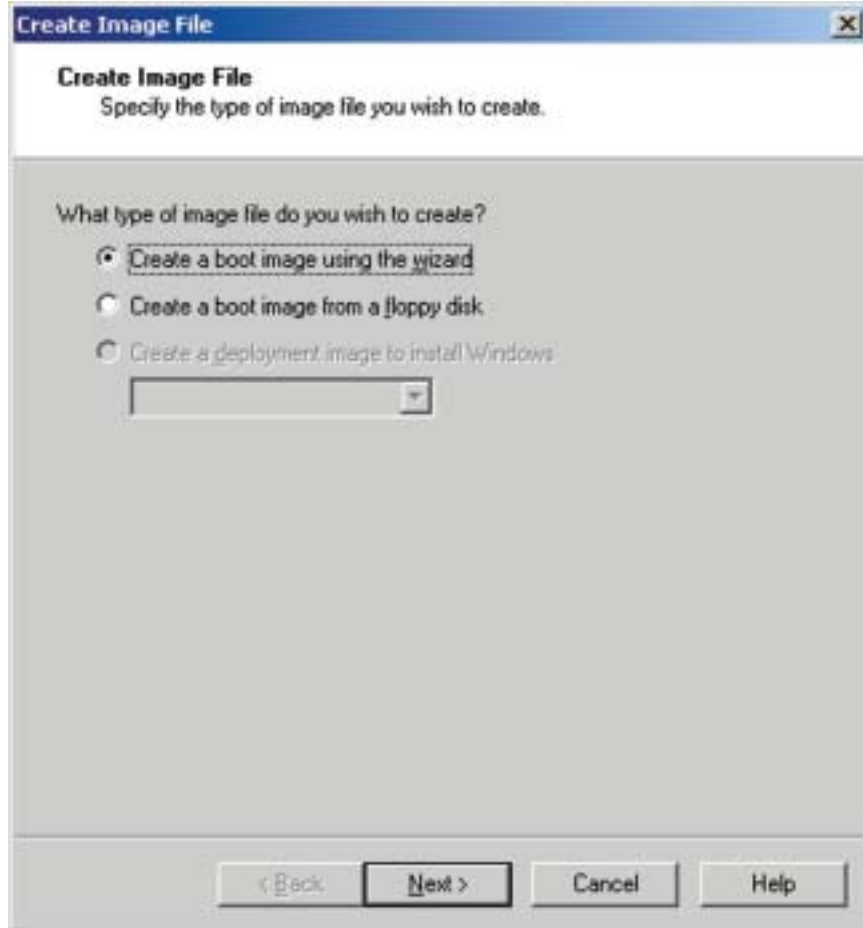


Figure 2. CBM's Create Image File Wizard – Create Image File

6.3 Type in the name of the image file, "VirusScan.img", then click "Next". See Figure 3.



**Create Image File**

**Image File Name**  
Please specify the name for this image file.

Image file name:  
VirusScan.img

< Back 

Figure 3. CBM's Create Image File Wizard – Image File Name

- 6.4 Check "Add this boot image to a menu file" and select "Create a new menu file for this image", use the default menu file name "VirusScan.mnu". Input "Scan for viruses on the client PC" into the "Menu title" field, and "Scan all local hard drives on the client PC and log the scan report to the server." into the "Menu description" area. Click "Next". See Figure 4.



Figure 4. CBM's Create Image File Wizard – Select Menu File

6.5 At the "Assign clients to the image" wizard screen, click "Next". See Figure 5.



Figure 5. CBM's Create Image File Wizard – Assign Clients to the Image

6.6 The image will be assigned to the client after the image is created. (See step 8).

If this is the first time using the CBM wizard to create a boot image, you will be asked to supply a copy of the DOS system files on a floppy. This only needs to be done once. After copying the files, click "Next".

- 6.7 Check "Enable network connection" on the "Network Connectivity" wizard screen, and select "Computer Name" as "MAC Address", "Specified" as the "Logon" and specify the logon name and password that was created in step 2 above. In the "Drive mapping" group, select an available Drive letter, such as Z:, and type in the share name, \\Demo\VirusScan, which is created in step 1, into the "Path" text box. Then click "Next". See Figure 6.

