SIEMENS

SIMATIC

Process Control System PCS 7 Trend Micro Office Scan configuration V7.3 including Patch 2

Commissioning Manual

08/2009
A5E02634981-01

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

> ⚠DANGER
>
> indicates that death or severe personal injury **will** result if proper precautions are not taken.

> ⚠WARNING
>
> indicates that death or severe personal injury **may** result if proper precautions are not taken.

> ⚠CAUTION
>
> with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

> CAUTION
>
> without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

> NOTICE
>
> indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation for the specific task, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

> ⚠WARNING
>
> Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be adhered to. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E02634981-01
℗ 08/2009

Table of contents

1 Using virus scanners

1.1 Preface

Important information about this whitepaper

The compatibility of the virus scanners recommended for PCS 7 and WinCC has been tested with the systems. The recommended settings for these virus scanners have been chosen to ensure the reliable real time operation of PCS 7 is not adversely affected by the virus scanner software.

These recommendations describe how to discover and make effective as comprehensively as possible the currently known, best possible compromise between the target, virus and damage software, and ensure an as determinable as possible time response of the PCS 7 control system can be achieved in all operating phases.

If you choose different settings for the virus scanner, this could have negative effects on the real-time behavior.

Purpose of this documentation

This documentation describes the recommended settings for virus scanner software in combination with PCS 7 and WinCC following the virus scanner installation.

Required knowledge

This documentation is aimed at anyone who is involved in configuring, commissioning and operating automated systems based on SIMATIC PCS 7 or WinCC. Knowledge of administration and IT techniques for Microsoft Windows operating systems is assumed.

Validity of the documentation

The documentation applies to process control systems equipped with the respective product version of PCS 7 or WinCC.

NOTICE

Note that certain virus scanners are only approved for certain product versions.

Additional information is available in the Internet at the following address:

http://support.automation.siemens.com/WW/view/en/10154608

1.2 Using virus scanners

1.2.1 Introduction

Using virus scanners in a process control system is only effective when they are part of a comprehensive security concept. A virus scanner alone cannot protect a process control system against hostile attacks.

The security concept PCS 7 / WinCC is available on the Internet under:

http://support.automation.siemens.com

Virus scanners should comply with the requirements described in the security concepts of PCS 7 / WinCC.

1.2.2 Definitions and information

Basic principle

The use of a virus scanner should never inhibit a plant in runtime.

Virus scanners

A virus scanner is a software that detects, blocks or eliminates harmful program routines (computer viruses, worms, etc.).

Scan engine (scanner module)

The scan engine is a component of the virus scanner software that can examine data for harmful software.

Virus signature file (virus pattern file or virus definition file)

This file provides the virus signatures to the scan engine, which uses it to search through data for harmful software.

Virus scan client

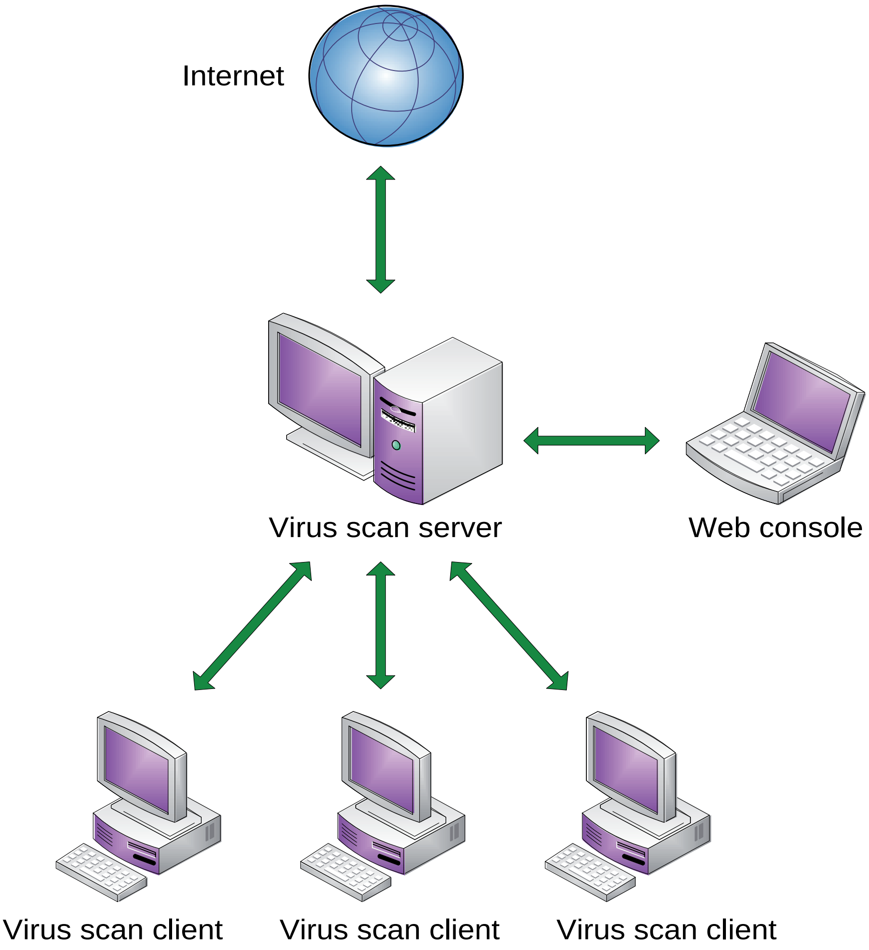
The virus scan client is a computer which is examined for viruses and managed by the virus server.

Virus scan server

The virus scan server is a computer which centrally manages virus scan clients, loads virus signature files and deploys them on the virus scan clients.

1.2.3 Principle structure of the virus scanner architecture

A virus scan server receives its virus signatures from the update server of the respective virus scan manufacturer in the Internet or from an upstream virus scan server and manages its virus scan clients.
Remote access to the virus scan server is available via web console.



1.2.4 Using antivirus software

Information for configuration of local virus scanners

- Integrated firewall of the virus scanner
  The local Windows firewall is used as of PCS 7 V7.0 and configured with the SIMATIC Security Control (SSC) component. The firewalls integrated in the virus scanners are therefore not installed.
- Manual scan (manual scan, on demand scan)
  A manual scan should never be performed on virus scan clients during process mode (runtime). This should take place at regular intervals, e.g. during maintenance, on all computers of the system.
- Automatic scan (auto-protect, on-access scanning)
  With automatic scanning, it is sufficient to check the incoming data traffic.
- Scheduled scan (planned search, on demand scan)
  A scheduled scan should never be performed on virus scan clients during process mode (runtime).
- Displaying messages
  To ensure that process mode is not inhibited, no messages should be displayed on the virus scan clients.
- Drives
  To avoid overlapping scanning of network drives, only local drives are scanned.
- E-mail scan
  Scanning of e-mail can be disabled except on the engineering station which receives e-mails.
- Division into groups
  Organize your virus scan clients in groups.
- Deployment of the virus signature (pattern update)
  The deployment of the virus signatures to the virus scan clients is performed by the upstream virus scan server. Test the virus signatures in a test system before deploying them in process mode to ensure that work correctly. Distribute the virus signatures manually to the respective groups.
- Update the virus scan engine
  Do not conduct the virus scan engine update in runtime as these updates will probably require you to restart the virus scan client.

