



6.0 ServerProtect™

Patch 1

Getting Started Guide

Comprehensive server and storage virus protection

for Storage



Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<https://docs.trendmicro.com/en-us/enterprise/serverprotect.aspx>

Trend Micro, the Trend Micro t-ball logo, ServerProtect, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2022. Trend Micro Incorporated. All rights reserved.

Document Part No.: SPEM56439/140521

Release Date: February 2022

Protected by U.S. Patent No.: 5,951,698

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<https://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro ServerProtect collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

Table of Contents

Chapter 1: Getting Started with Trend Micro ServerProtect

Introduction to Trend Micro ServerProtect	1-2
How Does ServerProtect Work	1-2
How Does ServerProtect Manage Servers	1-3
Communication Methods	1-3
ServerProtect Architecture	1-4
The Management Console	1-4
The Information Server	1-5
Information Server Tips	1-5
The Normal Server	1-6
ServerProtect Domains	1-7
ServerProtect for Storage Architecture Overview	1-8
ServerProtect for Storage with RPC Scanner	1-8
Product Architecture in 7-Mode	1-8
Product Architecture in Cluster-Mode	1-9
Organizational Overview	1-11
ServerProtect for Storage with EMC CAVA Scanner Architecture Overview	1-12
Organizational Overview	1-15
Specific Functions for EMC VNX/VNXe	1-16
ServerProtect for Storage with ICAP Scanner	1-16
Scan Actions	1-17
Deployment	1-17
Real-time Scan Versus On-demand Scan (Scan Now)	1-18
Working with Tasks	1-19
When ServerProtect Finds a Virus (Virus Actions)	1-20
Virus Logs	1-22
Deploying Updates	1-23
ServerProtect Virus Detection Technology	1-24
Pattern Matching	1-24

MacroTrap	1-25
How MacroTrap Works	1-25
Compressed Files	1-26
Damage Cleanup Services	1-27
OLE Layer Scan	1-27
IntelliScan	1-28
ActiveAction	1-28
When to Select ActiveAction	1-28
Mapped Network Drive Scan	1-29
Additional Features	1-29
Centralized Management	1-30
Enhanced Network Security on Installation	1-30
Swift Response to Virus Outbreaks	1-30
Flexible Control over Infected Files	1-30
NetworkTrap Tool	1-30
State-of-the-Art Virus Detection Technology	1-31
Viewable Scanning Statistics	1-31
Compatibility	1-31

Chapter 2: Installing ServerProtect for Storage

System Requirements	2-2
Normal Server	2-2
Information Server	2-3
Management Console	2-4
VMWare	2-6
Hyper-Visor	2-6
Storage Devices	2-6
Installation Scenarios	2-7
Specifying Your Installation Environment	2-7
Firewall Setting for ServerProtect Components	2-10
Managing ServerProtect Across a Wide Area Network ...	2-11
Installing ServerProtect	2-12
Before Installing ServerProtect	2-12
Installing the Complete ServerProtect Package	2-12
Installing an Information Server	2-17

Installing the Management Console	2-20
Installing a Normal Server	2-23
Installing a Normal Server from the Setup Program	2-23
Installing a Normal Server from the Management Console	2-27
Installing ServerProtect in Silent Mode	2-28
Installing ServerProtect for Storage with RPC Scanner or ICAP Scanner	2-31
Installing ServerProtect for Storage with EMC CAVA Scanner	2-31
Before Installing ServerProtect for Storage with EMC CAVA Scanner	2-32
Installing ServerProtect for Storage with EMC CAVA Scanner	2-32
Removing ServerProtect	2-33
Removing a Normal Server	2-33
Removing an Information Server	2-34
Removing the Management Console	2-34

Chapter 3: Managing ServerProtect

Using the Management Console	3-3
Opening the Management Console	3-3
The Main Window View of the Management Console	3-4
Main Menu	3-5
Side Bar	3-6
Domain Browser Tree	3-8
Configuration Area	3-10
Managing ServerProtect Domains	3-10
Creating ServerProtect Domains	3-11
Renaming ServerProtect Domains	3-13
Deleting ServerProtect Domains	3-14
Moving Normal Servers between Domains	3-14
Managing Information Servers	3-14
Selecting Information Servers	3-15

Managing Normal Servers	3-16
Moving a Normal Server between Domains	3-17
Moving a Normal Server between Information Servers ..	3-17
Managing NetApp Devices in Scan Server	3-17
Adding a NetApp 7-Mode Device	3-18
Adding a Cluster-Mode AV Connector	3-19
Using Multiple Scan Servers for Single NetApp Devices .	3-21
Removing a NetApp 7-Mode Device or Cluster-Mode AV Connector from Scan Server	3-22
Configuring NetApp 7-Mode Device or Cluster-Mode AV Connector Options	3-22
Updating NetApp 7-Mode Device or Cluster-Mode AV Connector Information	3-22
Using Scan Servers as Normal Servers	3-24
Notifying NetApp Device clients upon infection	3-25
Viewing the status of a NetApp Device	3-26
Configuring NetApp Device RPC Connection Status Notifications	3-27
Notifying NetApp Devices of New Update Components	3-28
Managing ICAP Client List in Scan Server	3-29
Accepting a Scan Request from ICAP Clients	3-29
Adding an ICAP Client to ICAP Client List	3-30
Removing an ICAP Client or IP Range from ICAP Client List	3-30
Configuring Updates	3-31
Update Components	3-31
How Updates Work	3-32
Verifying the Current Version of Files	3-33
Downloading Updates	3-34
Configuring a Download Source	3-34
Setting Trend Micro Update Server as the Download Source	3-34
Setting a Local or Network Drive as the Download Source	3-35

Creating a Download Source Folder	3-36
Using Download Now	3-36
Configuring a Scheduled Download	3-37
Configuring Download Settings	3-39
Configuring the Download Settings	3-39
Configuring the Proxy Server Settings	3-40
Deploying Updates	3-42
Configuring Deploy Now	3-42
Configuring a Scheduled Deployment	3-44
Rolling Back the Previous Deployment Action	3-45
Managing Tasks	3-47
ServerProtect Task Wizard	3-48
Default Tasks	3-50
Creating Tasks	3-50
Creating a Task	3-50
Creating a Scheduled Task	3-52
Specifying a Target for Scan Now	3-54
Creating a Default Task	3-55
Opening the Existing Task List	3-56
Running an Existing Task	3-58
Modifying Existing Tasks	3-58
Modifying an Existing Task	3-58
Modifying a Target Server for an Existing Task	3-59
Modifying a Task Definition for an Existing Task	3-60
Viewing an Existing Task	3-62
Removing an Existing Task	3-64
Configuring Notification Messages	3-64
Standard Alerts	3-64
Notification Events	3-65
Configuring a Standard Alert	3-65
Outbreak Alerts	3-66
Configuring an Outbreak Alert	3-67
Setting Alert Methods	3-69
Configuring an Alert to be Sent by Internet Mail	3-69

Scanning Viruses for Normal Server	3-71
Defining Actions Against Viruses	3-73
Scanning Profiles	3-75
Saving a Scanning Profile	3-75
Deleting a Scanning Profile	3-76
Scanning Viruses for Storage Devices	3-77
Defining Actions Against Viruses in RPC Scanner and EMC CAVA Scanner	3-78
Defining Actions Against Viruses in ICAP Scanner	3-79
Using Real-Time Scan	3-80
Configuring Real-Time Scan	3-81
Using Scan Now (Manual Scan)	3-84
Configuring Scan Now	3-85
Running the Scan Now Tool on Windows Normal Servers 3-88	
Running the Scan Now Tool	3-89
Stopping the Scan Now Tool	3-89
Scheduled Scanning	3-90
Configuring a Scheduled Scan	3-90
Using RPC Scanner	3-91
Configuring RPC Scanner	3-91
Duplicating RPC Scanner Configuration	3-92
Using EMC CAVA Scanner	3-94
Configuring EMC CAVA Scanner	3-94
Duplicating EMC CAVA Scanner Configuration	3-97
Using ICAP Scanner	3-98
Configuring ICAP Scanner	3-98
Duplicating ICAP Scanner Configuration	3-100
Selecting File Types to Scan	3-101
Supported File Extensions for Scanning	3-103
Excluding a File Extension from Scanning	3-105

Chapter 4: Upgrading Existing ServerProtect

Overview of ServerProtect Upgrade Feature	4-2
Use the Installation Package to Upgrade ServerProtect Locally	4-3
Use the Installation Package to Upgrade ServerProtect Remotely	4-4
Perform a Silent Mode Installation to Upgrade the Normal Servers	4-5
Installing ServerProtect in Silent Mode	4-5
Upgrading ServerProtect for NetApp or EMC Celerra	4-8
Upgrading the ServerProtect Evaluation Copy	4-9
Troubleshooting ServerProtect for Storage with RPC Scanner	4-9

Chapter 5: Managing ServerProtect with Trend Micro Control Manager

Control Manager Integration Summary	5-2
Registering With Trend Micro Control Manager	5-3
Verifying ServerProtect status in Control Manager	5-6
Unregistering from Control Manager	5-6

Chapter 6: Technical Support

Troubleshooting Resources	6-2
Using the Support Portal	6-2
Threat Encyclopedia	6-2
Contacting Trend Micro	6-3
Speeding Up the Support Call	6-3
Sending Suspicious Content to Trend Micro	6-4
Email Reputation Services	6-4
File Reputation Services	6-4
Web Reputation Services	6-5

Other Resources	6-5
Download Center	6-5
Documentation Feedback	6-5

Appendix A: Converting the ServerProtect Trial Version

The Software Evaluation Period Window	A-2
Viewing the Serial Number List	A-2
Updating a Serial Number	A-4
Frequently Asked Questions (FAQs)	A-5
Virus Scan for NetApp Device	A-5
Upgrading ServerProtect	A-5
ServerProtect Virus Scan	A-6
Miscellaneous	A-7

Index

Index	IN-1
-------------	------

Chapter 1

Getting Started with Trend Micro™ ServerProtect™

The topics included in this chapter are:

- *Introduction to Trend Micro™ ServerProtect™ on page 1-2*
- *How Does ServerProtect Work on page 1-2*
- *ServerProtect Architecture on page 1-4*
- *Real-time Scan Versus On-demand Scan (Scan Now) on page 1-18*
- *Working with Tasks on page 1-19*
- *When ServerProtect Finds a Virus (Virus Actions) on page 1-20*
- *Virus Logs on page 1-22*
- *Deploying Updates on page 1-23*
- *ServerProtect Virus Detection Technology on page 1-24*
- *Additional Features on page 1-29*

Introduction to Trend Micro™ ServerProtect™

Trend Micro™ ServerProtect™ is the latest generation of award-winning software for protecting file servers on corporate networks. It is designed specifically to protect the entire network from viruses of any kind by adopting advanced virus-catching technology to ensure that your network stays virus-free. ServerProtect detects new file infections, identifies viruses in existing files, and detects activity indicating an “unknown” virus may have entered the network environment on either the server or workstation.

ServerProtect enables network administrators to manage multiple Microsoft Windows and Novell NetWare network servers from a single portable management console. The console enables administrators to configure servers in the same domain simultaneously and to generate integrated virus incident reports from all of them.

By giving administrators a means to configure, monitor, and maintain antivirus efforts through the ServerProtect Management Console, ServerProtect improves and simplifies the implementation of corporate virus policy. This results in lower virus protection costs.

Trend Micro ServerProtect for Storage is an enhanced version of ServerProtect developed exclusively to provide antivirus solutions for NetApp devices, EMC Celerra, VNX/VNXe series and storage devices supporting ICAP antivirus scanner.

How Does ServerProtect Work

ServerProtect monitors all activity in a file server network. Whenever ServerProtect detects that a file in its domain is being accessed, it checks the file for infection.

If it finds that the file is infected, it sends notification messages to pre-defined recipients and takes action on the virus according to the ServerProtect configuration. The ServerProtect activity log records all the activities of the system.

ServerProtect allows you to design personal scanning profiles—saving you from having to re-configure frequently needed settings. You can even assign

multiple scanning options to a profile and use the profile for special circumstances, for example: scanning incoming files only.

How Does ServerProtect Manage Servers

ServerProtect secures your client/server network using a three-tier architecture: the Management Console, the Information Server (middleware), and the Normal Server.

Together, these components create a powerful, centrally managed, cost-effective antivirus security system.

The Management Console provides a user-friendly, Windows-based interface for configuring system components. Management Console instructions are sent to the Information Server, which then passes them on to the Normal Servers.

Communication Methods

The Management Console uses Transmission Control Protocol/Internet Protocol (TCP/IP) with a password-protected logon to communicate with the Information Server. The Information Server uses a remote Procedure Call (RPC) to connect to Windows or the NetWare Normal Servers.

ServerProtect Architecture

ServerProtect protects networks through a three-tier architecture: the Management Console, the Information Server, and the Normal Server. The following illustrates the relationship between these three components:

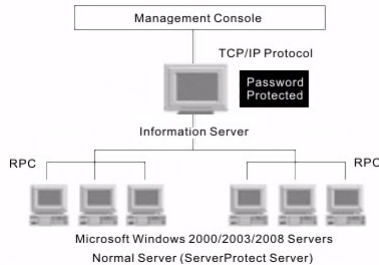


FIGURE 1-1. ServerProtect Three-tier Architecture

The Management Console

The ServerProtect Management Console is a portable console which gives network administrators centralized control of multiple network servers and domains. The console enables you to simultaneously configure Normal Servers in a specified domain and generate integrated virus incident reports for them. The Management Console has the following parts:

- Main menu
- Side bar (Shortcut bar)
- ServerProtect domain browser tree
- Configuration area

The ServerProtect domain browser tree shows all the ServerProtect Normal Servers in the domain, the status information of each server including the version of the virus pattern, the version of the scan engine file, type and that of the operating system, data flow direction of real-time scanning and others. Note that the administrator can configure how all this data is displayed.

**Tip**

You can use the Management Console to remotely install one or more Normal Servers. See [Installing a Normal Server on page 2-23](#).

The Information Server

An Information Server is the main communication hub (middleware) between the Management Console and the Normal Servers it manages. It simplifies control of Normal Servers by allowing administrators to send instructions and receive information from remote sites.

**WARNING!**

An Information Server by itself is defenseless unless a Normal Server is installed on the same computer.

Information Server Tips

- If you are performing the very first ServerProtect installation on your network, you need to set the destination server as an Information Server, and then configure the other Normal Servers to this Information Server.
- An Information Server must have at least one member domain for supporting Normal Servers.
- Because an Information Server is simply a delivery system for information, the number of Normal Servers it can manage is, theoretically, only limited by the available bandwidth. You might, however, choose to moderate the number of Normal Servers you assign to an Information Server for ease of management.
- If you have many servers in different locations, set up an Information Server (IS) in each location.



Note

Benchmark testing results have verified that an Information Server can manage up to 250 Normal Servers. This number serves as a reference only. The Information Server can manage more Normal Servers depending on the available bandwidth.



Note

The Information Server and the Management Console are native 32-bit components of ServerProtect. However, on the 64-bit platform, these components of ServerProtect will run on **Windows On Windows (WOW)** 64 mode.

The Normal Server

A Normal Server can be any server on a network where ServerProtect is installed. This is the first line of defense in the ServerProtect architecture and where all the action takes place. These servers perform the actual antivirus functions of the system, and are managed by an Information Server.

ServerProtect offers several ways for installing Normal Servers:

- Using the setup program. See [Installing a Normal Server from the Setup Program on page 2-23](#).
- Using the Management Console. See [Installing a Normal Server from the Management Console on page 2-27](#).
- Using silent mode. See [Installing ServerProtect in Silent Mode on page 2-28](#).