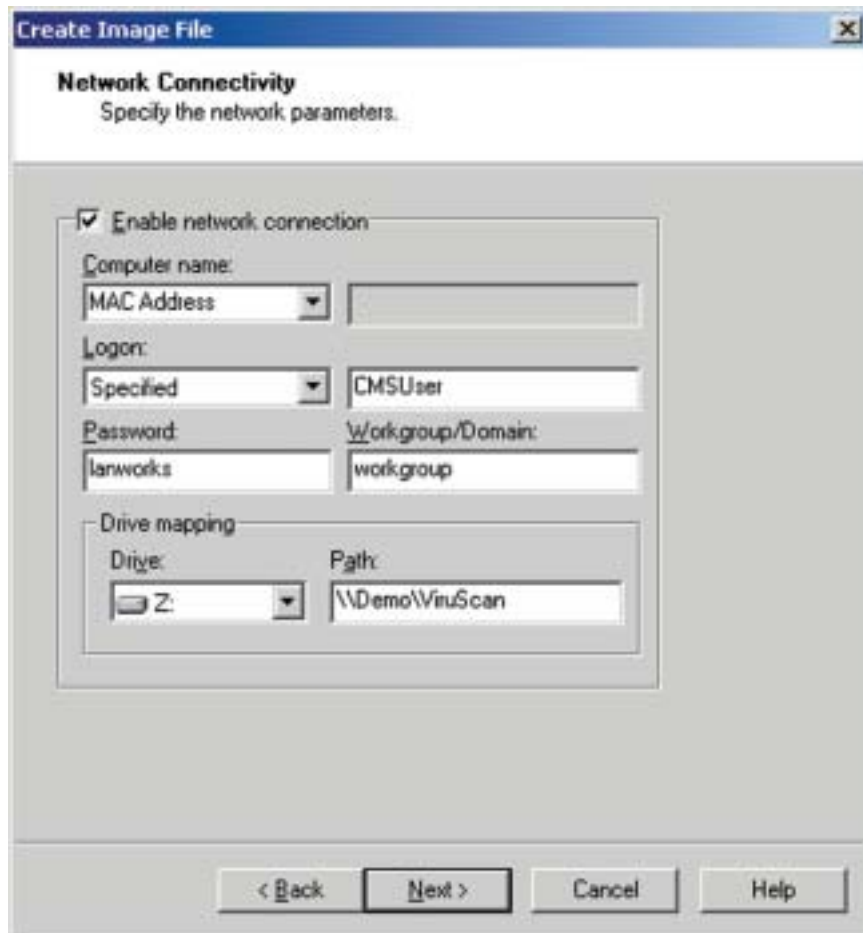


Figure 6. CBM's Create Image File Wizard – Network Connectivity

6.8 On the "Add Files" wizard screen, click the "Add Files..." button and select the VIRUSCAN.BAT file created



in step 4. Click "Next". See Figure 7. *Figure 7. CBM's Create Image File Wizard – Add Files*

6.9 From the "Image Options" wizard screen, select "Normal disk capacity", and check "Pre-OS" and "Keep UNDI in memory" in the "Options" group. Select "Shutdown" upon "Termination". Click "Next". See Figure 8.