Note on installation

The software installation must be carried out from a virus-free storage location (e.g. from a file server with its own virus scanner or from a certified DVD). During the software installation, automatic changes are often carried out in the operating system. An enabled virus scanner must not obstruct or falsify the software installation.

Configuration 2

2.1 Introduction

Only Corporate Edition V7.3 of the Trend Micro "OFFICE Scan" virus scanner has been approved for some versions of PCS 7. The settings described below that have changed in comparison to the standard version were tested for PCS7.

Approved virus scanners for the following PCS 7 versions

You can find the latest overview of the virus scanners authorized for a PCS 7 version at the following Internet address:
http://support.automation.siemens.com/WW/view/en/10154608

2.2 Integrated firewall

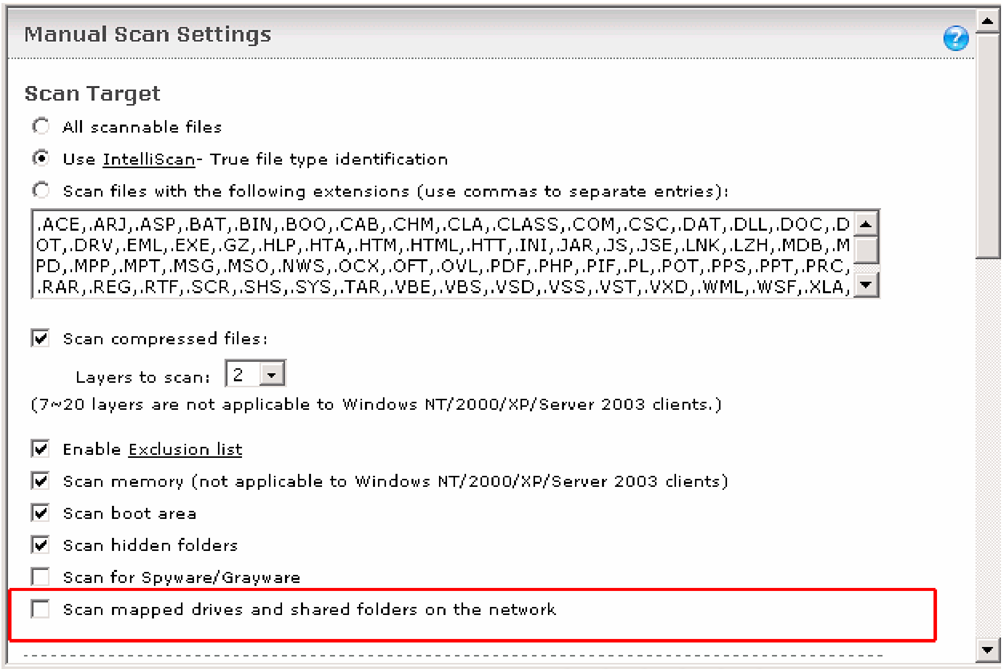
The "Install Enterprise Client Firewall" option can be disabled at the time of installation.

2.3 Manual search

Settings in the "Manual Scan Settings" dialog box

"Scan Target" area

- "Scan mapped drives and shared folders on the network" check box: **Disabled**



Manual Scan Settings

Scan Target

○ All scannable files

● Use IntelliScan- True file type identification

○ Scan files with the following extensions (use commas to separate entries):

.ACE,.ARJ,.ASP,.BAT,.BIN,.BOO,.CAB,.CHM,.CLA,.CLASS,.COM,.CSC,.DAT,.DLL,.DOC,.DOT,.DRV,.EML,.EXE,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JS,.JSE,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSO,.NWS,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.POT,.PPS,.PPT,.PRC,.RAR,.REG,.RTF,.SCR,.SHS,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.VXD,.WML,.WSF,.XLA,

☑ Scan compressed files:

Layers to scan: 2

(7~20 layers are not applicable to Windows NT/2000/XP/Server 2003 clients.)

☑ Enable Exclusion list

☑ Scan memory (not applicable to Windows NT/2000/XP/Server 2003 clients)

☑ Scan boot area

☑ Scan hidden folders

☐ Scan for Spyware/Grayware

☐ Scan mapped drives and shared folders on the network

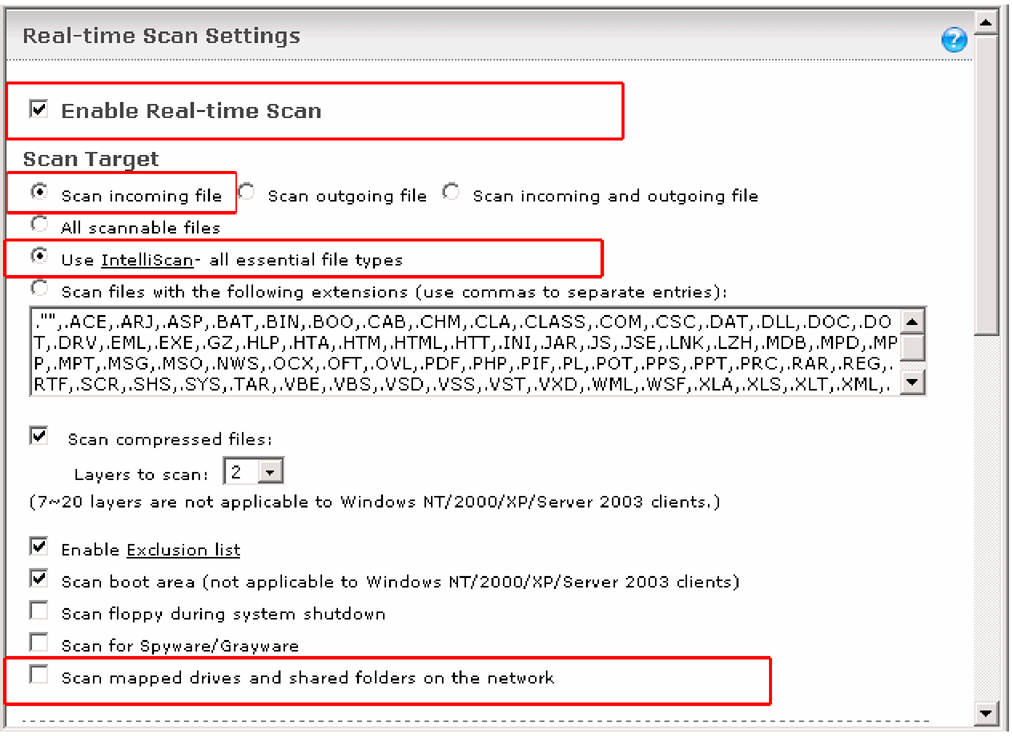
Figure 2-1 Dialog box "Manual Scan Settings"