Each of the listed installation methods can be tailored to your specific company needs. See [Installing a Normal Server on page 2-23](#).

**Note**

If the operating system is 32-bit, then 32-bit binaries of the Normal Server component of ServerProtect will be installed. If the operating system is 64-bit, then 64-bit binaries of Normal Server component of ServerProtect will be installed.

**WARNING!**

Because it is time-consuming to install servers individually from the setup program, Trend Micro recommends that you install your servers from the ServerProtect Management Console.

ServerProtect Domains

ServerProtect domains are virtual groupings of Normal Servers used to simplify their identification and management. You can create, rename, or delete domains according to the needs of your network.

Normal Servers in a domain can only be assigned to one Information Server. Information Servers, on the other hand, can manage several domains.

The most efficient way to manage network protection is to group all servers in relevant ServerProtect domains. For example, you can create a ServerProtect domain called "NS" to manage Normal Servers more efficiently. See [Managing ServerProtect Domains on page 3-10](#).

**WARNING!**

The concept of ServerProtect domains are not that of a Microsoft Windows domain; it is simply a logical grouping of Normal Servers running ServerProtect.

ServerProtect domains have the following features:

- **Domain filter:** Network administrators can set up a filter on an Information Server to control what can be viewed from the domain browser tree on the Management Console.

- **Flexible domain management:** After logging on to the console, IT professionals can add, rename, move or delete domains according to their preference.



Note

The main feature of the Management Console is to centralize the control multiple Normal Servers via a number of Information Server. However a Management console can only connect to and control one Information Server at any given time.

ServerProtect for Storage Architecture Overview

ServerProtect for Storage brings together two products from the ServerProtect family: ServerProtect for Network Appliance devices and ServerProtect for EMC Celerra. It also provides security for the storage devices using Internet Content Adaptation Protocol (ICAP).

ServerProtect for Storage with RPC Scanner

This section describes the product architecture of ServerProtect for Storage with RPC Scanner in 7-Mode and Cluster-Mode, and explains the ServerProtect for Storage with RPC Scanner organizational flow.

Product Architecture in 7-Mode

7-Mode Device indicates the machine where Data ONTAP 7-Mode is installed.

ServerProtect for Storage with RPC Scanner scans viruses using "on-access" mode, which takes place on a Scan Server. In turn, the Information Server manages the Scan Servers.

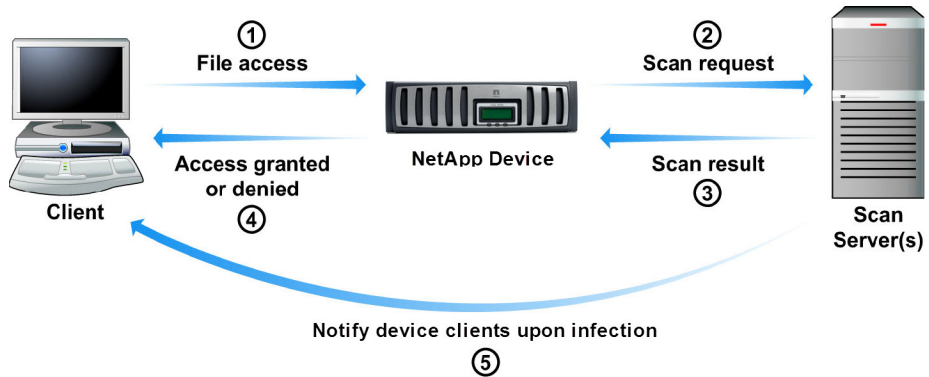


FIGURE 1-2. ServerProtect for Storage product architecture in 7-Mode

When a user tries to access a file or store a new file in a NetApp 7-Mode Device, the NetApp 7-Mode Device performs a virus check. If the filename extension matches the file scanning criteria (for example, an ".EXE" or a ".VBS" file), the NetApp 7-Mode Device sends a manual scan request (Scan Now) to the Scan Server(s). The Scan Server then passes back the scan result to the NetApp 7-Mode Device and according to the scan result, the user is either allowed to open, save, or is denied to access the file.

Product Architecture in Cluster-Mode

Cluster-Mode Device (also known as C-Mode Device) is the machine where Data ONTAP Cluster-Mode is installed. Cluster-Mode AV Connector (called by NetApp as Clustered Data ONTAP Antivirus Connector) is an agent program

provided by NetApp and installed together with the Normal Server to manage the Cluster-Mode Device.

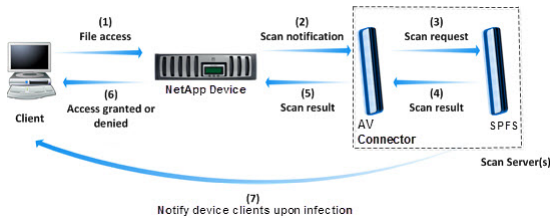


FIGURE 1-3. ServerProtect for Storage product architecture in Cluster-Mode

In Cluster-Mode, When a user tries to access a file or store a new file in a NetApp Cluster-Mode Device, the Cluster-Mode Device performs a virus check. If the filename extension matches the file scanning criteria (for example, an ".EXE" or ".VBS" file), the Cluster-Mode Device sends a scan notification to the Cluster-Mode AV Connector. The Cluster-Mode AV Connector sends a scan request (Scan Now) to the Scan Server(s). The Scan Server passes back the scan result to the Cluster-Mode AV Connector, and the Cluster-Mode AV Connector sends it to the Cluster-Mode Device. According to the scan result, the user is either allowed to open, save, or is denied to access the file.

To learn more about setting your NetApp Device file scanning criteria and Cluster-Mode, refer to your NetApp Device documentation.



Note

Since only specific file types contain viruses, establishing the right file scanning criteria can help optimize Scan Server performance, reduce bandwidth usage, and minimize scanning time. To learn how ServerProtect for Storage can efficiently and safely scan files, see [IntelliScan on page 1-28](#).

If a file contains a virus, ServerProtect for Storage performs a designated action. Refer to [Scanning Viruses for Normal Server on page 3-71](#) for additional information about scan actions. For example, if the file is cleanable

and ServerProtect for Storage is configured to perform a Clean action, the following will occur:

1. The Scan Server cleans the file and informs the NetApp Device that the file is no longer infected.
2. The NetApp Device allows its client to access the cleaned file and replaces the original file with the cleaned one.



Note

The NetApp Device "trusts" registered Scan Servers. Therefore, if a Scan Server also functions as a Normal Server (as a file or data server) and happens to send a file to the NetApp Device, it will not request the file to be scanned. To protect both the NetApp Device and the Normal Server, set the ServerProtect Real-time Scan to "Incoming & outgoing." See [Using Real-Time Scan on page 3-80](#) to set Real-time Scan to "Incoming & outgoing."

Organizational Overview

This section provides an explanation of the ServerProtect for Storage organizational flow in 7-Mode.

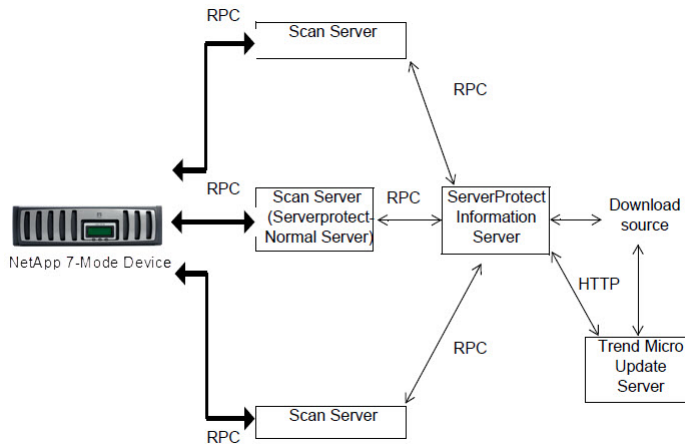


FIGURE 1-4. ServerProtect for Storage organizational flow in 7-Mode

ServerProtect for Storage uses an agent to communicate with the NetApp 7-Mode Device via remote procedure calls (RPCs). This agent performs the following functions:

- Registers the Normal Server with the NetApp 7-Mode Device as a "Scan Server." This informs the NetApp 7-Mode Device of the availability and location of a Scan Server
- Watches for NetApp 7-Mode Device file-scanning requests
- Returns scan results to the NetApp 7-Mode Device
- Answers any queries from the NetApp 7-Mode Device
- Informs the NetApp 7-Mode Device of any pattern file or scan engine updates
- Communicates with the NetApp 7-Mode Device to check the connection between the Scan Server and the NetApp 7-Mode Device

The organization flow in Cluster-Mode is similar to that in 7-Mode. The only difference is that ServerProtect for Storage communicates with the NetApp Cluster AV Connector instead of the NetApp 7-Mode Device.

ServerProtect for Storage with EMC CAVA Scanner Architecture Overview

The main components of the EMC VNX/VNXe antivirus system include:

- Data Mover (includes the VC Client) located on the EMC VNX/VNXe File Server
- AV Server (includes ServerProtect for Storage and Common Event Enabler (CEE)) located on a machine separate from the EMC VNX/VNXe File Server

Scanning is done on a separate AV Server rather than on the File Server. This ensures virus scanning will not impact the File Server's processing power. Connecting multiple AV Servers with the File Server evenly distributes the scanning workload. Scan requests and files are sent to AV Servers in a "round-robin" method. This evenly distributes the workload and improves scan performance.

Remote Procedure Call (RPC) connections maintain constant communication between the File Server and the AV Server(s) for round-the-clock assurance that only virus-free files are saved to the EMC data storage system.

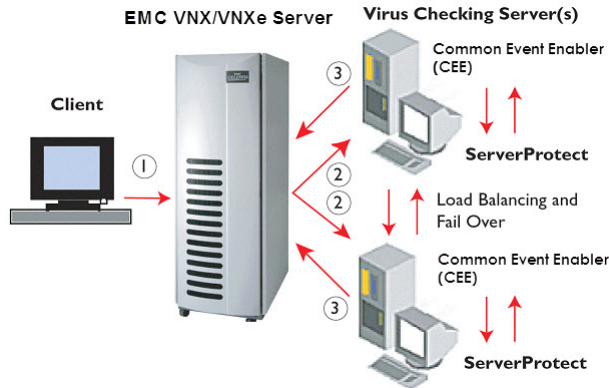


FIGURE 1-5. ServerProtect for Storage with EMC CAVA Scanner Architecture

The following is a description of the ServerProtect and EMC VNX/VNXe antivirus system workflow:

1. A user or application running a Windows client accesses the file from EMC VNX/VNXe using the Common Internet File System (CIFS) protocol.
2. When a client attempts to modify, close, or save a file to the EMC VNX/VNXe system, the EMC VNX/VNXe File Server triggers a request.
3. The Virus Checking (VC) Client on the EMC VNX/VNXe will request a virus check by sending the Universal Naming Convention (UNC) path name to the CEE of the AV Server.
4. The request is sent to AV Servers in a round-robin fashion.
5. On the AV Server, CEE requests ServerProtect to scan the file for viruses using the Real-time Scan function.
6. Simplified scan results:

- NON-INFECTED: file not infected, or disinfected (file can be opened)
- INFECTED: infected and not cleanable (file access is denied)

Protecting the EMC VNX/VNXe File Server is the main focus of SPFS. In SPFS, virus scanning is made in "on-access" mode, and takes place on a separate machine (AV Server) that is running Windows 2008, Windows 2012, Windows 2016, Windows 2019, or Windows 2022. The AV Server protects the File Server. This differs from the regular version of ServerProtect whose focus is to protect the Normal Server.

When a client attempts to modify, close or save a file to the Server, the VC Client on the EMC VNX/VNXe Server will request a virus check by sending the Universal Naming Convention (UNC) path name to CEE on an AV Server. CEE then requests ServerProtect to scan the file using Real-time Scan mode.

If the file is infected, ServerProtect performs a designated virus action. If CEE reports the file has been successfully cleaned, the File Server lets clients access the file or saves it to its attached data storage system.

Organizational Overview

ServerProtect for Storage communicates with the EMC VNX/VNXe File Server via Remote Procedure Call (RPC).

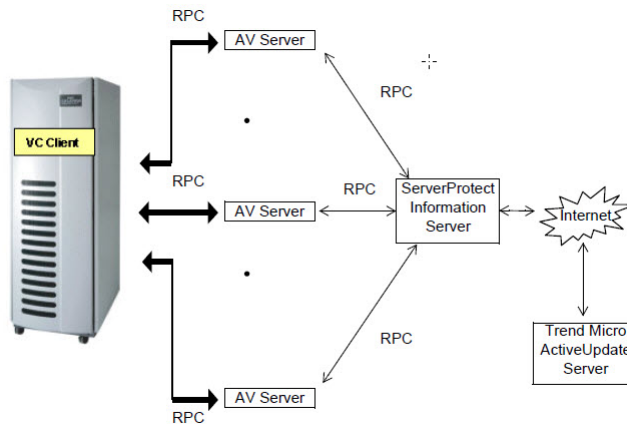


FIGURE 1-6. ServerProtect for EMC Celerra Organizational Flow

ServerProtect performs the following functions:

- Works with CEE to become an AntiVirus Server (AV Server) for a EMC VNX/VNXe File Server
- Notifies the VC Client (on the EMC VNX/VNXe File Server) that CEE and ServerProtect are installed and the Real-time Scan service is running
- Monitors for requests from the VC Client to scan files
- Lets CEE return scan results to the VC Client
- Informs the VC Client of any pattern file or scan engine updates
- Communicates with the VC Client to check the connection between the AV Server and the EMC VNX/VNXe File Server
- Works with the VC Client to provide load balancing among multiple AV Servers via round-robin method

Specific Functions for EMC VNX/VNXe

An AV Server receives a scan request when a user tries to access a file on the EMC VNX/VNXe File Server. The AV Server then scans the file using the ServerProtect Real-time Scan function. To protect both the EMC VNX/VNXe File Server system and the AV Server, the default setting for the ServerProtect Real-time Scan function is incoming and outgoing.

Trend Micro strongly recommends not changing this setting. For more information about Real-time Scans, refer to [Using Real-Time Scan on page 3-80](#). If the file is infected, the AV Server performs one of the following actions, depending on the previous configuration:

- **Bypass:** Skips over the file without taking any corrective action in a Real-time Scan (see the Warning that follows these action descriptions).
- **Delete:** Deletes the infected file.
- **Rename:** Changes the name of the infected file by modifying the file extension to ".VIR".
- **Clean:** Attempts to clean the virus code from the file.
- **Quarantine:** Moves the infected file to a designated folder.



WARNING!

Trend Micro recommends using only the **Clean**, **Delete**, and **Quarantine** actions, rather than using the **Bypass** action. If a file is infected and the virus action is set to **Bypass**, the file will remain infected after entering the EMC VNX/VNXe File Server system.

ServerProtect for Storage with ICAP Scanner

ServerProtect for Storage uses the Internet Content Adaptation Protocol (ICAP) to communicate between the storage device and the ICAP scanner.

This section describes the ICAP Scanner workflow in ServerProtect for Storage.

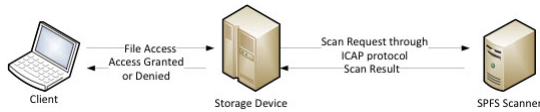


FIGURE 1-7. ServerProtect for ICAP Scanner workflow

When a user attempts to access a file located on a storage device, the storage device sends a scan request to ServerProtect through ICAP. ServerProtect scans the file for viruses, and then according to the scan result, either allows or denies the access to the file.

Scan Actions

The ICAP Scanner in ServerProtect for Storage provides the following scan actions:

- **Clean:** The ICAP Scanner cleans an infected file and sends the cleaned file back to the storage device.
- **Block:** If the infected file is not cleanable, the ICAP Scanner notifies the storage device that the file is not cleanable, without sending back the infected file.