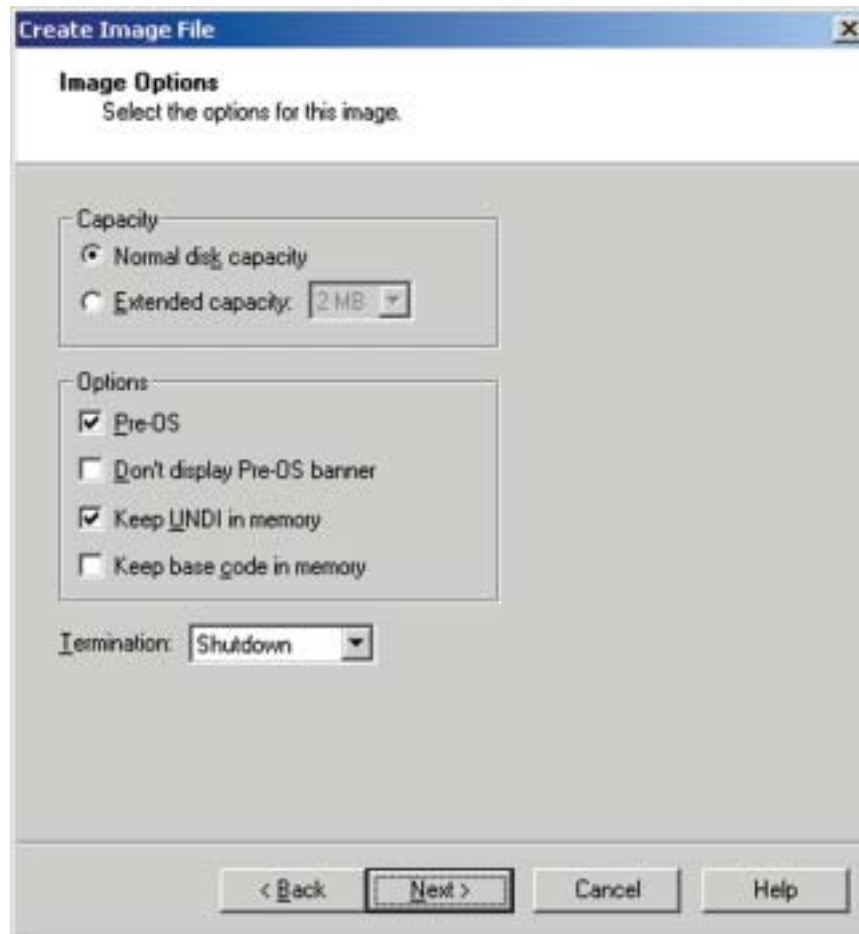


Figure 8. CBM's Create Image File Wizard – Image Options

6.10 Review the "Image Summary", check the "Open image when done" and then click "Finish" to create the boot image. See Figure 9.

When the image creation is done, the image is opened for editing See Figure 10.