2.4 Real-time Scan

Settings in the "Real-time Scan Settings" dialog box

"Scan Target" area

- Check box "Enable Real-time scan": **Enabled**
- "Scan Incoming File" check box: **Enabled**
- Option button "Use IntelliScan – Detect true file type": **Enabled**
- "Scan mapped drives and shared folders on the network" check box: **Disabled**



Real-time Scan Settings

☑ Enable Real-time Scan

Scan Target

● Scan incoming file ○ Scan outgoing file ○ Scan incoming and outgoing file

○ All scannable files

● Use IntelliScan- all essential file types

○ Scan files with the following extensions (use commas to separate entries):

."",.ACE,.ARJ,.ASP,.BAT,.BIN,.BOO,.CAB,.CHM,.CLA,.CLASS,.COM,.CSC,.DAT,.DLL,.DOC,.DOT,.DRV,.EML,.EXE,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JS,.JSE,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSO,.NWS,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.POT,.PPS,.PPT,.PRC,.RAR,.REG,.RTF,.SCR,.SHS,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.VXD,.WML,.WSF,.XLA,.XLS,.XLT,.XML,.

☑ Scan compressed files:

Layers to scan: 2

(7~20 layers are not applicable to Windows NT/2000/XP/Server 2003 clients.)

☑ Enable Exclusion list

☑ Scan boot area (not applicable to Windows NT/2000/XP/Server 2003 clients)

☐ Scan floppy during system shutdown

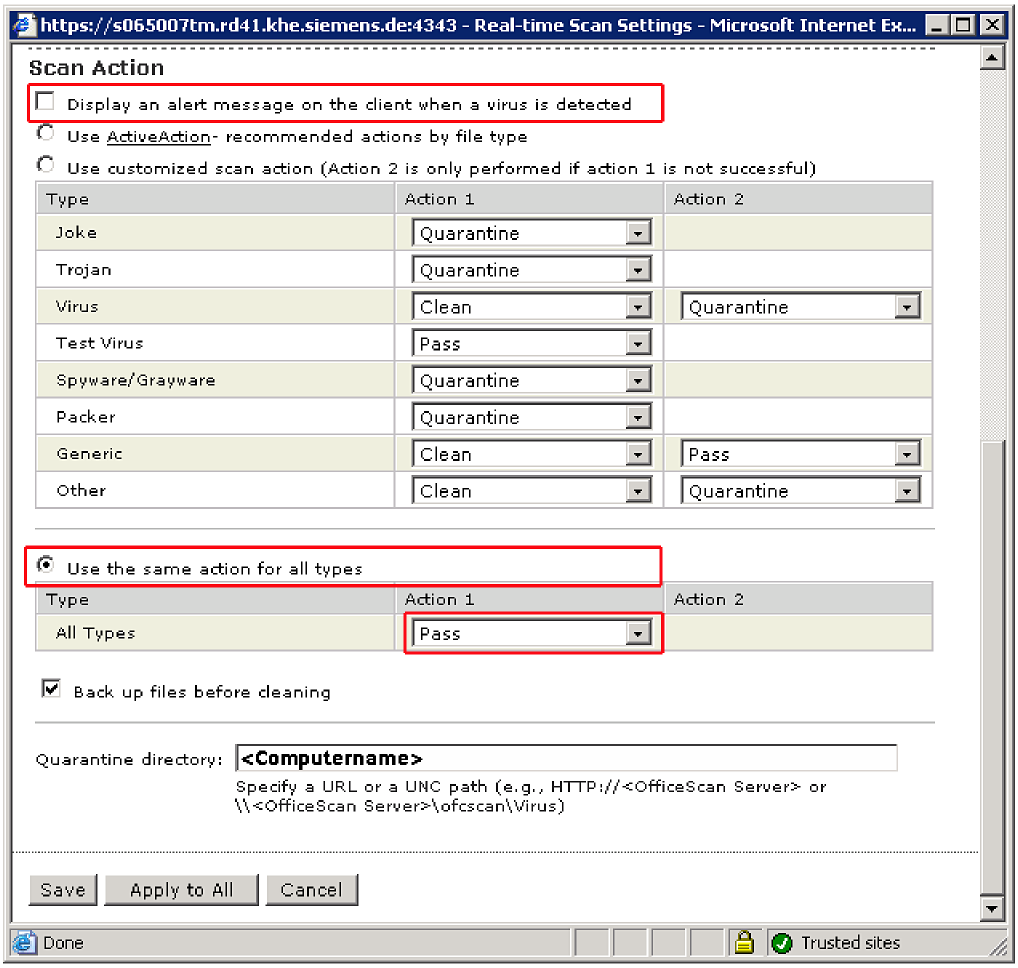
☐ Scan for Spyware/Grayware

☐ Scan mapped drives and shared folders on the network

Figure 2-2 "Real-time Scan Settings" dialog box: Figure 1 of 2

"Scan Action" area

- "Display an alert message on the client when a virus is detected" check box: **Disabled**
- "Use the same action for all types" check box: Enabled;
  Setting selected for the "All Types" type in the "Action1" column: **Pass**



https://s065007tm.rd41.khe.siemens.de:4343 - Real-time Scan Settings - Microsoft Internet Ex...

Scan Action

□ Display an alert message on the client when a virus is detected

○ Use ActiveAction- recommended actions by file type

○ Use customized scan action (Action 2 is only performed if action 1 is not successful)

Type	Action 1	Action 2
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Spyware/Grayware	Quarantine	
Packer	Quarantine	
Generic	Clean	Pass
Other	Clean	Quarantine