Deployment

ServerProtect for Storage enables you to deploy multiple scan servers with multiple storage devices. An ICAP scanner in ServerProtect for Storage can

handle requests from multiple storage devices. Similarly, a storage device can send scan requests to multiple ServerProtect for Storage ICAP scanners.

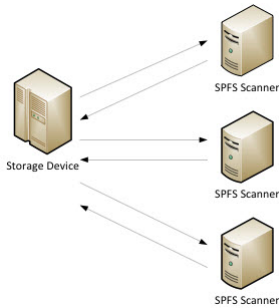


FIGURE 1-8. A storage device can send scan requests to multiple ServerProtect ICAP Scanners

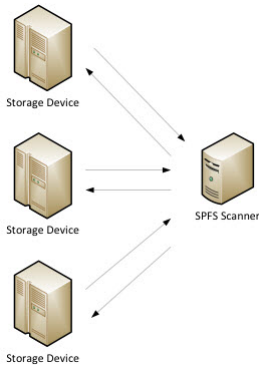


FIGURE 1-9. A ServerProtect ICAP Scanner can handle scan requests from multiple storage devices

Real-time Scan Versus On-demand Scan (Scan Now)

ServerProtect features two powerful scan functions, Real-time Scan and Scan Now.

Real-time Scan runs continuously on a server and provides the maximum level of virus protection. All file I/O events on the server are monitored and infected files are prevented from being copied to or from the server. See [Using Real-Time Scan on page 3-80](#).

Scan Now is a manual virus scan (that is, it occurs immediately after being invoked). Use Scan Now to check a server that you suspect may have been exposed to a computer virus or about which you want immediate information. See [Using Scan Now \(Manual Scan\) on page 3-84](#).

**Tip**

To ensure maximum protection, Trend Micro recommends using both Real-time Scan and Scan Now.

Real-time Scan and Scan Now benefits include:

- **Redundant File Scan:** If a file containing a virus is accidentally downloaded or copied, Real-time Scan will stop it. Even if for any reason Real-time Scan is disabled, Scan Now will still detect it.
- **Efficient File Scan:** By default, Real-time Scan is configured to scan files. It has the advantage of minimizing the impact to system resources. See [Scanning Viruses for Normal Server on page 3-71](#).
- **Effective and Flexible File Scan:** ServerProtect gives IT professionals effective and numerous scan configuration options to protect their networks based on their individual needs. See [Scanning Viruses for Normal Server on page 3-71](#).

Working with Tasks

ServerProtect allows IT professionals to create multiple tasks which can be deployed on demand or on a scheduled basis.

Use ServerProtect tasks to:

- Deploy updates
- Run Real-time Scan

- Run Scan Now
- Purge, delete, export, or print logs
- Generate virus scan statistics

ServerProtect tasks benefits include:

- Simultaneous multiple function deployment
- Unattended routine antivirus maintenance procedures on your network
- Improved antivirus management efficiency and control over antivirus policy

Tasks are assigned to a "task owner" who is responsible for maintaining the task. See [Managing Tasks on page 3-47](#).

After you install ServerProtect on a server, three default tasks already exist: Scan, Statistics, and Deploy. These tasks are essential for managing and monitoring antivirus activities on your network. You can modify the target servers of these three default tasks, as well as their definitions.

When ServerProtect Finds a Virus (Virus Actions)

ServerProtect allows you to configure the type of action that the software takes on infected files. In addition to the antivirus protection offered by previous versions, a Spyware pattern is now available in ServerProtect 5.8, forming a virus category of its own. You can choose a specific course of actions to handle certain types of viruses at will. The Damage Cleanup Engine is made more powerful by including the feature of Generic Clean.

There are five possible actions that ServerProtect can take on an infected file:

- **Bypass/Ignore:** For a manual scan, ServerProtect skips the file without taking any corrective action. However, detection of the virus is still recorded in the program's log entries. For Real-time Scan, if the scan direction is set as **Outgoing** or **Incoming & Outgoing**, ServerProtect treats the file as "deny-write," protecting it from duplication or modification. See [Defining Actions Against Viruses on page 3-73](#) for more information.

- **Delete:** The infected file is deleted.
- **Rename:** The infected file extension is renamed to .vir. This prevents the file from being executed or opened. If a file of that name with the .vir extension already exists, the file will be renamed to .v01, .v02, and so on, until .v99.
- **Quarantine:** The infected file is moved to a folder of your choice. You can also change the file extension of the moved file to prevent it from being inadvertently opened or executed.
- **Clean:** Attempt to clean the virus code from the file. Because the cleaning process sometimes corrupts the file and makes it unusable, you can back up the file before cleaning.

If the ICAP Scanner cleans an infected file, it sends the cleaned file back to the storage device.

- **Block** (ICAP Scanner only): If the infected file is not cleanable, the ICAP Scanner notifies the storage device that the file is not cleanable, without sending back the infected file.

All virus events and associated courses of action are recorded in the log file. For more information, refer to the “Viewing the infection logs” topic in the online help and [Defining Actions Against Viruses on page 3-73](#).

**Note**

If you select **Clean** as the virus action, you can specify a secondary action if the cleaning process is unsuccessful.

**Note**

On a 64-bit operating system, ServerProtect detects both 32-bit viruses and 64-bit viruses.

**Note**

ServerProtect 5.8 does not support clean action against spyware infected files. When using ActiveAction, the actual effect of an action applied to a spyware infected file will be equivalent to that of the **Bypass** action.

**Note**

For ICAP Scanner, ServerProtect for Storage only provides **Clean** and **Block** actions for an infected file.

Virus Logs

The real power of a centralized antivirus system is its ability to record and present information regarding the network's antivirus policy from a single console. IT professionals can easily access information while they are monitoring their network servers.

ServerProtect provides comprehensive information about scanning, file updating, and deploying results. Furthermore, ServerProtect saves the information in a log file which can be either retrieved or exported. For example, you can analyze the scanning statistics for virus scanning on your network. These statistics include information such as what the most common viruses are or which users introduced viruses to the network. In addition, you can export the log information to a database or spreadsheet application for further analysis.

On each Normal Server, ServerProtect supports backing up of log database file when it exceeds the default size limit of 10-MB or after configured number of days. The default size for the log file is 10,000 entries, or up to 10-MB. After the log file exceeds 10,000 entries or 10-MB, which ever is smaller in size, ServerProtect automatically renames the log file and creates a new log file. ServerProtect, however, does not impose number of days limit, unless it is configured. For information on configuring log backup, refer to *Configuring the Log Database Backup Options* topic in Online Help.

You can also take action on the infected files directly from the Scan Result window, providing you a convenient way to take appropriate actions on a virus infection event. For more information about log files, refer to the

ServerProtect online help from the ServerProtect Management Console. For more information on Virus logs, refer to the “Viewing log information and Viewing Information Server logs” topics in the Online Help.

Deploying Updates

Trend Micro update is an upgrade and update deployment module for Trend Micro antivirus software. It simplifies the maintenance of Trend Micro software and reduces the total cost of your network’s antivirus security. Because of the number of viruses that are developed monthly, a successful virus policy depends on the use of virus pattern files and scan engine files, that can deal with the latest threats. See [Configuring Updates on page 3-31](#).



Note

Trend Micro releases new versions of these downloadable update files on a regular basis.

ServerProtect update features include:

- **Update component selection:** Trend Micro provides a rich set of anti virus utilities in ServerProtect 5.8 for updating, including newly-added Spyware pattern and other virus patterns, Damage Cleanup Engine and a Damage Cleanup Template, as well as Anti-rootkit driver.
- **Unattended scheduled update:** You can create scheduled update tasks to update all Normal Servers while you are asleep.
- **Flexible file download:** You can designate an Information Server to download updates from the Trend Micro update site, then have other servers obtain the updated files from it.
- **Centralized update deployment:** You can deploy updates to servers on your network from the Management Console.
- **Firewall and proxy server compatibility:** ServerProtect works with the majority of existing firewalls and proxy servers.
- **Update activity logging:** ServerProtect records all update activity in a log file for future reference.

- **Update Roll-back option:** If you encounter a problem while deploying an update, you can only roll-back the component which is most recently updated. Note that the rollback operation can only be carried out on virus patterns and Virus Scan Engine.

Updating ServerProtect is a two-step process:

1. Download updates from the Trend Micro update server. See [Downloading Updates on page 3-34](#).
2. Deploy the downloaded updates to other Normal Servers on the network. See [Deploying Updates on page 3-42](#).

This highly efficient approach saves download time and minimizes network bandwidth usage.



Tip

You can automate the deployment of updates for Normal Servers by creating a scheduled update task. See [Creating Tasks on page 3-50](#).

ServerProtect Virus Detection Technology

ServerProtect uses advanced virus detection technology. In this section, we feature the tools which support this state of the art technology and how IT professionals can benefit from it.

Pattern Matching

Using a process called "pattern matching," ServerProtect draws on an extensive database of virus patterns to identify known virus signatures. Key areas of suspect files are examined for tell-tale strings of virus code and compared against thousands of virus signatures that Trend Micro has on record.

For polymorphic or mutation viruses, the ServerProtect scan engine permits suspicious files to execute in a protected area within which it is decrypted. ServerProtect then scans the entire file, including the freshly decrypted code, and looks for strings of mutation-virus code.

If such a virus is found, ServerProtect performs the action you previously specified to handle it. ServerProtect virus actions include **clean** (autoclean), **delete**, **bypass** (ignore), **quarantine** (move), or **rename**. Virus actions can be customized for both boot viruses and file viruses. See [Scanning Viruses for Normal Server on page 3-71](#).

**Note**

It is important to keep the Spyware pattern and virus pattern files up to date. More than a thousand new viruses are created each year. Trend Micro makes it easy to update the pattern file by supporting scheduled updates. See [Configuring a Scheduled Deployment on page 3-44](#) for more information.

MacroTrap™

ServerProtect includes patented MacroTrap™ technology to guard against macro viruses in Microsoft™ Office files and templates. Macro viruses are the fastest spreading computer viruses. Because they are harbored in files that are commonly passed around by email, these kinds of viruses are easily spread. See [Configuring Real-Time Scan on page 3-81](#) for MacroTrap configuration information.

**Note**

Trend Micro MacroTrap protects network users from receiving and sending macro viruses.

How MacroTrap Works

The MacroTrap performs a rule-based examination of all Macro code that is saved in association with a document. Macro virus code is typically contained as a part of the invisible template (for example, *.dot in Microsoft Word) that travels with the document. Trend Micro MacroTrap checks the document for signs of a macro virus by seeking out instructions that perform virus-like activity. Examples of virus-like activity are copying parts of the template to other templates (replication), or code to execute harmful commands (destruction).

Compressed Files

Compressed file archives (that is, a single file composed of many separate compressed files) are the preferred form to distribute files by email and the Internet. Because some antivirus software is not able to scan these kinds of files, compressed file archives are sometimes used as a way to "smuggle" a virus into a protected network or computer.

The Trend Micro scan engine can scan files inside compressed archives. It can even scan compressed files that are composed of other compressed files -- up to a maximum of five compression layers.

The Trend Micro scan engine used in ServerProtect can detect viruses in files compressed using the following formats:

- ARJ (.arj) and ARJ_SFX (.exe)
- BINHEX
- BASE64
- CABINET (.cab)
- DIET (.com)
- GNU ZIP (.gz)
- LHA (.lzh) and LHA_SFX (.exe)
- LZEXE (.exe)
- Microsoft Office Open XML format (.docx, .xlsx, .pptx, .one)
- PKLITE (.exe or .com)
- PKZIP (.zip) and PKZIP_SFX (.exe)
- RAR (.rar)
- TAR
- UNIX COMPACTED (.z)
- UNIX LZW (.Z)
- UNIX PACKED (.z)

- UUENCODE

**Note**

The Trend Micro scan engine can currently only clean compressed files using the PKZIP algorithm. If a virus is found in an archive using other algorithms, they must first be decompressed in a temporary directory, then cleaned.

For compressed file configuration information, see [Configuring Real-Time Scan on page 3-81](#) and [Configuring Scan Now on page 3-85](#).

Damage Cleanup Services

Damage Cleanup Services (DCS) detects Trojans, based on their behavior, and restores modified system files. DCS also terminates Trojan-related processes, and deletes files that the Trojan "drops" in the system.

**Note**

If a spyware infected file is detected, only bypass can be applied. The file will be bypassed without any other treatment. Clean function does not apply to spyware infection.

OLE Layer Scan

Microsoft™ Object Linking and Embedding (OLE) allows embedding Microsoft Office™ files within themselves. This means that you could have a Microsoft Word document inside an Excel spread sheet, and in turn this Excel spread sheet could be embedded in a Microsoft™ PowerPoint presentation.

OLE offers a large number of benefits to developers, at the same time it can lead to potential infection. To address this issue, Trend Micro has added a new scan feature "OLE layer scan" that complements state-of-the-art ServerProtect virus protection. See [Scanning Viruses for Normal Server on page 3-71](#).

**Tip**

OLE layer scan offers five layers of protection. Trend Micro recommends a setting of two OLE layers for Scan Now and a setting of one for a Real-time Scan. A lower setting will improve server performance.

IntelliScan

IntelliScan is a new method of identifying which files to scan that is both more secure, and more efficient, than the standard "Scan All files" option.

For executable files (that is, .zip, .exe), the true file type is determined from the file content. In the event that a file is not executable (such as .txt), IntelliScan will use the file header to verify the true file type. See [Scanning Viruses for Normal Server on page 3-71](#).

The following are just a couple of the benefits IntelliScan offers to administrators:

- **Performance optimization:** Server system resources allotted to scan will be minimal, thus using IntelliScan will not interfere with other crucial applications running on the server.
- **Time saving:** Because IntelliScan uses true file type identification, IntelliScan scan time is significantly less than that of all files scan (this means that only files with a greater risk of being infected are scanned). This time difference is noticeable when you use IntelliScan with Scan Now. See [Configuring Scan Now on page 3-85](#).

ActiveAction

ActiveAction is a set of pre-configured scan actions that can be performed on viruses and other types of malware. ActiveAction can be configured for both Scan Now and Real-time Scan.

When to Select ActiveAction

Trend Micro recommends that you select ActiveAction if you are not familiar with virus actions or if you are unsure of which scan action is the most suitable for a certain virus.

Viruses vary significantly from one another; this requires appropriate virus actions for each virus type. Customizing scan actions for file viruses requires knowledge of viruses and can be a tedious task. For this reason, Trend Micro recommends the use of ActiveAction.

Some advantages of using ActiveAction versus customized scan actions are:

- **Time saving:** You spend no time customizing virus actions.
- **Worry-free maintenance:** ActiveAction uses Trend Micro recommended scan actions so you can concentrate on other tasks and not worry about making mistakes.
- **Updateable scan actions:** Trend Micro includes new ActiveAction scan actions with every new pattern. Viruses constantly change how they attack, thus scan actions should be frequently modified to prevent possible infection.

For ActiveAction configuration information, see [Defining Actions Against Viruses on page 3-73](#).

**Note**

When using ActiveAction, the action for spyware virus is bypass/bypass.

Mapped Network Drive Scan

ServerProtect can scan one or several network drive(s); the shared network folders have to be mapped first before selecting this feature. This is helpful because Real-time Scan scans and protects mapped drives as it does with local drives, therefore reducing the risk of infection. See [Configuring Real-Time Scan on page 3-81](#).

Additional Features

To help IT professionals protect their networks with more flexibility, ServerProtect includes additional features.