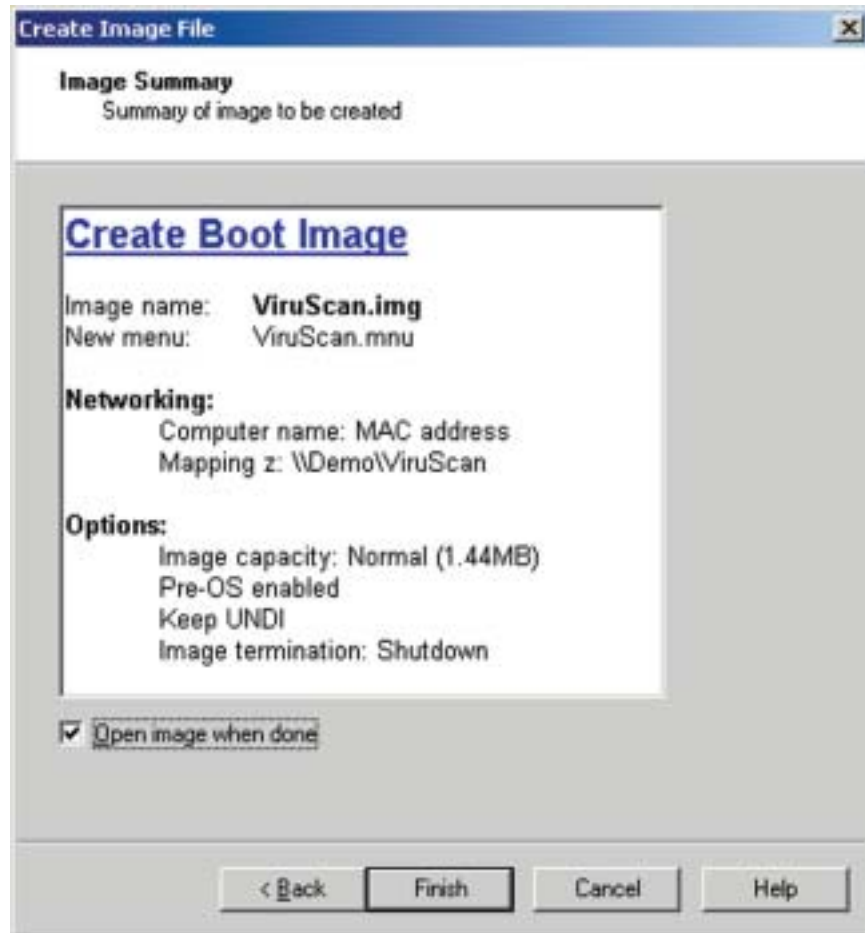


Figure 9. CBM's Create Image File Wizard – Image Summary

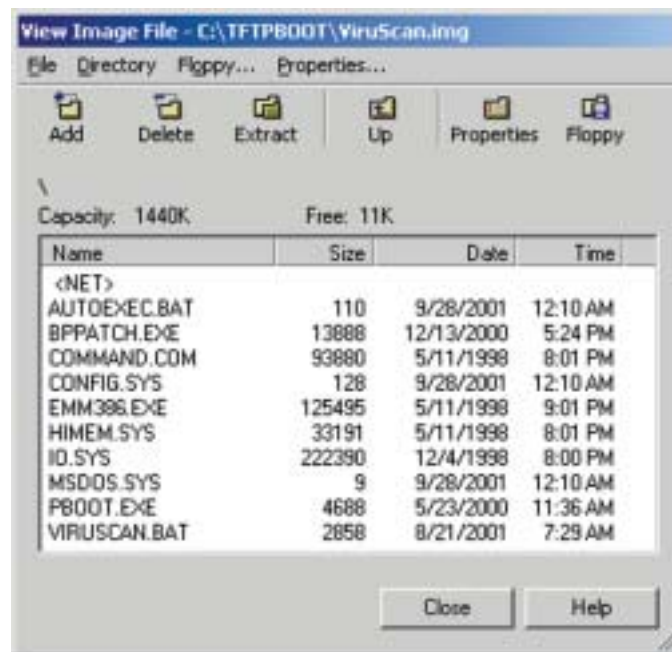


Figure 10. Open Boot Image: ViruScan.img

6.11 From the "View Image File" window, right click on the AUTOEXEC.BAT file and select "Edit..." from the action menu.

6.12 In the "Edit Text File" dialog, add the command "call viruscan.bat" before the last command "pboot /shutdown", then click "OK". See Figure 11.

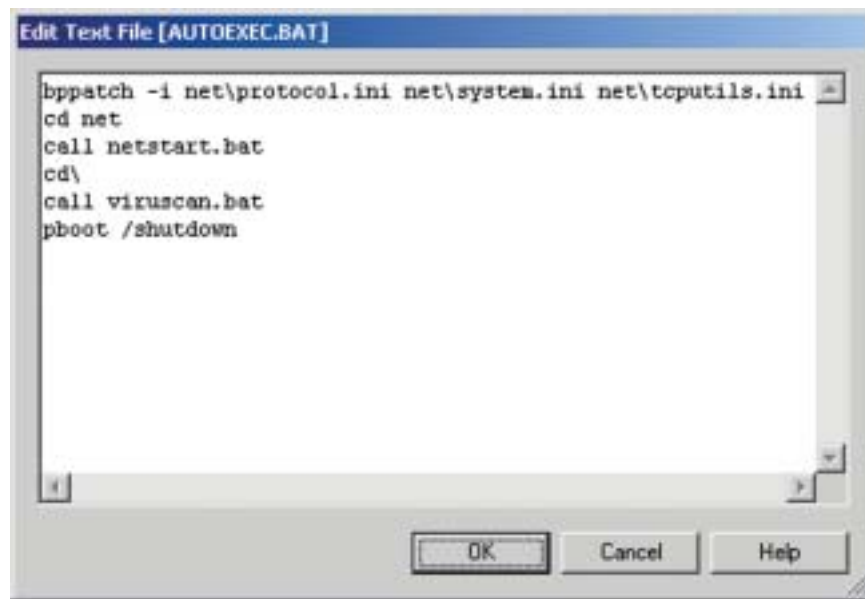


Figure 11. Edit AUTOEXEC.BAT

6.13 Click the "Close" to close the "View Image File" window and save the image file.

The boot image file (VirusScan.img) and the boot menu file (VirusScan.mnu) are now created and displayed on the right pane of the CBM window.

7. Set the VirusScan.img as the default image in the boot menu.


From the CBM window, double click on the boot menu file (VirusScan.mnu) created in step 6.4. The "Edit Menu File" dialog appears. See Figure 12. Select the menu item created for virus scanning and click the  icon on the toolbar, a small red arrow displayed to the left of this item means this menu item is set to the default menu item.



Figure 12: Set the default menu item


8. Create a client and assign the boot image to the client
- 8.1 Click on the  button on the tool bar or select "New Client..." from the "Clients" menu of the CBM. "New Client" dialog appears.
- 8.2 On the "Identification" tab, input a name for the client, such as "John\_Smith", type in the MAC address of the network interface card (NIC) the client uses. In the "Image file" field, enter "VirusScan.mnu", which is the boot menu file that just been created. See Figure 13. A description text can be typed in from the "Description" tab. Click "OK" to save the client.



Figure 13. Create New Client

Now the client "John\_Smith" will be shown on the left pane (Clients) of CBM window. See Figure 14.