● Use the same action for all types

Type	Action 1	Action 2
All Types	Pass	

☑ Back up files before cleaning

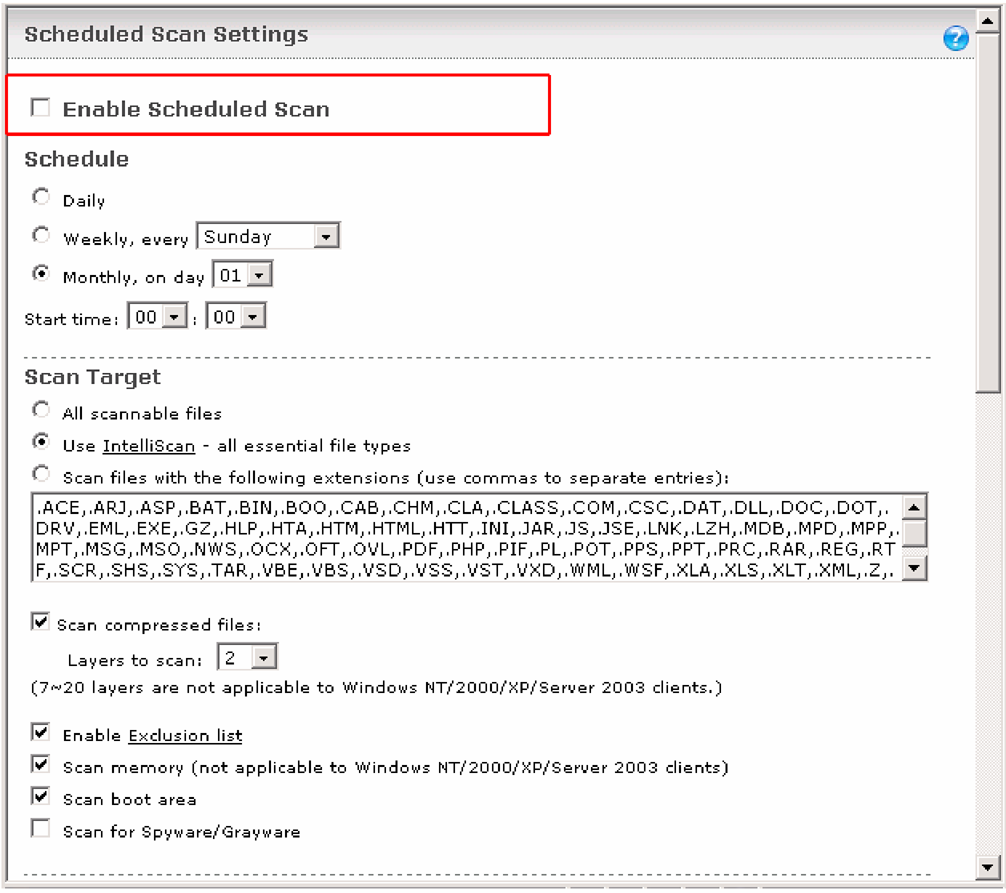
Quarantine directory: <Computername>
Specify a URL or a UNC path (e.g., HTTP://<OfficeScan Server> or \\<OfficeScan Server>\ofcscan\Virus)

Figure 2-3 "Real-time Scan Settings" dialog box: Figure 2 of 2

2.5 Scheduled Scan

The "Enable Scheduled Scan" check box must be disabled during runtime for PC stations operating in process mode (runtime).

- Check box "Enable Scheduled Scan": **Disabled**



Scheduled Scan Settings

□ Enable Scheduled Scan

Schedule

○ Daily

○ Weekly, every Sunday

● Monthly, on day 01

Start time: 00 : 00

Scan Target

○ All scannable files

● Use IntelliScan - all essential file types

○ Scan files with the following extensions (use commas to separate entries):

.ACE,.ARJ,.ASP,.BAT,.BIN,.BOO,.CAB,.CHM,.CLA,.CLASS,.COM,.CSC,.DAT,.DLL,.DOC,.DOT,.DRV,.EML,.EXE,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JS,.JSE,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSO,.NWS,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.POT,.PPS,.PPT,.PRC,.RAR,.REG,.RTF,.SCR,.SHS,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.VXD,.WML,.WSF,.XLA,.XLS,.XLT,.XML,.Z,.

☑ Scan compressed files:

Layers to scan: 2

(7~20 layers are not applicable to Windows NT/2000/XP/Server 2003 clients.)

☑ Enable Exclusion list

☑ Scan memory (not applicable to Windows NT/2000/XP/Server 2003 clients)

☑ Scan boot area

□ Scan for Spyware/Grayware

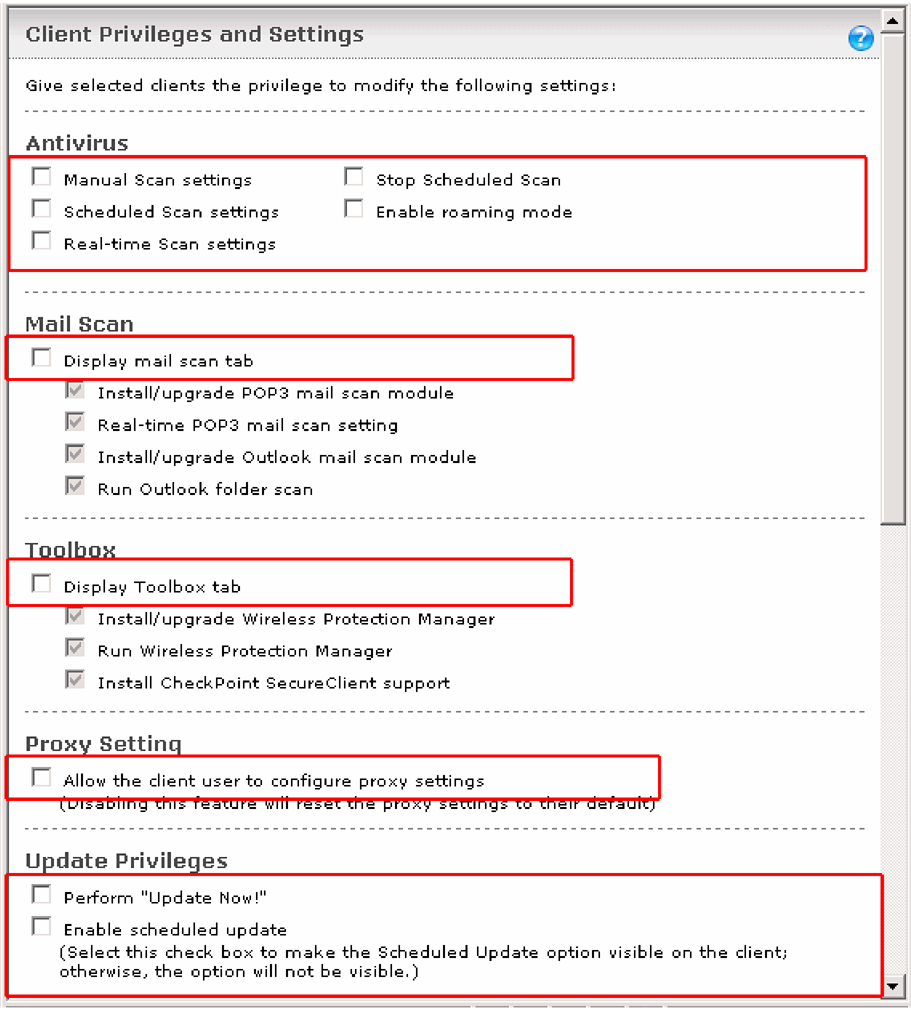
Figure 2-4 Dialog box "Scheduled search settings"