Centralized Management

ServerProtect provides a Windows-based console (the Management Console) to help you manage virus protection for multiple servers on your network. The console is portable and can be run on any 32-bit or 64-bit Windows server.

Enhanced Network Security on Installation

During Normal or Information Server installation, you must enter the administrator user name and password of the selected target servers.

Swift Response to Virus Outbreaks

If a virus tries to infect a file in a shared folder on a server under the protection of ServerProtect, a message box appears, identifying the computer in the network on which the virus originated from. This message box also displays the following information: the type of scan, the name of the virus, the name of the infected file, the name or ID of the computer involved and the user name. In addition, it also displays the action taken on the virus and the source of infection. See [Configuring Notification Messages on page 3-64](#).

Flexible Control over Infected Files

When ServerProtect detects an infected file, you can choose to restore the file after cleaning, send suspect or uncleanable files to Trend Micro, delete the backup file made before cleaning, or return cleaned files to the user by email.

NetworkTrap Tool

Certain viruses actively seek out shared folders (an example of this type of virus is PE.FunLove.4099) to infect as many connected users as possible. The NetworkTrap tool lets you share a folder and automatically copies the contents of the Bait folder to the newly created shared folder (the Bait' folder contains files that viruses are likely to infect). This shared folder works with the new virus notification to create an effective virus trap. For more

information on this topic, refer to the “NetworkTrap Tool” section in the online help.

State-of-the-Art Virus Detection Technology

New configurable scanning tools like ActiveAction, IntelliScan, and OLE layer scan offer faster and more efficient scanning.

Viewable Scanning Statistics

ServerProtect enables you to efficiently monitor your network antivirus security. It displays scanning statistics on your network, including the following, for a given interval: total number of viruses found, top ten viruses found, top ten infected users, total number of non-cleanable viruses, and more.

Compatibility

ServerProtect is fully compatible with versions of Microsoft Windows 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, and 2022 Server operating systems. It also supports Network File System (NFS) drivers, and SOCKS 4 for the Trend Micro update server.

ServerProtect is compatible with 32-bit and 64-bit operating systems. ServerProtect automatically detects 32-bit and 64-bit Windows Servers. If the operating system is 32-bit, then 32-bit binaries of the Normal Server component of ServerProtect will be installed or uninstalled. If the operating system is 64-bit, then 64-bit binaries of the Normal Server component of ServerProtect will be installed or uninstalled.

Chapter 2

Installing ServerProtect for Storage

This chapter includes the following information to successfully install ServerProtect for Storage on your network(s):

- *System Requirements on page 2-2*
- *Installation Scenarios on page 2-7*
- *Installing ServerProtect on page 2-12*
- *Installing ServerProtect for Storage with RPC Scanner or ICAP Scanner on page 2-31*
- *Installing ServerProtect for Storage with EMC CAVA Scanner on page 2-31*
- *Removing ServerProtect on page 2-33*

**Note**

You must log on with administrator privileges in order to install an Information Server.

**Note**

Trend Micro recommends not installing a previous version of Normal Server and register it to the ServerProtect Information Server.

System Requirements

Normal Server

- CPU: 2.5 GHz Intel™ Pentium™ IV processor or 3.0 GHz EM64T Intel™ processor or 2.0 GHz AMD Athlon™ 64-bit processor (or equivalent)
- DRAM: Minimum 1-GB, 2-GB recommended
- Operating System:
 - Microsoft Windows Server 2008 Standard/Enterprise SP2 (x86 or x64)
 - Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 (x64)
 - Microsoft Windows 2008 Server Core
 - Microsoft Windows Server 2012 Foundation, Essentials, Standard or Datacenter (x64)
 - Microsoft Windows Server 2012 R2 Foundation, Essentials, Standard or Datacenter (x64)
 - Microsoft Windows Storage Server 2012 Standard or Workgroup (x64)
 - Microsoft Windows Storage Server 2012 R2 Standard or Workgroup (x64)
 - Microsoft Windows Server 2016 Essentials, Standard, Datacenter (x64)
 - Microsoft Windows Storage Server 2016 Standard or Workgroup (x64)
 - Microsoft Windows Server 2019 Essentials, Standard, Datacenter (x64)
 - Microsoft Windows Server IoT 2019 (x64)
 - Microsoft Windows Server 2022 Essentials, Standard, Datacenter (x64)

- Microsoft Windows Server IoT 2022 (x64)
- Disk Space: 1-GB
- A CD-ROM drive if the installation is performed locally.
- Network protocols and services: TCP/IP, Microsoft Network and RPC services must be running on Windows Server family operating system.

Information Server

- CPU: 3.0 GHz Intel™ Pentium™ IV processor or 3.0 GHz EM64T Intel™ processor or 2.0 GHz AMD Athlon™ 64-bit processor (or equivalent)
- DRAM: Minimum 1-GB, 2-GB recommended
- Operating System:
 - Microsoft Windows Server 2008 Standard/Enterprise SP2 (x86 or x64)
 - Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 (x64)
 - Microsoft Windows 2008 Server Core
 - Microsoft Windows Server 2012 Foundation, Essentials, Standard or Datacenter (x64)
 - Microsoft Windows Server 2012 R2 Foundation, Essentials, Standard or Datacenter (x64)
 - Microsoft Windows Storage Server 2012 Standard or Workgroup (x64)
 - Microsoft Windows Storage Server 2012 R2 Standard or Workgroup (x64)
 - Microsoft Windows Server 2016 Essentials, Standard, Datacenter (x64)
 - Microsoft Windows Storage Server 2016 Standard or Workgroup (x64)
 - Microsoft Windows Server 2019 Essentials, Standard, Datacenter (x64)

- Microsoft Windows Server IoT 2019 (x64)
- Microsoft Windows Server 2022 Essentials, Standard, Datacenter (x64)
- Microsoft Windows Server IoT 2022 (x64)
- Disk Space: 1-GB
- A CD-ROM drive if the installation is performed locally.
- Network protocols and services: TCP/IP, Microsoft Network and RPC services must be running on Windows Server family operating system.

The services listed above must be running on the installed machine. Trend Micro recommends an allocated bandwidth usage of minimum 128 Kilobytes per second to optimize deployment of component updates between ServerProtect Information Server and Normal Server. If RPC communication malfunctions over either the Named Pipe protocol or TCP, ServerProtect will automatically switch from the non-functioning protocol to the other. To manage Windows Server, an Information Server must be installed.



Note

For ActiveUpdate 2.8, additional 3-GB disk space is required if Smart Duplicate is needed to be turned on, in which case the cached pattern number must be set to value of 14.

Management Console

- CPU: 2.5 GHz Intel™ Pentium™ IV processor or 3.0 GHz EM64T Intel™ processor or 2.0 GHz AMD Athlon™ 64-bit processor (or equivalent)

For Server Environment:

- DRAM: Minimum 1-GB, 2-GB recommended
- Operating System:
 - Microsoft Windows Server 2008 Standard/Enterprise SP2 (x86 or x64)

- Microsoft Windows Server 2008 R2 Standard/Enterprise SP1 (x64)
- Windows Server 2012 Foundation, Essentials, Standard or Datacenter (x64)
- Windows Server 2012 R2 Foundation, Essentials, Standard or Datacenter (x64)
- Microsoft Windows Storage Server 2012 Standard or Workgroup Edition (x64)
- Microsoft Windows Storage Server 2012 R2 Standard or Workgroup Edition (x64)
- Microsoft Windows Server 2016 Essentials, Standard, Datacenter (x64)
- Microsoft Windows Storage Server 2016 Standard or Workgroup (x64)
- Microsoft Windows Server 2019 Essentials, Standard, Datacenter (x64)
- Microsoft Windows Server IoT 2019 (x64)
- Microsoft Windows Server 2022 Essentials, Standard, Datacenter (x64)
- Microsoft Windows Server IoT 2022 (x64)

For Client Environment:

- DRAM: Minimum 512-MB, 1-GB recommended
- Operating System:
 - Microsoft Windows Vista Business/Enterprise/Ultimate SP1 (x86 or x64)
 - Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 (x86 or x64)
 - Microsoft Windows 8 Professional/Enterprise (x86 or x64)
 - Microsoft Windows 10 Professional/Enterprise (x86 or x64)

- Microsoft Windows 11 Professional/Enterprise (x64)
- Disk Space: 500-MB

VMWare

- Any version of VMware ESX/ESXi running on any operating system supported by ServerProtect for Storage
- Any version of VMware vSphere™ running on any operating system supported by ServerProtect for Storage

Hyper-Visor

- Microsoft Windows Server 2008 R2 Standard/Enterprise with Hyper-V
- Microsoft Windows Server 2008 Standard/Enterprise with Hyper-V

Storage Devices

- EMC VNX/VNXe
- EMC Celerra
- EMC Isilon
- EMC Unity
- EMC PowerScale
- NetApp Storage Devices running Data ONTAP 7.x and 8.x
- NetApp Storage Devices running ONTAP 9.x
- NetApp ONTAP Select 9.x Cluster-Mode
- NetApp Cloud Volumes ONTAP 9.x
- Amazon FSx for NetApp ONTAP
- IBM N Series running Data ONTAP
- Hitachi NAS
- HP 3PAR File Persona

- Nutanix Files 3.5.2 or later
- Huawei OceanStor Storage

Installation Scenarios

This section will help you select the most appropriate scenario to install ServerProtect on your network(s). The following scenarios focus on Local Area Networks (LANs), although it is also possible to manage ServerProtect across Wide Area Networks (WANs) such as, corporate Intranets, using TCP/IP. See [Managing ServerProtect Across a Wide Area Network on page 2-11](#).

Specifying Your Installation Environment

Trend Micro ServerProtect supports Microsoft Windows and Novell NetWare platforms. If you are installing ServerProtect on your network for the first time, you must set the destination server as an Information Server, then configure the Normal Servers to join it. An Information Server must have at least one ServerProtect domain to manage its Normal Servers. See [ServerProtect Domains on page 1-7](#).



Note

If you have many servers concentrated in different geographical locations, set up an Information Server (IS) in each location. See [Information Server Tips on page 1-5](#).

The following table shows the different installation environments for each ServerProtect setup component on Microsoft Windows platforms.

TABLE 2-1. Installation Scenarios on MS Windows

OPERATING SYSTEM	INFORMATION SERVER	NORMAL SERVER	MANAGEMENT CONSOLE
Windows Server 2008 family 32-bit	Yes	Yes	Yes
Windows Server 2008 family 64-bit	Yes (WOW64)	Yes	Yes (WOW64)

OPERATING SYSTEM	INFORMATION SERVER	NORMAL SERVER	MANAGEMENT CONSOLE
Windows Server 2008 Core 32-bits	No	Yes	No
Windows Server 2008 Core 64-bits	No	Yes	No
Windows Server 2008 R2 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2012 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2012 R2 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2016 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2019 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Server 2022 family	Yes (WOW64)	Yes	Yes (WOW64)
Windows Vista Desktop family	No	No	Yes
Windows 7 Desktop family	No	No	Yes
Windows 8 Desktop family	No	No	Yes
Windows 10 Desktop family	No	No	Yes
Windows 11 Desktop family	No	No	Yes

**Note**

Windows Vista desktop family means Business edition, Enterprise edition, and Ultimate edition.

Windows 7 desktop family means Professional edition, Enterprise edition, and Ultimate edition.

Windows 8 desktop family means Windows 8, Windows 8 Pro, Windows 8 Enterprise.

Windows 10 desktop family means Windows 10, Windows 10 Pro, Windows 10 Enterprise.

Windows 11 desktop family means Windows 11, Windows 11 Pro, Windows 11 Enterprise.

Windows Server 2008 family and Windows Server 2008 R2 family both mean Standard version, enterprise version, storage and datacenter server.

Windows Server 2012 family and Windows Server 2012 R2 family both mean Standard version, essentials version, foundation version, storage and datacenter server.

Windows Server 2016 family means Standard version, essentials version, storage and datacenter server.

Windows Server 2019 family means Standard version, essentials version, IoT and datacenter server.

Windows Server 2022 family means Standard version, essentials version, IoT and datacenter server.

**Note**

Hyper-V is supported by Windows Server 2008 and Windows Server 2012.

Firewall Setting for ServerProtect Components

This section describes firewall settings. Be sure to configure your firewall correctly before you install ServerProtect components.

- **Firewall Setting for the Machine with Management Console**

- Open 1000 - 1009 port for TCP protocol

1000 - 1009 is used by the Management Console to receive the event response message from the Information Server.

The Management Console will listen to port 1000 during startup. If the port is occupied by a certain program, the Management Console will find one available port from 1001 - 1009.

- **Firewall Setting for Information Server**

- Open 5005 - 5014 ports for TCP protocol.

Port 5005 is used to receive commands from the Management Console. Normally, port 5005 must be opened. If it is used by a certain program, please find one available port from 5006 - 5014 and open the firewall.

- Open 3000 - 3009 for UDP protocol

Port 3000 is used to receive broadcast messages. If port 3000 is occupied by a certain program, please find one available port from 3001 - 3009 and open the firewall.

- Open 137 - 139 and 445 for RPC Over named pipe

- 137 (UDP)
- 138 (UDP)
- 139 (TCP)
- 445 (TCP)

**Note**

These ports are opened to enable ServerProtect to use Remote Procedure Call (RPC) Over named pipe protocol to communicate.

- Open 3628(TCP)
Port 3628 is used to receive event response messages.
- Open 1921 for SPX/TCP with Netware
Port 1921 is used to communicate with Netware through the SPX/TCP protocol.
- **Firewall Setting for Windows with Normal Server**
 - Open 5168 for listening RPC over TCP/IP from Information Server
Port 5168 is used to receive commands from Information Server.
 - Open 137 - 139 and 445 for named pipe.
 - 137 (UDP)
 - 138 (UDP)
 - 139 (TCP)
 - 445 (TCP)
- **Firewall Setting for the Netware Machine with Normal Server**
 - Open port 9921 (SPX/TCP)
This port is used to receive commands from Information Server.

Managing ServerProtect Across a Wide Area Network

ServerProtect can be managed from multiple locations across a WAN. However, to ensure proper network performance, Trend Micro suggests that you install Information Servers in the same network domain of a workgroup of the network as the Normal Servers they manage.

Because the Management Console uses TCP/IP to communicate with Information Servers, it's easy to manage ServerProtect from any point inside most company Intranets.

Installing ServerProtect

For a server network system on which ServerProtect has never been installed or already has been uninstalled, it is recommended that the user choose the complete ServerProtect package installation, which includes installing the Management Console, Information Server and the Normal Server. The program installed in this way will guarantee that the ServerProtect be readily operational, and that the installation operation itself be straight forward and smoothly carried out.

This section guides you through the ServerProtect installation process.

Before Installing ServerProtect

As with any server software installation or upgrade, Trend Micro recommends that this activity be performed when the impact to users is minimal; that is, outside business hours and after a full system backup has been completed. Before carrying out a network installation, make sure that the network connections among the related server computers are established.

It is also good practice to install the program on a test server first so that installation issues, if any, can be identified and handled properly before the installation. Before installing ServerProtect, make sure you carefully read the Installation Scenarios section. See [Installation Scenarios on page 2-7](#).

**Note**

You must be logged on with administrator privileges in order to install ServerProtect.

Installing the Complete ServerProtect Package

To install the complete ServerProtect package, including the Management Console, Information Server and the Normal Server, execute the setup program on one or more Windows platform computers.