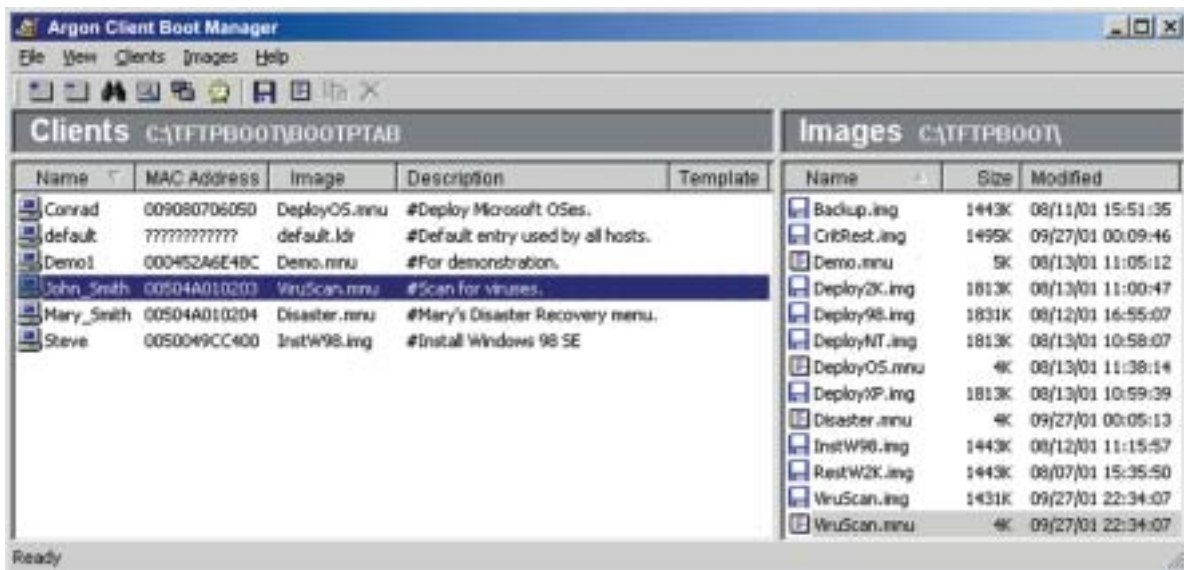



Figure 14: Client Boot Manager – Client and Images been added

Repeat Steps 8.1 and 8.2 to add all clients and assign the VirusScan.mnu boot menu file to them.

9. Turn on the client PC, make sure the boot ROM (e.g. MBA) is the first boot device (please refer to the PC's User Manual for how to setup boot order on the PC). The PC will boot from the boot ROM and download the boot image which contains the virus scan utility. When the boot image executes, it scans the PC's hard drives for viruses, logs the reports to the server, and then shuts down the PC upon finish.

## How to conduct an off-hours centralized virus scanning

CBM supports Remote Wake-Up (RWU) with a time scheduler, which allows system administrators to perform any centralized network boot task at any time (even at off-hours) without physically visiting the client PCs.

1. From the CBM window, select the clients to be woken up and scanned. Ensure that these clients are assigned to a proper boot image file or menu boot file. If it is assigned to a menu boot file, make certain the virus scanning image is the default one in the menu.
2. Click on the  icon on the CBM toolbar, or select "Wakeup..." from the "Clients" menu, a "Wakeup Selected Clients" dialog appears. See Figure 15.

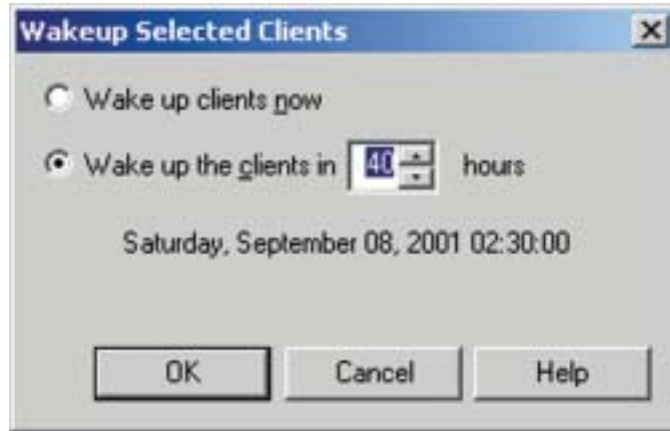


Figure 15: Wakeup Selected Clients

3. The selected client PCs can be woken up immediately, or scheduled at a later time that the administrator chooses (for example, at 2:30 a.m. on Saturday morning).
4. Once the client PCs were woken up, they download a menu boot file, in which the virus scanning boot image is set to default; or download the boot image.
5. The client PCs download the virus scanning boot image from the server and run the boot image.
6. The commands in the boot image check the client PCs' DOS accessible local drives for viruses, log the reports, and finally, shut down the PCs.