2.6 Client Privileges and Settings

Setting in the "Client Privileges and Settings" dialog box

The following areas must be disabled:
"Antivirus", "Mail Scan", "Toolbox", "Proxy Settings" and "Update Privileges"

- "Display **Mail Scan** tab" check box: **Disabled**
- "Display **Toolbox** tab" check box: **Disabled**
- "Allow the client user to configure proxy settings" check box: **Disabled**
- "Perform 'Update Now!'" check box: **Disabled**
- "Enable scheduled update" check box: **Disabled**



Client Privileges and Settings

Give selected clients the privilege to modify the following settings:

Antivirus

□ Manual Scan settings
□ Scheduled Scan settings
□ Real-time Scan settings
□ Stop Scheduled Scan
□ Enable roaming mode

Mail Scan

□ Display mail scan tab
☑ Install/upgrade POP3 mail scan module
☑ Real-time POP3 mail scan setting
☑ Install/upgrade Outlook mail scan module
☑ Run Outlook folder scan

Toolbox

□ Display Toolbox tab
☑ Install/upgrade Wireless Protection Manager
☑ Run Wireless Protection Manager
☑ Install CheckPoint SecureClient support

Proxy Setting

□ Allow the client user to configure proxy settings
(Disabling this feature will reset the proxy settings to their default)

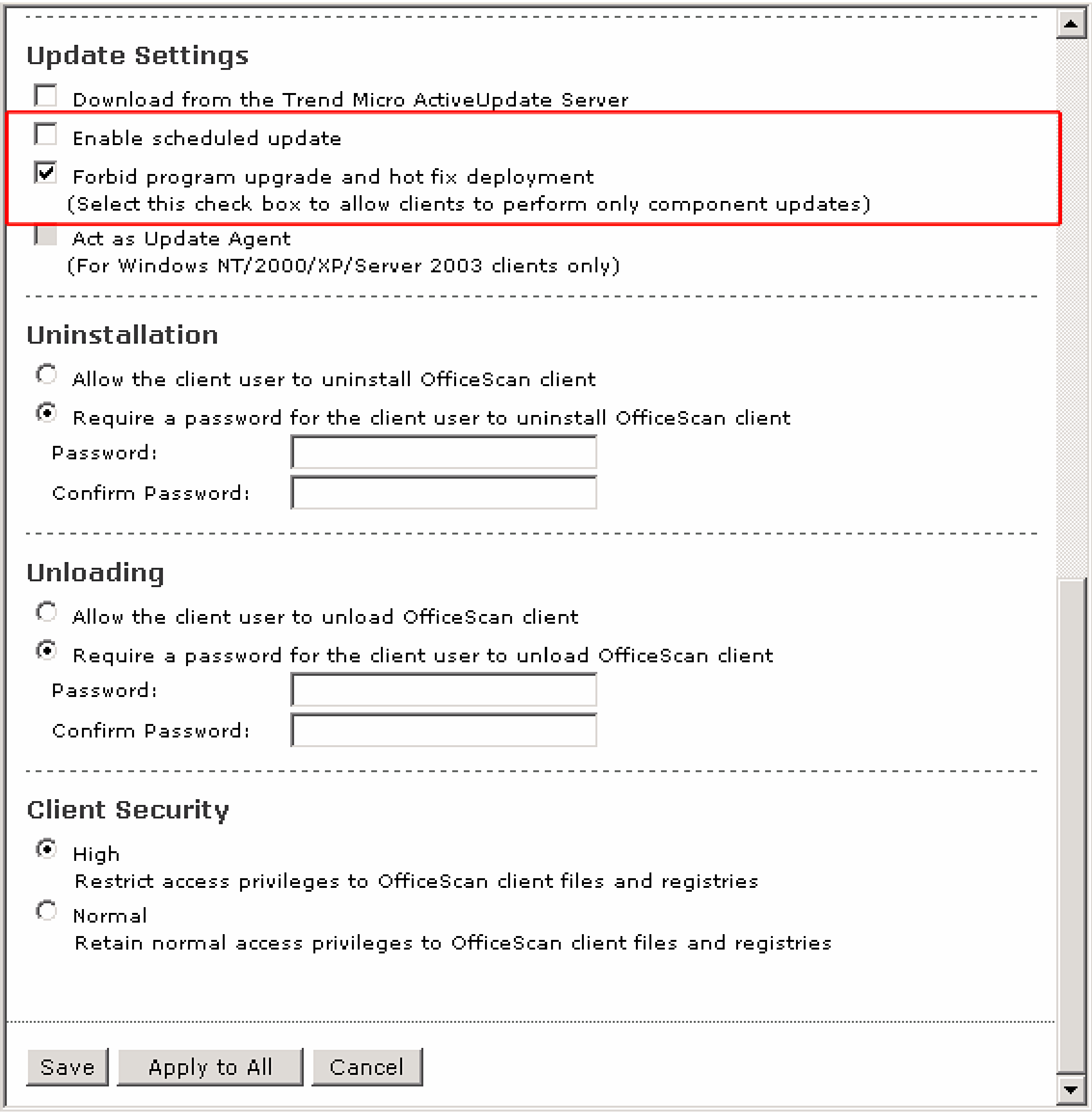
Update Privileges

□ Perform "Update Now!"
□ Enable scheduled update
(Select this check box to make the Scheduled Update option visible on the client; otherwise, the option will not be visible.)

Figure 2-5 "Client Privileges and Settings" dialog box: Figure 1 of 2

"Update settings" area

- Check box "Enable Scheduled Update": **Disabled**
- Check box "Forbid program upgrade and hot fix deployment": **Enabled**



Update Settings

□ Download from the Trend Micro ActiveUpdate Server

□ Enable scheduled update

☑ Forbid program upgrade and hot fix deployment
(Select this check box to allow clients to perform only component updates)

□ Act as Update Agent
(For Windows NT/2000/XP/Server 2003 clients only)

Uninstallation

○ Allow the client user to uninstall OfficeScan client

● Require a password for the client user to uninstall OfficeScan client

Password:

Confirm Password:

Unloading

○ Allow the client user to unload OfficeScan client

● Require a password for the client user to unload OfficeScan client

Password:

Confirm Password:

Client Security

● High
Restrict access privileges to OfficeScan client files and registries

○ Normal
Retain normal access privileges to OfficeScan client files and registries