Procedure

1. Insert the Enterprise CD-ROM and run **SETUP.EXE**. The ServerProtect **Welcome** screen appears.

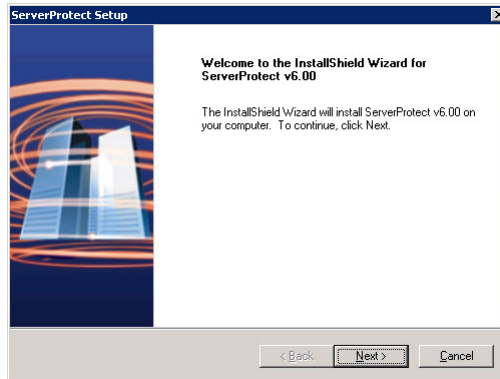


FIGURE 2-1. ServerProtect Welcome screen

2. Click **Next**. The **Software License Agreement** screen appears. You must agree to the license conditions to proceed with Setup.

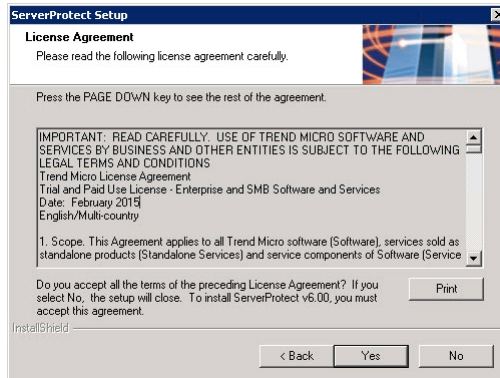


FIGURE 2-2. Software License Agreement screen

3. Click **Yes**. ServerProtect checks the boot sector of the storage hardware for viruses.

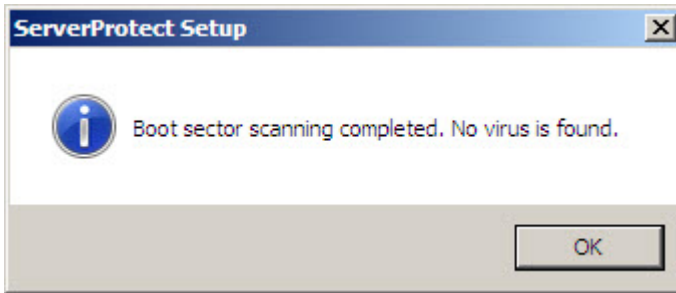


FIGURE 2-3. Scan Result Information window

4. Click **OK** to continue. The **User Information** screen appears.

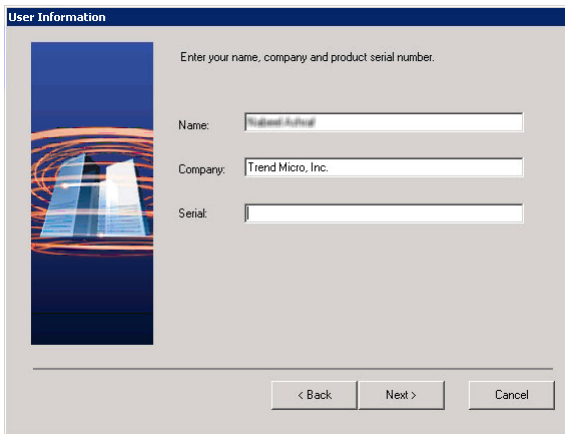


FIGURE 2-4. ServerProtect User Information screen

5. Provide your user information including the product's serial number.
Even with the serial number field left empty, the ServerProtect will still be installed to allow the user enjoy a trial version of the program valid for a 30-day period. If the serial number entered is invalid, the installation program appears a message box, showing "The serial number is incorrect, please try again".
6. Click **Next** to continue. The **Select Components** screen appears.

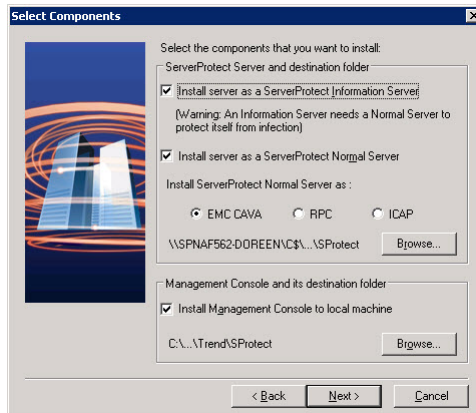


FIGURE 2-5. ServerProtect Select Components screen

7. Select all the check boxes to install complete package for ServerProtect for Storage.



Note

If you choose to install a Normal Server, you must select the scanner type you want to install.

If you want to protect NetApp Devices using RPC, select **RPC**.

If you want to protect a storage device supporting ICAP, select **ICAP**.

If you want to protect Huawei OceanStor Storage, select **EMC CAVA**.

For details, see [Installing ServerProtect for Storage with EMC CAVA Scanner on page 2-31](#).

Make sure the selection of the components is adequate for the desired setup. You can choose hidden shared storage devices, such as **C\$** or **D\$**, as destination folders.

The default installation path is:

<drive>:\Program Files\Trend\SPProtect

**Note**

To protect the Information Server, Trend Micro recommends that you install a Normal Server on the computer where the Information Server managing is installed.

8. Click **Yes** on the pop-up dialog to continue installing Normal Server.
9. Click **Next**. If you chose to install either a Normal Server or an Information Server, the **Input Logon Information** screen will appear. Under **Logon Information**, type the appropriate data in the **Domain name**, **User name**, **Password**, and **Confirm Password** fields. Click **Next** to continue.

Input Logon Information

To install a Normal Server or an Information Server, you must enter the administrator account information of the target server. ServerProtect will run as this administrator account for network connection purposes.

Logon Information

Domain name:

User name:

Password:

Confirm password:

< Back Next > Cancel

FIGURE 2-6. Input Logon Information screen

10. Follow the instructions given in the following sections to complete the Installation.
-

Installing an Information Server

The Information Server carries out the commands issued by the Management Console and manages Normal Servers hosted by its Information Server domain(s).

Procedure

1. Execute the setup program and complete the necessary steps to provide product information.
2. Select the **Install server as a ServerProtect Information Server** check box on the **ServerProtect Select Components** screen. See [ServerProtect Select Components screen on page 2-15](#).
3. Click **Browse** to specify the path where you want to install the Information Server. The **ServerProtect Install Path Selection** screen appears.

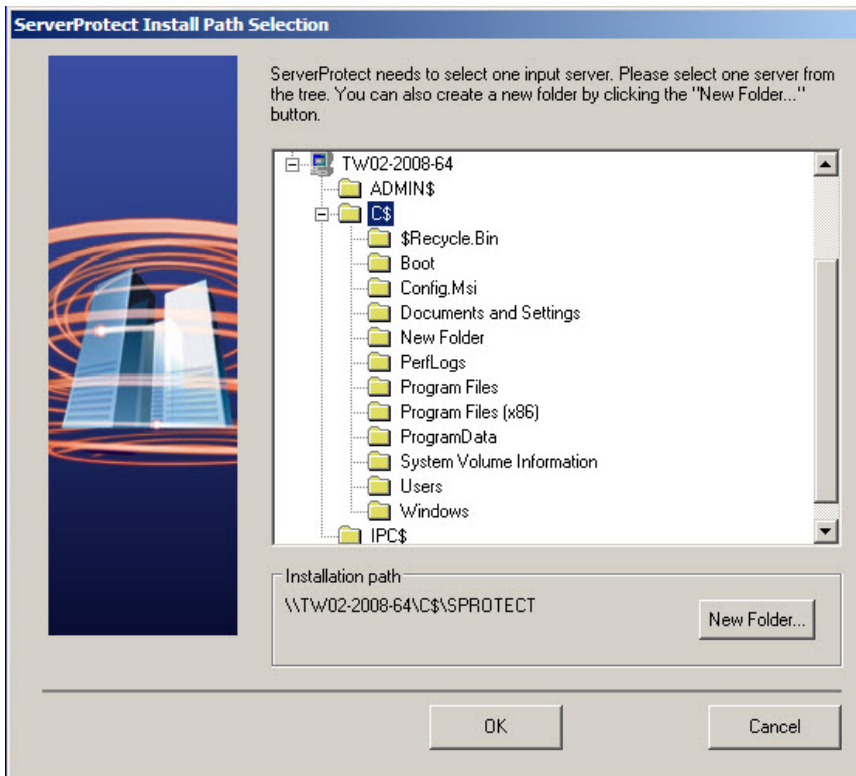


FIGURE 2-7. ServerProtect Install Path Selection screen

4. Double-click the target server and choose the installation path for ServerProtect Information Server files. Click **New Folder** if installation needs to be installed in a new folder. Click **OK** to bring back the **ServerProtect Select Components** screen. See [ServerProtect Select Components screen on page 2-15](#).
5. Click **Next**. The **Input Logon Information** screen appears. Under **Logon Information**, type the valid data in the fields of **Domain name**, **User name**, **Password**, and **Confirm Password** and click **Next**. The **ServerProtect Setup Information Server** screen appears.

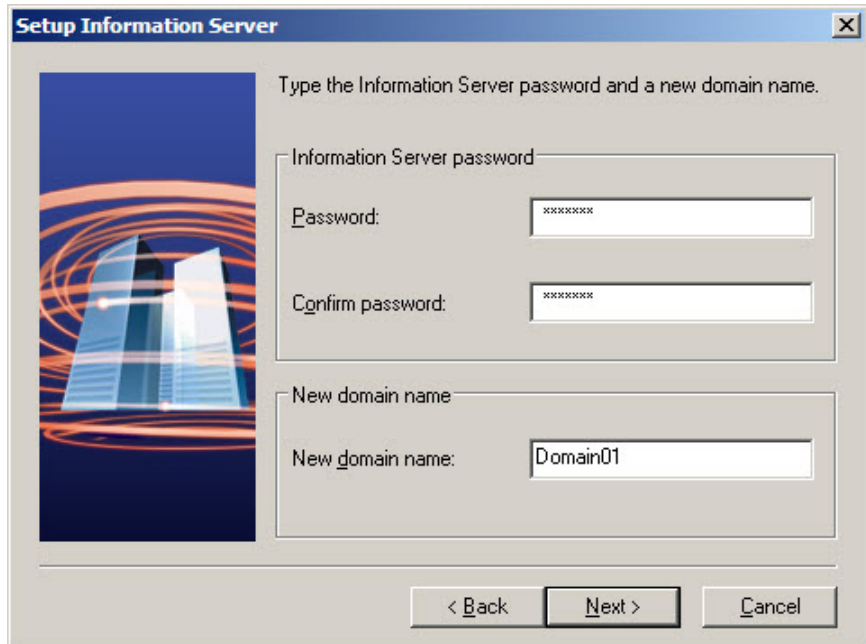


FIGURE 2-8. ServerProtect Setup Information Server screen

6. Provide a password and make the confirmation as requested. This prevents unauthorized access to this Information Server from either the Management Console or the setup program.
7. Click **Next**. The **Start Copying Files** window appears. Verify the information listed on the screen.
8. Click **Next** to continue with the setup program. ServerProtect now starts copying all program components and starts all services. After all program components have been copied and all services have started successfully, the **ServerProtect Setup** screen appears.

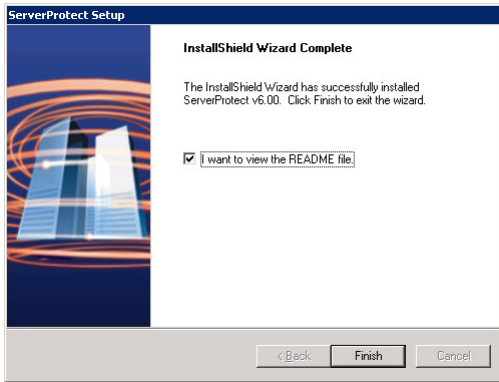


FIGURE 2-9. ServerProtect Setup Complete screen

9. Click **Finish**.
-

Installing the Management Console

Administrators can remotely manage ServerProtect Normal Servers using the Management Console. The Management Console is the ServerProtect component users interact with; it can be installed on the same computer along with the Information Server and the Normal Server, or on a different computer.

Procedure

1. Execute the setup program and complete the necessary steps to provide product information.
2. At the **Select Components** screen, select the **Install Management Console to local machine** check box. You can change the local installation path by clicking **Browse**. The Management Console must be installed in a Windows Storage Server environment.



Note

Trend Micro does not currently support remote installation of the Management Console.

3. If you want to be the only one to view the ServerProtect program from the Windows Start menu, click **Personal program folder**. Otherwise, click **Common program folder**.
4. Click **Next**. The **Select Program Folder** screen appears.
5. Select the folder where you want to install the program, and then click **Next**. The **Start Copying Files** screen appears.
6. Click **Next** to continue with the setup program. Setup starts copying all program components and starts all services. After all program components have been copied, the **ServerProtect Setup** screen appears.

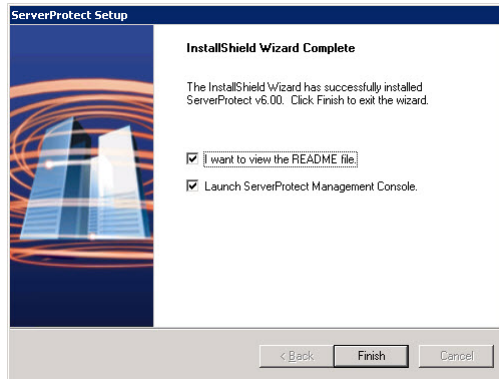


FIGURE 2-10. ServerProtect Setup Complete screen

7. Click **Finish**. The **Select an Information Server** window appears.

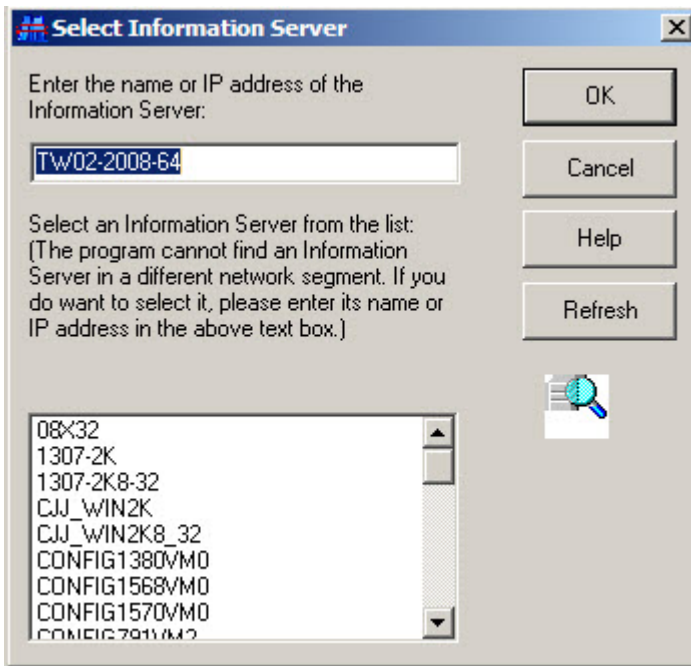


FIGURE 2-11. Select an Information Server screen

8. Select the Information Server that the Management Console will control. Do one of the following:
 - Select a server from the list.
 - Provide the name of the server.
 - Provide the IP address of the server.



Note

If an Information Server resides on a different network segment from the one where the Management Console is installed, the server will not appear in the list.

9. Click **OK** to save your changes or click **Cancel** to close the window without saving.
-

Installing a Normal Server

Use the setup program the first time you install a Normal Server. After that, use the Management Console to install additional Normal Servers.

Installing a Normal Server from the Setup Program

The setup program allows you to install a Normal Server both locally and remotely to the server network. The installation procedures for separately Normal Server of Microsoft Windows will be presented separately.

Procedure

1. Execute the setup program and provide the necessary product information.
2. Select the **Install server as a ServerProtect Normal Server** check box on the **Select Components** screen, and then select a scanner type you want to install. See [ServerProtect Select Components screen on page 2-15](#). Click **Browse** to locate the target server and folder where you want to install a Normal Server. The **ServerProtect Install Path Selection** screen appears.