Virus scanning - and repair - can now be done without any human intervention at all when using your virus scanning tools together with CMS. If any new virus patterns are introduced, the administrator just needs to upgrade the virus scanning utility or virus patterns, or signature definition files on the server.

## Appendix: Sample Files

### CONFIG.SYS (for VIRUSCAN.IMG)

```
files=30
buffers=30
device=himem.sys /testmem:off
device=emm386.exe noems
dos=high,umb
lastdrive=z
device=net\ifshlp.sys
```

### AUTOEXEC.BAT (for VIRUSCAN.IMG)

```
bppatch -i net\protocol.ini net\system.ini net\tcputils.ini
cd net
call netstart.bat
cd\
call viruscan.bat
pboot /shutdown
```

### VIRUSCAN.BAT

```
@ECHO OFF
Path=A:\;A:\NET;
bppatch /s > setenv.bat
call setenv.bat
Z:
md \Log\%ha8% > NUL
```

```
Rem =====
Rem Syntax of F-PROT:
Rem F-PROT [drive,file,directory] [options]
Rem Options of F-PROT used in the example:
Rem /HARD Scan all files on all hard drives in the computer
Rem /AUTO Do not request the permission before removing each virus.
Rem This parameter works with /DISINF, /DELETE, or /RENAME
Rem /DISINF Disinfect whenever possible.
Rem /RENAME Rename infected COM/EXE files to VOM/VXE. If files with those
Rem extensions already exist, .VVV is used instead. Infected document
Rem files are not renamed.
Rem /DELETE Delete infected files.
Rem /DISINF /RENAME /DELETE together means: disinfect when possible, otherwise
Rem attempt to rename infected COM/EXE files to VOM/VXE, but if that
Rem fails the files are deleted.
Rem /ARCHIVE Scan inside .ZIP and .ARJ files. Support for .LZH and .RAR
Rem archives, as well as self-extracting archives may be added later.
Rem /APPEND Append the report to an an existing file (only used with /REPORT).
Rem /REPORT=X:\VirusRpt.log Send the output to a file, in addition to displaying it on the screen.
Rem /WRAP Wrap text so the report fits in 78 columns.
Rem /NOBREAK Disable ESC and Ctrl_C during scanning.
Rem =====

F-PROT /HARD /AUTO /DISINF /RENAME /DELETE /ARCHIVE /NOBREAK /REPORT=Z:\Log\%ha8%\Virus.Rpt /WRAP /APPEND

if errorlevel 8 goto suspicious
if errorlevel 7 goto NoMem
if errorlevel 6 goto Single
if errorlevel 5 goto CTRL_C
if errorlevel 4 goto Mvirus
if errorlevel 3 goto BFvirus
if errorlevel 2 goto selftest
```

```
if errorlevel 1 goto terminate
if errorlevel 0 goto success

goto end

:success
Echo End of virus scanning. No virus found.
goto end

:terminate
Echo Abnormal termination - unrecoverable error.
Echo This can mean any of the following:
Echo . Internal error in the program.
Echo . DOS version prior to 3.0 was used.
Echo . ENGLISH.TX0, SIGN.DEF or MACRO.DEF corrupted or not present.
goto end

:selftest
Echo Selftest failed - program has been modified.
goto end

:BFvirus
Echo A Boot/File virus infection found.
goto end

:Mvirus
Echo Virus found in memory.
goto end

:CTRL_C
Echo Program terminated with ^C or ESC.
goto end

:Single
Echo A virus was removed.
Echo This code is only meaningful if the program is used to scan just a single file.
goto end

:NoMem
Echo Insufficient memory to run the program.
goto end

:suspicious
Echo At least one suspicious file was found, but no infections.
goto end

:end
Echo.
Echo Virus scanning finished. The system will be shutdown.
```

Copyright 2002, Argon Technology Corporation. All rights reserved. Prices subject to change without notice. All pricing in US Dollars.

Argon and Client Management Services are trademarks and the Argon logo is a trademark of Argon Technology Corporation. All other company and product names may be trademarks of their respective companies.  
Argon Technology Corporation 7895 Tranmere Drive, Suite 201A, Mississauga, ON L5S 1V9 Canada. To learn more about Argon solutions, visit [www.ArgonTechnology.com](http://www.ArgonTechnology.com) or call (905) 673-9978 / Fax: (905) 673-9013