Figure 2-6 "Client Privileges and Settings" dialog box: Figure 2 of 2

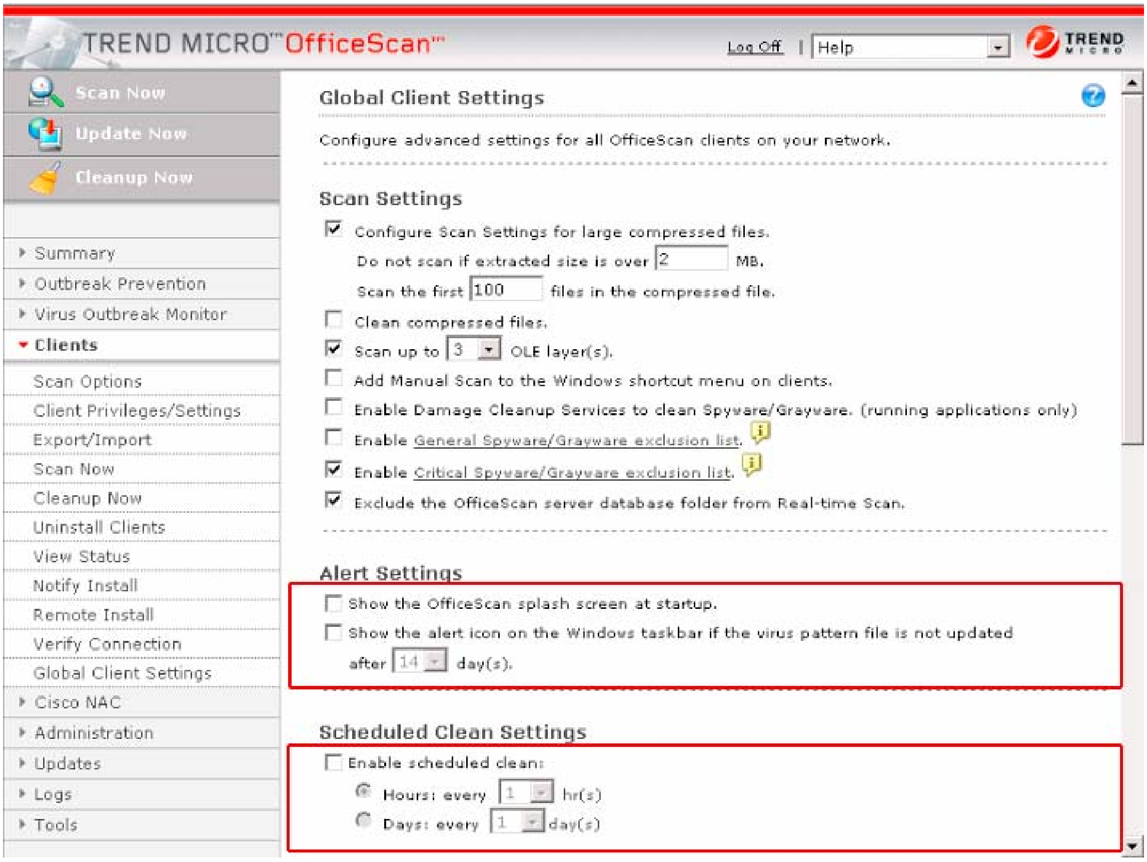
2.7 Global Client Settings

Settings in the "Global Client Settings" dialog box

The global settings relate to all virus scan clients registered on the virus scan server.

"Alert Settings" area

- "Show the OfficeScan splash screen at startup" check box: Disabled
- Check box "Show the alert icon on the Windows taskbar if …": Disabled



Global Client Settings

Configure advanced settings for all OfficeScan clients on your network.

Scan Settings

☑ Configure Scan Settings for large compressed files.
Do not scan if extracted size is over 2 MB.
Scan the first 100 files in the compressed file.
☐ Clean compressed files.
☑ Scan up to 3 OLE layer(s).
☐ Add Manual Scan to the Windows shortcut menu on clients.
☐ Enable Damage Cleanup Services to clean Spyware/Grayware. (running applications only)
☐ Enable General Spyware/Grayware exclusion list.
☑ Enable Critical Spyware/Grayware exclusion list.
☑ Exclude the OfficeScan server database folder from Real-time Scan.

Alert Settings

☐ Show the OfficeScan splash screen at startup.
☐ Show the alert icon on the Windows taskbar if the virus pattern file is not updated after 14 day(s).

Scheduled Clean Settings

☐ Enable scheduled clean:
● Hours: every 1 hr(s)
○ Days: every 1 day(s)

Figure 2-7 Dialog box "General client settings"

2.8 Client Update

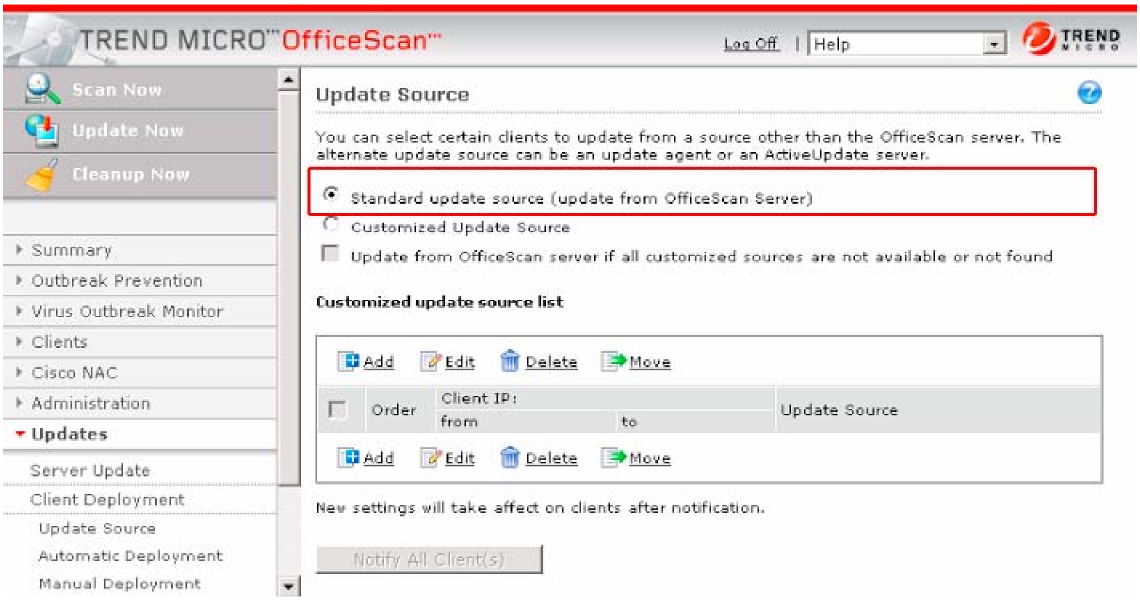
Information on updates

Do not perform an update of the virus scan engine in process mode (runtime) because some updates require a reboot of the virus scan client.

Settings in the "Client Update" dialog box

"Update Source" area

- Option button "Standard update source (update from Office Server)": Enabled



Update Source

You can select certain clients to update from a source other than the OfficeScan server. The alternate update source can be an update agent or an ActiveUpdate server.