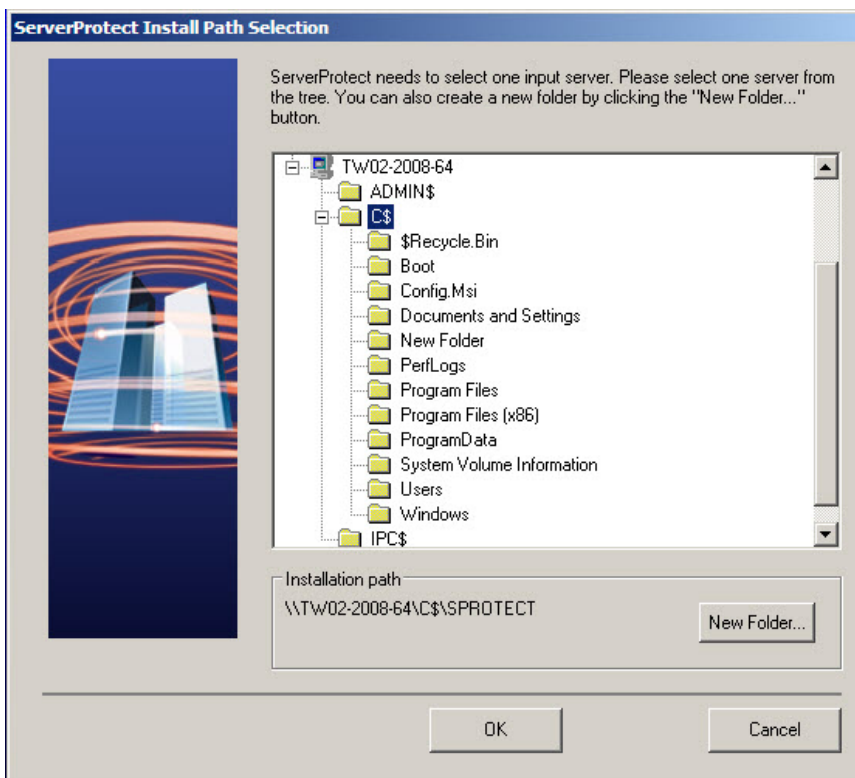


FIGURE 2-12. ServerProtect Install Path Selection screen with Windows Server

3. Click the appropriate network to expand the directory tree and select a target server.
4. Double-click on the target server. In the **Enter Password** screen subsequently appears, type an administrator user name and password and click **OK**. The target server's local drives appear on the tree.

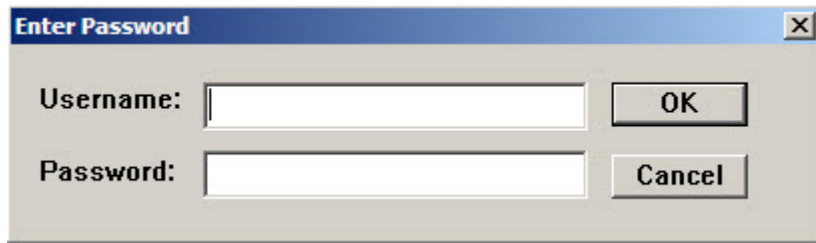


FIGURE 2-13. ServerProtect Target Server Logon screen

5. Select the installation path for the Normal Server. Click **New Folder** if installation needs to be installed in a new folder. Click **OK** to continue.
6. Click **Next** in the **ServerProtect Select Components** screen. The **Input Logon Information** screen appears.
7. Under **Logon Information**, type the appropriate data next to the **Domain name**, **User name**, **Password**, and **Confirm Password** fields.
8. Click **Next**, the **Select Information Server** screen appears.

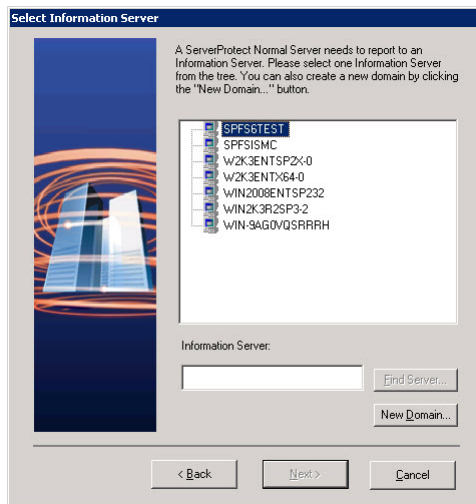


FIGURE 2-14. Select Information Server screen

9. To locate the Information Server, do one of the following:

- Type the name or IP address of the Information Server in the text box below the tree. Click **Find Server**.
 - Double-click the target server for the Information Server in the browser tree.
10. Click **New Domain** if a new ServerProtect domain is needed to host the Normal Server.

**Note**

If an Information Server resides on a network different from the one the Normal Server does, the server does not show up in the list. To locate the Information Server in this case, type the server name or the IP address in the **Information Server** fields.

11. Type the Information Server password and click **OK**. This password was assigned during Information Server installation.

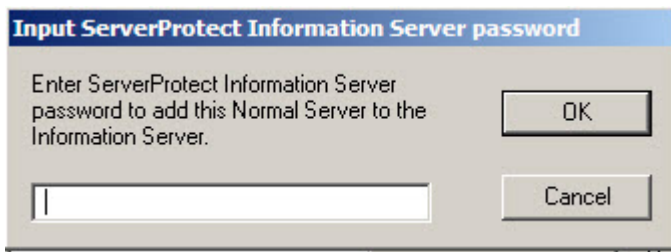



FIGURE 2-15. Input ServerProtect Information Password dialog

Click **Next**. The **Start Copying Files** dialog appears. Verify the information listed on the screen.

12. Click **Next** to continue with the setup program. ServerProtect now starts copying all program components and starts all services. After all program components have been copied and all services have started successfully, the **Setup Complete** screen appears.

13. Click **Finish**. An icon () will be added to your Windows taskbar, notifying you that the scanner is on.
-

Installing a Normal Server from the Management Console

It can be assumed at this point that the Information Server on which the Management Console is logged is already managing at least one Normal Server. This server will be used as a source for installing the new Normal Server, so it must be of the same type as the one that needs to be installed. For example, a Windows Storage server requires a Windows storage type server as its source. The system will select a Normal Server of the same type as the default source server if it is the one existing in the domain.



Note

While installing a Windows Normal Server from the Management Console, ensure that the operating system of the source and the target servers are of the same platform. For example, if the operating system of the source server is 32-bit, then the operating system of the target server should also be 32-bit.

Ensure that ServerProtect was not installed on the target server before.

Procedure

1. From the domain browser tree, select the domain to which you want to add a server. Do one of the following:
 - Select **Domain > Install New SPFS(s)** from the main menu.
 - Right-click the domain that you selected in the previous step and click **Install New SPFS(s)**.

The **Select a Source Server** window opens.

2. Select an existing Windows Normal Server and a scanner type that you want to install from the list box, and then click **OK**. A confirmation window appears. Click **OK** to bring up the **Add Server(s) to Domain** window.

3. Do one of the following to add a server to the domain:

- Select the server name in the left list box
- Type the server name in **Server name**.

Click **Add** to enter the server name into the right list box.

4. Repeat step 3 until the right list box displays all the servers that you want to add into the new domain. To remove a server previously added, highlight the name in the right list box and click **Remove**. Click **Remove All** to remove all those servers listed in the right list box.
5. Click **OK** to save the changes or click **Cancel** to close the window without adding a server.
-

Installing ServerProtect in Silent Mode

Installing ServerProtect in silent mode can be quite useful to remotely install Normal Servers under Microsoft Windows environment.

Procedure

1. Install an Information Server. See [Installing an Information Server on page 2-17](#).
 2. Locate the SMS folder in the default installation path, and share it.
-



Note

Share the SMS folder with read and write permissions.

Make sure the target servers you want to install as Normal Servers can access the folder. If you want to perform more than one silent installation, map the SMS folder on the target servers.

3. At the target server, navigate to the SMS folder or drive that is mapped to the folder, open the file `Setup.ini`, and then add one of the following lines at the end of the file to specify the scanner type:
 - To install Normal Server as RPC Scanner:

```
[CommonSection]
```

```
NormalServerType=1
```

- To install Normal Server as ICAP Scanner:

```
[CommonSection]
```

```
NormalServerType=2
```

- To install Normal Server as EMC CAVA Scanner:

```
[CommonSection]
```

```
NormalServerType=4
```



Note

If the `NormalServerType` in `Setup.ini` is not specified, the setup installs the Normal Server as EMC CAVA Scanner by default.

4. At the target server, open a command prompt, go to the SMS folder or drive that is mapped to the folder, and then enter the following command: `<drive>:\setup -SMS -s -m"SPFS"`

Example:

- a. At the target server, map the SMS folder to drive "M".
- b. Open a command prompt.
- c. Go to drive M: by typing `M:`.
- d. Type the following: `M:\setup -SMS -s -m"SPFS"`
- e. Press **Enter**.

Silent install will proceed and the target server will be registered with the Information Server.

For a silent installation, Normal Servers are installed in the "SMS" domain. There is no way to change the domain name during the silent installation. You can, however, rename the SMS domain after all the Normal Servers have been installed.

You can also specify a path to which ServerProtect is installed. For example, to install ServerProtect to the path "D:\Utility\AntiVirus\SProtect", do the following:

- a. Locate the Setup.ini file in the source folder.
- b. Add the following lines:

```
[CommonSection]
```

```
ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect
```

Where:

ServerTargetUNCPath: Sets the location where the Normal Server is installed.