● Standard update source (update from OfficeScan Server)
○ Customized Update Source
□ Update from OfficeScan server if all customized sources are not available or not found

Customized update source list

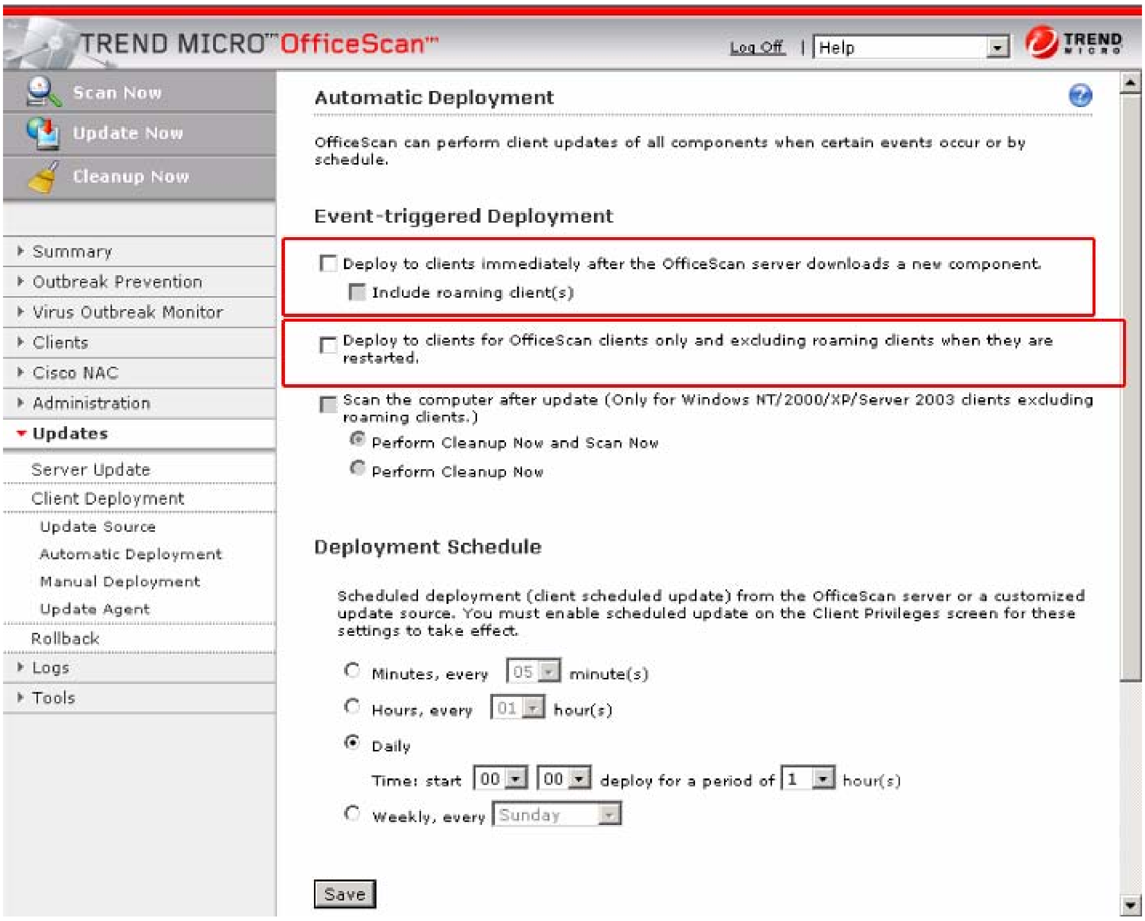
□	Order	Client IP: from	to	Update Source

New settings will take affect on clients after notification.

Figure 2-8 "Client Update" dialog box: "Update Source" area

"Automatic Deployment" area

- "Deploy to clients immediately after OfficeScan server downloads a new component" check box: Disabled
- "Deploy to clients for OfficeScan clients only and excluding rooming clients when they are restarted)" check box: Disabled



Automatic Deployment

OfficeScan can perform client updates of all components when certain events occur or by schedule.

Event-triggered Deployment

☐ Deploy to clients immediately after the OfficeScan server downloads a new component.

☐ Include roaming client(s)

☐ Deploy to clients for OfficeScan clients only and excluding roaming clients when they are restarted.

☐ Scan the computer after update (Only for Windows NT/2000/XP/Server 2003 clients excluding roaming clients.)

● Perform Cleanup Now and Scan Now

○ Perform Cleanup Now

Deployment Schedule

Scheduled deployment (client scheduled update) from the OfficeScan server or a customized update source. You must enable scheduled update on the Client Privileges screen for these settings to take effect.

○ Minutes, every 05 minute(s)

○ Hours, every 01 hour(s)

● Daily

Time: start 00 00 deploy for a period of 1 hour(s)

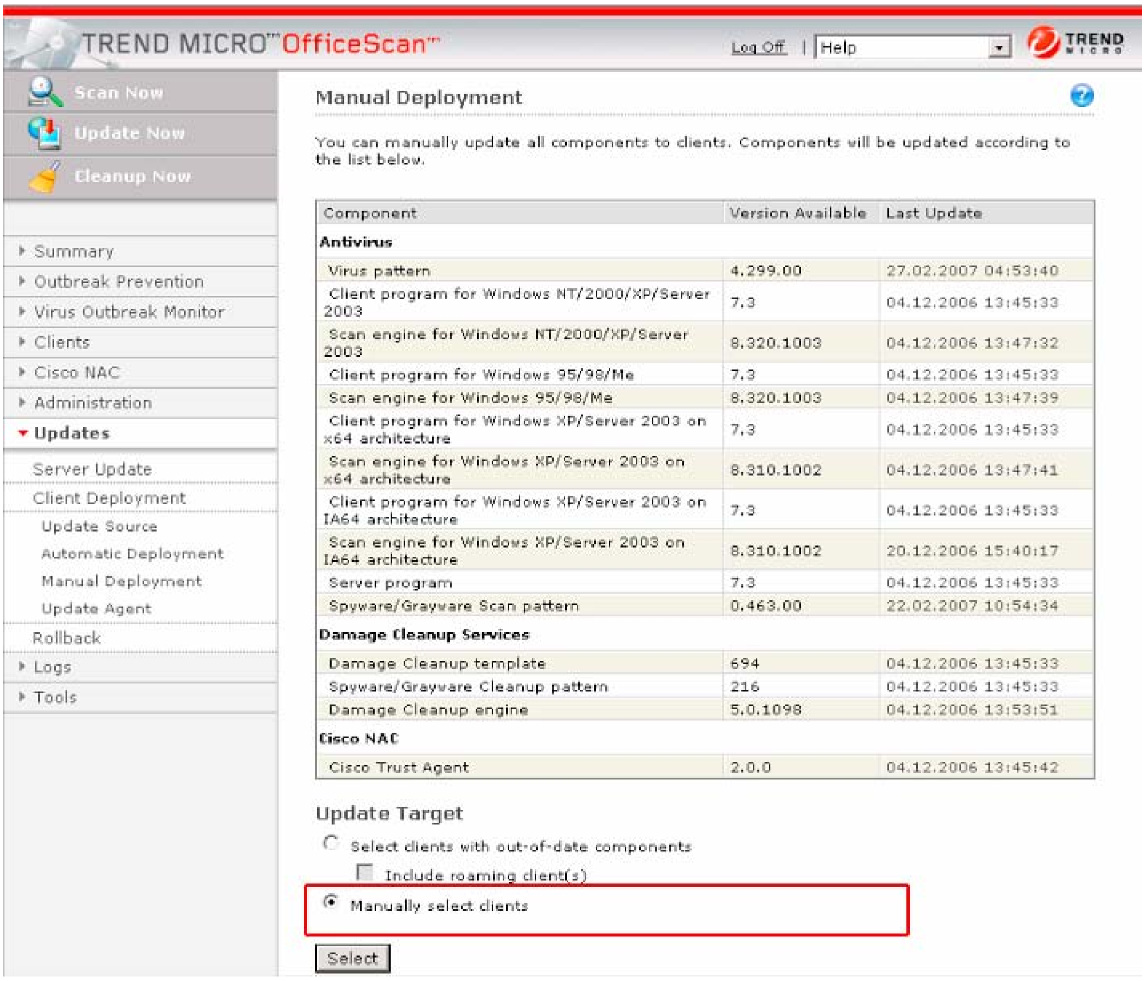
○ Weekly, every Sunday

Save

Figure 2-9 "Client Update" dialog box: "Automatic Deployment" area

"Manual Deployment" area

- Option button "Manually select clients": **Enabled**



Manual Deployment

You can manually update all components to clients. Components will be updated according to the list below.

Component	Version Available	Last Update
Antivirus		
Virus pattern	4.299.00	27.02.2007 04:53:40
Client program for Windows NT/2000/XP/Server 2003	7.3	04.12.2006 13:45:33
Scan engine for Windows NT/2000/XP/Server 2003	8.320.1003	04.12.2006 13:47:32
Client program for Windows 95/98/Me	7.3	04.12.2006 13:45:33
Scan engine for Windows 95/98/Me	8.320.1003	04.12.2006 13:47:39
Client program for Windows XP/Server 2003 on x64 architecture	7.3	04.12.2006 13:45:33
Scan engine for Windows XP/Server 2003 on x64 architecture	8.310.1002	04.12.2006 13:47:41
Client program for Windows XP/Server 2003 on IA64 architecture	7.3	04.12.2006 13:45:33
Scan engine for Windows XP/Server 2003 on IA64 architecture	8.310.1002	20.12.2006 15:40:17
Server program	7.3	04.12.2006 13:45:33
Spyware/Grayware Scan pattern	0.463.00	22.02.2007 10:54:34
Damage Cleanup Services		
Damage Cleanup template	694	04.12.2006 13:45:33
Spyware/Grayware Cleanup pattern	216	04.12.2006 13:45:33
Damage Cleanup engine	5.0.1098	04.12.2006 13:53:51
Cisco NAC		
Cisco Trust Agent	2.0.0	04.12.2006 13:45:42

Update Target

○ Select clients with out-of-date components

□ Include roaming client(s)

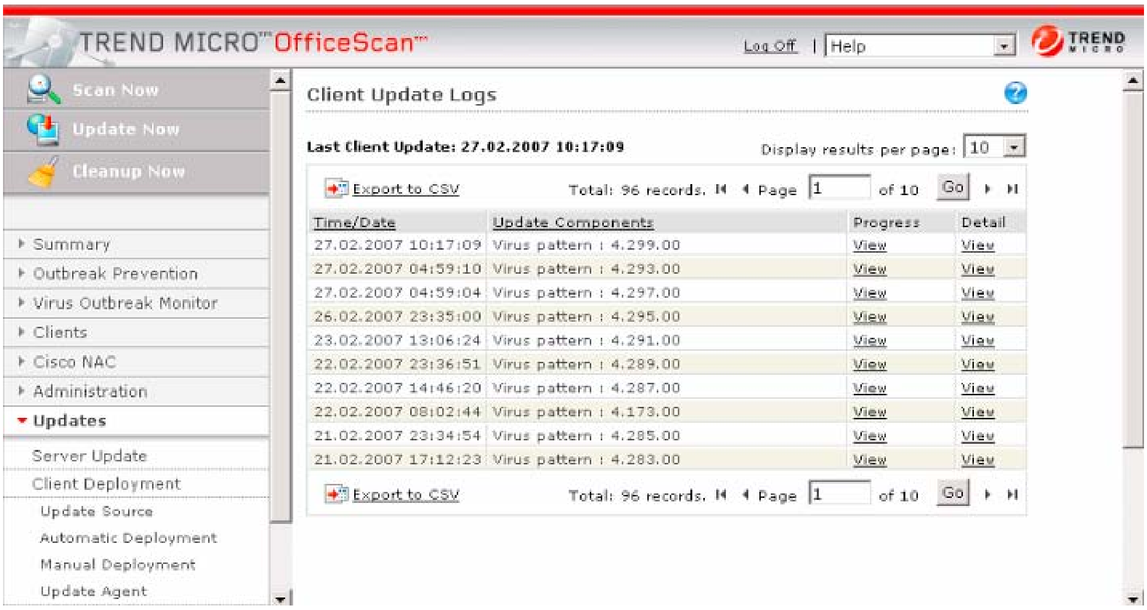
● Manually select clients

Select

Figure 2-10 "Client Update" dialog box: "Manual Deployment" area

2.9 Logs

Check the deployment of the virus signatures in the dialog box "Client update logs"



Client Update Logs

Last Client Update: 27.02.2007 10:17:09

Display results per page: 10

Total: 96 records. Page 1 of 10

Time/Date	Update Components	Progress	Detail
27.02.2007 10:17:09	Virus pattern : 4.299.00	View	View
27.02.2007 04:59:10	Virus pattern : 4.293.00	View	View
27.02.2007 04:59:04	Virus pattern : 4.297.00	View	View
26.02.2007 23:35:00	Virus pattern : 4.295.00	View	View
23.02.2007 13:06:24	Virus pattern : 4.291.00	View	View
22.02.2007 23:36:51	Virus pattern : 4.289.00	View	View
22.02.2007 14:46:20	Virus pattern : 4.287.00	View	View
22.02.2007 08:02:44	Virus pattern : 4.173.00	View	View
21.02.2007 23:34:54	Virus pattern : 4.285.00	View	View
21.02.2007 17:12:23	Virus pattern : 4.283.00	View	View

Total: 96 records. Page 1 of 10

Figure 2-11 "Client Update Logs" dialog box