To license the installed Normal Server, add the following lines to the Setup.ini file in the source folder.

```
[CommonSection]
```

```
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

Where:

XXXX-XXXX-XXXX-XXXX-XXXX: Represents the legal serial number.

You may not be able to register a Normal Server under the "SMS" domain due to the use of a domain controller on the Information Server. To resolve this issue, configure an IP address before using silent install. To configure an IP address, do the following:

- a. Go to the Setup.ini file in the SMS folder.
 - b. Replace the host name with its IP address next to AgentName then save the file.
-

Installing ServerProtect for Storage with RPC Scanner or ICAP Scanner

This section guides you through the ServerProtect for Storage with RPC Scanner or ICAP Scanner installation process.

Procedure

1. Install the Information Server. See [Installing an Information Server on page 2-17](#).
2. Install the Normal Server. See [Installing a Normal Server from the Setup Program on page 2-23](#).
3. Install the Management Console. See [Installing the Management Console on page 2-20](#). You can install additional Management Consoles on any Windows server or desktop system computer in the network.



Note

Only one Management Console can manage an Information Server at any given time.

-
4. Update ServerProtect pattern and scan engine files. See [Downloading Updates on page 3-34](#) and [Configuring Updates on page 3-31](#).
 5. Create additional ServerProtect domains to manage your Normal Servers. See [Creating ServerProtect Domains on page 3-11](#).
 6. Install the remaining Normal Servers using the Management Console. See [Installing a Normal Server from the Management Console on page 2-27](#).
- Steps 1, 2 and 3 can be executed simultaneously during the initial setup.
-

Installing ServerProtect for Storage with EMC CAVA Scanner

This section guides you through the ServerProtect for Storage with EMC CAVA Scanner installation process.

Before Installing ServerProtect for Storage with EMC CAVA Scanner

To ensure ServerProtect for Storage with EMC CAVA Scanner functions correctly, it is important that you perform the following pre-installation tasks in sequence before installing ServerProtect for Storage with EMC CAVA Scanner:

For ServerProtect for Storage with EMC CAVA Scanner:

1. Configure the AV User Account and Antivirus Group on the Windows Domain Server. For complete instructions, refer to the *EMC Celerra Event Enabler Technical Note*.
2. Install EMC Celerra Event Enabler (CEE)/EMC VNX Event Enabler (VEE), also known as Common Anti-Virus Agent (CAVA), on each server where ServerProtect Normal Server will be installed. Refer to the *EMC Celerra Event Enabler Technical Note* for the detailed instructions.

For Huawei OceanStor Storage:

1. Configure the AV User Account and Antivirus Group on the Windows Domain Server. For complete instructions, refer to the *Huawei OceanStor Storage Technical Note*.
2. Install Huawei Antivirus Agent on each server where ServerProtect Normal Server will be installed. Refer to the *Huawei OceanStor Storage Technical Note* for the detailed instructions.
3. Configure the Huawei OceanStor Storage to enable the antivirus feature. Refer to the *Huawei OceanStor Storage Technical Note* for the detailed instructions.

Installing ServerProtect for Storage with EMC CAVA Scanner

For Storage with EMC CAVA Scanner, make sure that CEE or VEE is already installed on the Windows Server where ServerProtect Normal Server will be installed. ServerProtect for Storage Normal is a part of the EMC antivirus system.

For Huawei OceanStor Storage, make sure that Huawei Antivirus Agent is already installed on the Windows Server where ServerProtect Normal Server

will be installed. ServerProtect for Storage Normal is part of the Huawei antivirus system.

Procedure

1. Install the Information Server. See [Installing an Information Server on page 2-17](#).
2. Install the Normal Server. See [Installing a Normal Server from the Setup Program on page 2-23](#).
3. Install the Management Console. See [Installing the Management Console on page 2-20](#). You can install additional Management Consoles on any Windows server or desktop system computer in the network.

**Note**

Only one Management Console can manage an Information Server at any given time.

-
4. Update ServerProtect pattern and scan engine files. See [Downloading Updates on page 3-34](#).
 5. Create additional ServerProtect domains to manage your Normal Servers. See [Creating ServerProtect Domains on page 3-11](#).
 6. Install the remaining Normal Servers using the Management Console. See [Installing a Normal Server from the Management Console on page 2-27](#).
- Steps 1, 2 and 3 can be executed simultaneously during the initial setup.
-

Removing ServerProtect

ServerProtect's three components can be removed either together or separately. Individual removal is discussed in the following sections.

Removing a Normal Server

There are two ways to remove a Normal Server:

To remove a Normal Server remotely:

1. Select the Normal Servers intended for removal from the Management Console.
2. From the main menu, navigate from **Domain > Uninstall ServerProtect**.

To remove a Normal Server locally:

1. Navigate from Windows Desktop's **Control Panel > Add/Remove Programs**.
2. Select the Normal Servers intended for removal and click the **Remove** button.

Removing an Information Server

The Information Server Service can only be removed locally.

Procedure

1. Click **Start > Control Panel > Add/Remove Programs**.
 2. Click **ServerProtect Information Server**, and then click **Remove**.
-

Removing the Management Console

The Management Console can only be removed locally.

Procedure

1. Click **Start > Control Panel > Add/Remove Programs**.
 2. Click **ServerProtect Management Console**, and then click **Remove**.
-

Chapter 3

Managing ServerProtect

This chapter covers the essential tools for managing ServerProtect. Additional management tools are explained in the online help of the Management Console.

The topics included in this chapter are:

- *Using the Management Console on page 3-3*
- *Managing ServerProtect Domains on page 3-10*
- *Managing Information Servers on page 3-14*
- *Managing Normal Servers on page 3-16*
- *Configuring Updates on page 3-31*
- *Deploying Updates on page 3-42*
- *Managing Tasks on page 3-47*
- *Configuring Notification Messages on page 3-64*
- *Scanning Viruses for Normal Server on page 3-71*
- *Using Real-Time Scan on page 3-80*
- *Using Scan Now (Manual Scan) on page 3-84*
- *Scheduled Scanning on page 3-90*

- *Selecting File Types to Scan on page 3-101*

Using the Management Console

ServerProtect allows you to manage virus protection over multiple Microsoft Windows network servers from a single, portable Management Console. It is password protected to ensure that only authorized users can change the settings of ServerProtect.

Opening the Management Console

The Management Console can run on any 32-bit or 64-bit Windows server or desktop computer on the network.

Procedure

1. Click **Start > Trend Micro ServerProtect Management Console**. The system prompts for the administration password to log on to the selected Information Server.

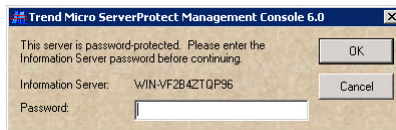


FIGURE 3-1. Trend Micro ServerProtect Management Console Logon window



Note

If you are managing more than one Information Server, you will be prompted to choose one from a list before proceeding.

2. Provide the valid password which is designated during the course of the Information Server installation. Click **OK** to continue. Note that the password is case-sensitive and that only one Information Server can be logged on at any given time.
3. If it is the first time for the ServerProtect to run on the system, a message box appears, indicating that new updates may be available on the Trend Micro ActiveUpdate Server to download and deploy. It is

highly recommend that an update be performed before using ServerProtect virus scan utilities on the network.

The Main Window View of the Management Console

The ServerProtect Management Console has an intuitive user interface that provides easy access to all the functions you need to configure and manage ServerProtect.

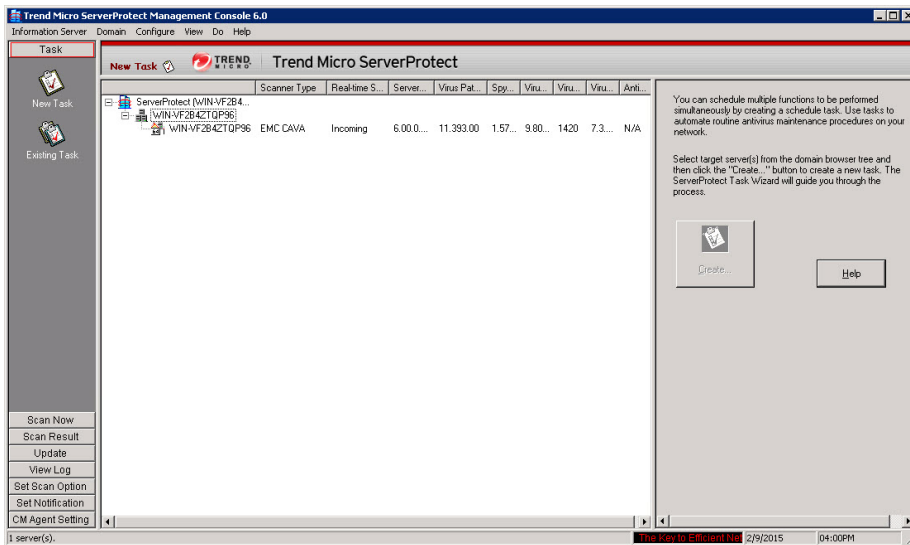


FIGURE 3-2. Management Console Elements

The Management Console has the following components:

- **Main Menu:** located below the title bar; contains six submenus, with each providing menu items for users to choose
- **Side Bar:** located on the left side of the application dialog, below the **Main Menu**; contains eight items, with each having additional options to choose

- **Domain Browser Tree:** located on the right of the **Side Bar** and below the **Main Menu**; the tree view presents the ServerProtect organization, including the **Information Server**, **Domain elements**, and **Normal Servers**
- **Configuration Area:** has a light gray background color on the right side of the main Window; provides information and UI elements to configure the virus scan and log report systems

Main Menu

The Main menu at the top of the screen includes:



- **Information Server:** Information Server configuration; for example, back up or restore the Information Server or move it on the network
- **Domain:** change the domain and server organization shown on the domain browser tree
- **Configure:** modify the scanning and log file configuration or set the console refresh frequency
- **View:** view ServerProtect log files, scan results, and the Trend Micro Virus Encyclopedia.
- **Do:**
 - **Create Task / Existing Task:** create or modify tasks
 - **Scan Now:** perform on-demand scans
 - **Update / Rollback:** update or roll back various ServerProtect antivirus elements
 - **Control Manager (CM) Agent Settings:** register, unregister and configure Trend Micro Control Manager settings
 - **Update Serial Number:** type a new serial number to replace an expired one
 - **Change Password:** change the IS password
 - **Find Domain:** find domains or servers

- **Connect to Server with STOP Sign:** use when the Normal Server is running and managed by one Information Server, but displays **STOP** in the Management Console
- **Submit File:** submit a suspicious file or a file that cannot be cleaned to the virus doctor at Trend Micro free of charge; virus doctor will clean the file and return it to you via e-mail
- **Create Debug Info:** manage log files that contain detailed debugging information and send them to Trend Micro technical support engineers for assistance
- **Send Feature Request:** use to send requests for new features that you would like to see added to ServerProtect
- **Help:** open the online help system or view the ServerProtect product information


Side Bar

The side bar is on the left side of the ServerProtect screen and includes seven groups of items. It provides shortcuts to different functional areas of the program.



- **Task Group**













-  **New Task:** To create a new task
-  **Existing Task List:** To view, run, modify, or delete an existing task

- **Scan Group**

-  **Scan Now:** To configure a manual virus scan

- **Scan Result Group**

-  **Real-time Scan:** To view the result of a real-time scan and EMC CAVA scanner
-  **Storage Scanner:** To view scan result of RPC Scanner and ICAP Scanner

-  **Scan Now:** To view the result of a manual scan
-  **Task Scan:** To view the scanning result performed by a task
- **Update Group**
 -  **Update:** To download and deploy updates to the Normal Servers located on the network
 -  **Rollback:** To roll back to a previous deployment action performed on your network
- **View Log Group**
 -  **View Log:** To view historical information about antivirus events that have occurred on the network
- **Set Scan Option Group**
 -  **Real-time Scan:** To configure a real-time virus scan on the network
 -  **Storage Scanner:** To configure Storage Scanner virus scan
 -  **Exclusion List:** To define files, directories, or viruses to be ignored by the ServerProtect virus scanning engine
 -  **Deny Write List:** To prevent certain files or directories from modification
- **Notification Group**
 -  **Standard Notification:** To configure a standard alert when the default condition is detected on the server
 -  **Outbreak Notification:** To configure an outbreak alert when many virus events occur over a relatively short period of time
 -  **CM Agent Settings:** To register, unregister and configure Trend Micro Control Manager settings

Domain Browser Tree

The browser tree displays the network components that your software is protecting and includes a root (the ServerProtect product icon), branches (domains), and nodes (the ServerProtect Normal Servers). There are four main visible items in the domain browser tree:

- Header
- Information Server
- Domain
- Normal Server

Header

The column fields above the domain browser tree display useful information, such as the computer's operating system, virus pattern, scan engine, program versions, real-time scan direction, and so on.

	Scanner Type	Real-time Scan	ServerProtect Progr...	Virus Pat...	Spy...	Viru...	Viru...	Viru...	Anti...
[-] ServerProtect [WIN-VF2B4...									
[-] WIN-VF2B4ZTQP96									

Right-click tree icons in the ServerProtect console to make configuration changes to the selected components. The frame that contains the domain browser tree can be resized.

Information Server



An Information Server is the server that handles key information and communication for domains. In addition, the Information Server links domains together.



An Information Server






Domain

Domains are groupings of servers on your ServerProtect network. Normal Servers that belong to a domain are managed together. ServerProtect domains are different from Windows domains.

-  A ServerProtect domain
-  A ServerProtect domain that includes an infected Normal Server

Normal Server

The Normal Server can be any server in which ServerProtect is installed on a network. In the ServerProtect architecture, a Normal Server is managed by the Information Server.

-  A Normal Server of 32-bit Microsoft Windows Server type
-  A Normal Server of 64-bit Microsoft Windows Server type
-  An infected Normal Server of 32-bit Microsoft Windows Server type
-  An infected Normal Server of 64-bit Microsoft Windows Server type
-  A Normal Server that has been disconnected or its service has been disabled

Configuration Area

On the right side of the ServerProtect screen is the configuration area, where you can type configuration data and view information about your corporate network.

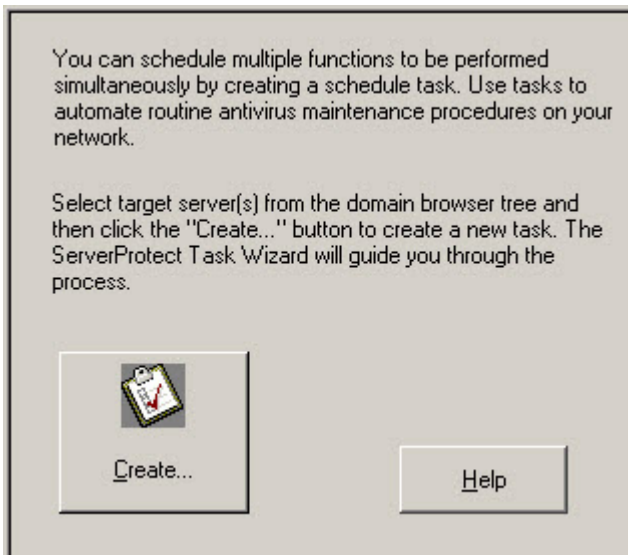


FIGURE 3-3. Configuration Area

Managing ServerProtect Domains

ServerProtect domains are virtual groupings of Normal Servers used to simplify their identification and management. You can create, rename, or delete domains according to the needs of your network.

**Note**

If one of the servers in a domain is infected, the domain icon will change and the infected server's icon will appear with a flame. This is to remind you to scan the infected server and prevent the virus from spreading throughout your network. To eliminate the infection icon(s), you need to purge all log entries under Scan Result in the Management Console, or simply open all these log entries.

Creating ServerProtect Domains

After creating a default domain through the ServerProtect installation program you can create a domain from the Management Console.

The maximum length of a domain name is 50 single-byte characters or 25 double-byte characters (for Chinese, Japanese, or Korean characters).

Procedure

1. Do one of the following:
 - Select the Information Server you want to add a domain. Navigate from the main menu **Domain > Add New Domain**.
 - Right-click the Information Server icon on the domain browser tree and then click **Add New Domain**.

The **Create New Domain** window appears.

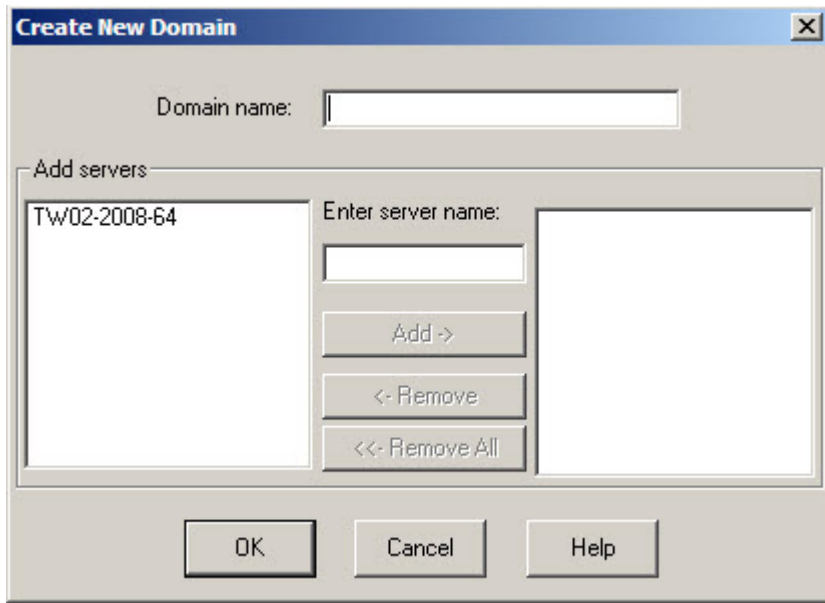


FIGURE 3-4. Create New Domain(s) window

2. Type a name in the **Domain name** field.
3. Identify the servers that you want to add to the domain. Do one of the following:
 - Select a server from the list on the left of the screen.
 - Type the server name in the **Enter server name** field.
4. Click **Add**.
5. Repeat steps 3 and 4 until the list on the right displays all the servers that you want to add in the new domain. To remove a server, select it in the list on the right and click **Remove**. Click **Remove All** to delete all the servers from the list on the right.

6. Click **OK** to save your changes or click **Cancel** to close the window without creating a new domain.
-

Renaming ServerProtect Domains

A domain with your server's name is created as the default domain during ServerProtect installation. You can change the name of any existing domain from the Management Console.

Procedure

1. Select the domain you want to rename in the domain browser tree.
2. Do one of the following:
 - Right-click the selected domain, and then click **Rename Domain**.
 - Select **Domain > Rename Domain** on the main menu.
 - Press the **F2** key on the keyboard.

The **Rename a Domain** window appears.

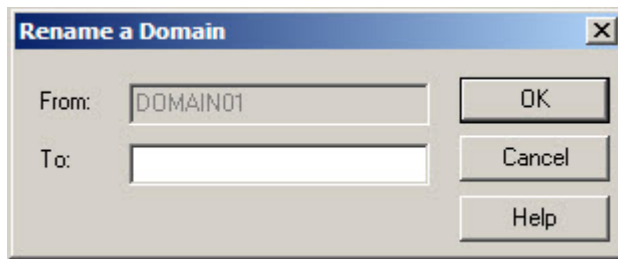


FIGURE 3-5. Rename a Domain window

3. Type the new domain name in the **To** text box and then click **OK**. Click **Cancel** to close the window without saving.
-

Deleting ServerProtect Domains

You can delete empty domains (domains that do not include any Normal Servers) you no longer need. You cannot delete a domain if it contains any Normal Servers.

Procedure

1. Select the domain that you want to delete on the domain browser tree.
2. Do one of the following:
 - Right-click the domain and then click **Delete Domain**.
 - Click **Domain > Delete Domain** on the main menu.
 - Press the **Delete** key of the keyboard.



Note

You cannot delete a domain if it contains any Normal Servers.

Moving Normal Servers between Domains

To improve management, sometimes you need to move (remove and add) Normal Servers from one domain to another. Select Normal Server(s) under one domain from the domain browser tree, then drag and drop between domains.

Alternatively, you can move a Normal Server when you create a ServerProtect domain. See [Creating ServerProtect Domains on page 3-11](#).

Managing Information Servers

The Information Server stores and delivers data to and from the Normal Servers. In a Windows Server network, the Normal Servers deliver their alert notifications to the Windows server.

Because an Information Server is simply a delivery system for information, the number of servers it can manage is, theoretically, only limited by the available bandwidth.

**Tip**

For large networks such as WANs, Trend Micro recommends that you install an Information Server in each network segment. This will reduce the impact on traffic.

Selecting Information Servers

Management Consoles can switch between Information Servers. However, only one Management Console can log on to an Information Server at any time. If you are not able to log on to an Information Server, verify whether another Management Console is connected to it.

Procedure

1. Click **Information Server** > **Select Information Server** on the main menu.

The **Select Information Server** window appears.

2. Do one of the following:
 - Type the name or IP address of the Information Server.
 - Select the Information Server from the list.

Note that if more than one network interface cards (NIC) are installed on the computer, only those Information Servers that connect to the primary NIC are visible in the list box window. To refresh the view of servers in the list, click **Refresh** button.

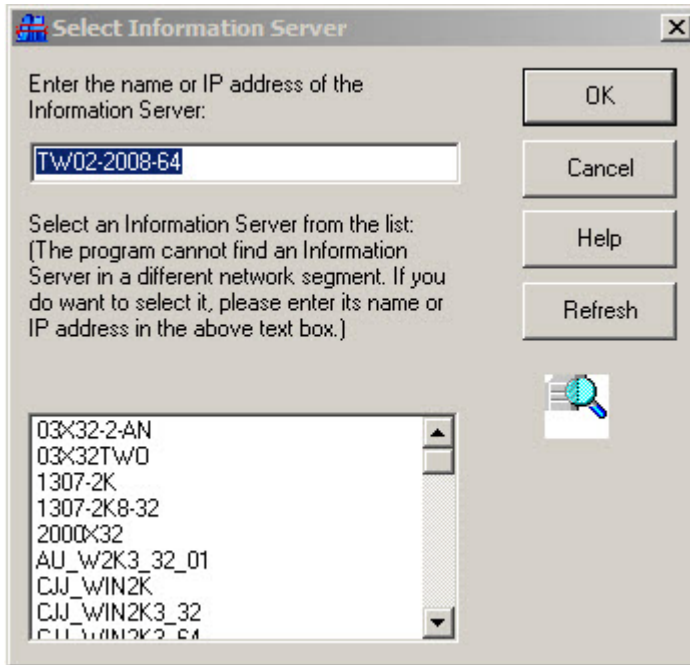


FIGURE 3-6. Trend Micro ServerProtect Management Console window

3. Click **OK** to save your changes or click **Cancel** to close the window without saving.

Managing Normal Servers

In the ServerProtect architecture, the Normal Server is the first line of defense against viruses, and is managed by an Information Server. It is at the bottom of the three-tier ServerProtect structure. This section explains how to manage Normal Servers.

Moving a Normal Server between Domains

To move a Normal Server from one ServerProtect domain to another, select a Normal Server in the domain browser tree, then drag and drop it between domains.

Moving a Normal Server between Information Servers

ServerProtect allows you to move a Normal Server from one Information Server to another. This feature is particularly useful to reduce the load on the Information Server.



Note

You can not use **Move NS(s) to Another IS** function to move one old normal server into ServerProtect 6.0 Information Server.

Procedure

1. Do one of the following:
 - Right-click the Normal Server that you want to move and then click **Move NS(s) to Another IS**.
 - Select the Normal Server that you want to move and then click **Domain > Move NS(s) to Another IS** in the main menu. The **Select Destination Information Server** window appears.
 2. Select the destination Information Server and submit it by clicking on the **OK** button. A dialog box **Move NS(s) to Another IS** dialog box appears.
 3. Fill either the **User Name/Password** fields or that of **GUID** with proper values. Submit the dialog box by clicking on the **OK** button.
-

Managing NetApp Devices in Scan Server

A Scan Server with RPC Scanner can protect multiple NetApp 7-Mode Devices and a Cluster-Mode AV Connector at the same time. Use the

ServerProtect Management Console to conveniently add NetApp 7-Mode Devices and a Cluster-Mode AV Connectors to a Scan Server.

You can also assign several Scan Servers to individual NetApp Devices for load balancing. See [Using Multiple Scan Servers for Single NetApp Devices on page 3-21](#).

Adding a NetApp 7-Mode Device

To add a NetApp 7-Mode Device in ServerProtect for Storage, you need the following:

- An account on the NetApp 7-Mode Devices with backup operator privileges or above
- NetApp 7-Mode Devices name or IP address

Procedure

1. Right-click a Normal Server, and then select **Devices List** on the domain browser tree.

The **Devices List** screen appears.

2. Click **Add**.

The **Add Devices** screen appears.

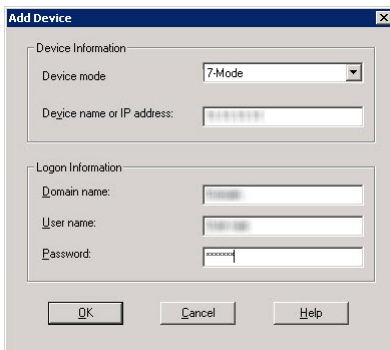


FIGURE 3-7. Add Devices Screen (1)

3. Do the following:
 - Select **7-Mode Devices** from the **Devices mode** drop-down list box.
 - In the **Devices name or IP address** text box, type the name or IP address of the NetApp 7-Mode Devices.
 - In the **Domain name** text box, type the name of the domain where the NetApp 7-Mode Devices is located.

**Note**

The domain name refers to the Windows domain in which NetApp 7-Mode Devices will authenticate registered users.

- In the **User name** and **Password** text boxes, type your NetApp 7-Mode Devices logon credentials (requires backup operator or above privileges).
4. Click **OK**.
-

Adding a Cluster-Mode AV Connector

To add a NetApp Cluster-Mode AV Connector in ServerProtect, you need the following:

- An account that has been added to privileged users on all Cluster-Mode Devices managed by the Cluster-Mode AV Connector

Procedure

1. Right-click a Normal Server, and then select **Devices List** on the domain browser tree.

The **Devices List** screen appears.

2. Click **Add**.

The **Add Devices** screen appears.

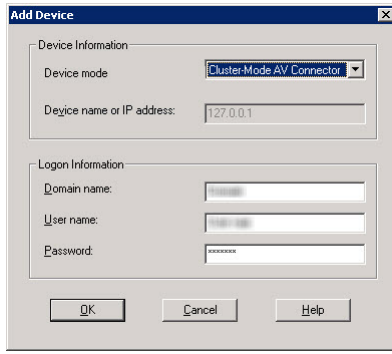


FIGURE 3-8. Add Devices Screen (2)

3. Do the following:
 - Select **Cluster-Mode AV Connector** from the **Devices mode** drop-down list box.
 - In the **Domain name** text box, type the name of the domain where the NetApp Cluster-Mode AV Connector is located.
 - In the **User name** and **Password** text boxes, type your NetApp Cluster-Mode AV Connector logon credentials.



Note

If a Cluster-Mode AV Connector manages multiple Cluster-Mode Devices, the logon account must be one of the privileged users on all Cluster-Mode Devices managed by the Cluster-Mode AV Connector. Refer to your NetApp Devices documentation for details.

4. Click **OK**.

**Note**

If the server computer, on which ServerProtect is to be installed, is running Windows Server 2008 or later releases of Microsoft Windows, add the Devices and the Scan Server into certain specified domains, and add their IP addresses in Forward Lookup and Reverse Lookup zones.

Moreover, if the Devices and Scan Server are in different domains, you must add the two domains in the Trust list by creating domain Trust.

Using Multiple Scan Servers for Single NetApp Devices

ServerProtect for Storage provides a fully scalable enterprise antivirus solution for organizations using NetApp Devices.

If there is a large volume of incoming files to the NetApp Devices, adding and registering multiple Scan Servers with the NetApp Devices evenly distributes the workload among the registered Scan Servers.

NetApp Devices send files to Scan Servers in "round-robin" fashion. For example, if you have three Scan Servers and the NetApp Device has four incoming files, the first Scan Server scans the first file, the second Scan Server scans the second file, the third Scan Server scans the third file, the first Scan Server scans the fourth file, and so on.

This even distribution of the workload reduces the loading of Scan Servers (load balancing).

The following procedure describes how to confirm that multiple Scan Servers are working for a single NetApp Device.

Procedure

1. Open the command prompt for the NetApp Device that you want to verify.
2. At the command prompt, type:

```
netapp> vscan scanners
```

The NetApp Device displays a list of Scan Servers by IP address and NetBIOS name.

Removing a NetApp 7-Mode Device or Cluster-Mode AV Connector from Scan Server

In several instances, it may be necessary to remove (delete) a NetApp 7-Mode Device or Cluster-Mode AV Connector from a Scan Server, for example, when changing, upgrading, or renaming a NetApp 7-Mode Device or Cluster-Mode AV Connector. To remove a NetApp 7-Mode Device or Cluster-Mode AV Connector, do the following:

Procedure

1. Right-click a Scan Server, and then select **Device List** on the domain browser tree. The **Device List** screen appears.
 2. Select one or more NetApp 7-Mode Devices or Cluster-Mode AV Connectors from the list. To select multiple several NetApp 7-Mode Devices or Cluster-Mode AV Connectors, press the **CTRL** key as you select.
 3. Click **Remove**. The **Remove Device** confirmation screen appears.
 4. Click **OK**.
-

Configuring NetApp 7-Mode Device or Cluster-Mode AV Connector Options

This section introduces the necessary information for configuring NetApp 7-Mode Device or Cluster-Mode AV Connector related settings from the Management Console.

Updating NetApp 7-Mode Device or Cluster-Mode AV Connector Information

Changing a NetApp 7-Mode Device's or a Cluster-Mode AV Connector's system information will require updating the logon information of the

NetApp 7-Mode Device or Cluster-Mode AV Connector in ServerProtect for Storage with RPC Scanner.

The following information is necessary to update a NetApp 7-Mode Device's system information in ServerProtect for Storage with RPC Scanner:

- An account on the NetApp 7-Mode Device with backup operator privileges or above
- NetApp 7-Mode Device name or IP address

Procedure

1. Right-click a Scan Server, and then select **Device List** on the domain browser tree.

The **Device List** screen appears.

2. Select one or more NetApp 7-Mode Devices from the list. To select multiple NetApp 7-Mode Devices, press the **CTRL** key as you select.

3. Click **Logon Info**.

The **Logon Information** screen appears.

4. Do the following:
 - In the **Domain name** text box, type the name of the domain where the NetApp 7-Mode Device is located.
 - In the **User name** and **Password** text boxes, type your NetApp 7-Mode Device logon credentials (requires backup operator or above privileges).
5. Click **Apply** to update the NetApp 7-Mode Device information.

The confirmation screen appears.

6. Click **OK**.

The following information is necessary to update a Cluster-Mode AV Connector's system information in ServerProtect for Storage:

- An account that has been added to privileged users on all Cluster-Mode Devices managed by the Cluster-Mode AV Connector

The procedure for updating a Cluster-Mode AV Connector's system information is similar to the procedure for updating a NetApp 7-Mode Device's system information.

Using Scan Servers as Normal Servers

Although the ideal configuration is to have a machine act primarily as a Scan Server to protect the NetApp Device, there may be situations where a Scan Server must also serve as an organization's Normal Server (file server, data server, etc.).

If you choose to use a Scan Server as a Normal Server, the Normal Server's Real-time Scan function is enabled by default.

Real-time Scan has the following options:

- incoming (default)
- outgoing
- incoming & outgoing



Note

For the highest level of security set Real-time Scan to **Incoming & outgoing**. However, if the computer only performs as a Scan Server, you can use the default setting (**Incoming**).

The following procedure describes how to set Real-time Scan to Incoming & outgoing.

Procedure

1. Select either the Information Server, domain, or a Normal Server (Scan Server) on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option > Real-time Scan** on the side bar

- Click **Configure > Scan Options > Real-time Scan** on the main menu

The **Real-time Scan configuration** screen appears.

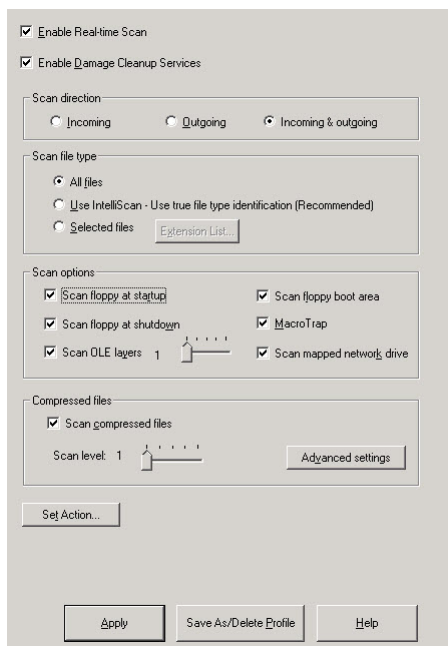


FIGURE 3-9. Real-time Scan Configuration Screen

3. Under **Scan direction**, click **Incoming & outgoing**.
4. Click **Apply**.

For more information about Real-time Scan, refer to [Using Real-Time Scan on page 3-80](#).

Notifying NetApp Device clients upon infection

ServerProtect can notify the user and the Network Administrator if a NetApp Device client has uploaded or accessed an infected file. The notification function is enabled by default.

Procedure

1. Right-click a Scan Server, and then select **Device List** on the domain browser tree. The **Device List** screen appears.
2. Click **Options**. The **Global Device Options** screen appears.

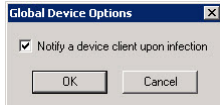


FIGURE 3-10. Global Device Options Screen

3. Select **Notify a device client upon infection**.
4. Click **OK**.



Note

This setting will affect all the NetApp Devices in the Devices list.

Viewing the status of a NetApp Device

You can see the status of a NetApp Device through the Management Console. NetApp Devices may appear offline for one of the following reasons:

- The NetApp Device is shut down or is not responding
- The network is not available
- The NetApp Device did not successfully register with the Information Server

Procedure

1. Right-click a Scan Server, and then select **Device List** on the domain browser tree. The **Device List** screen appears.

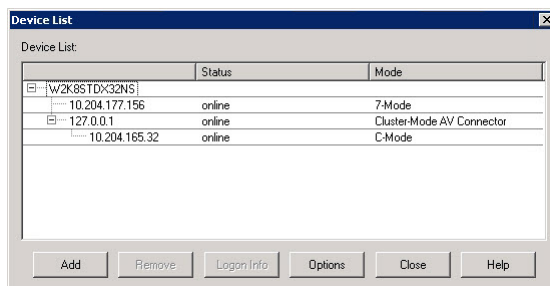


FIGURE 3-11. Device List Screen

2. Verify the status of a NetApp Device by looking at the **Device name**, **Status** and **Mode** fields in **Device List**.

7-Mode Devices, Cluster-Mode AV Connector or Cluster-Mode Devices may appear as **online** or **offline**.

Configuring NetApp Device RPC Connection Status Notifications

ServerProtect can notify the network administrator whenever an RPC connection to a NetApp Device succeeds or fails.

Procedure

1. Select the Information Server, domain, or a Normal Server on the domain browser tree.
2. Do one of the following:
 - Select **Configure > Notifications > Standard Alert** from the main menu.
 - Click **Set Notification**, and then **Standard Alert** on the side bar.
3. Select **Device RPC Connection Success/Failure**.

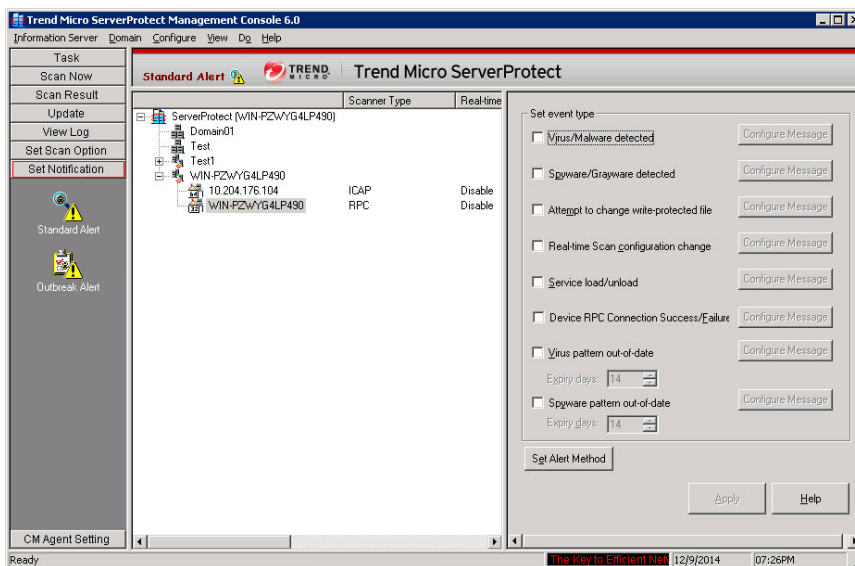


FIGURE 3-12. Standard Alert Configuration Screen

4. Click **Configure Message** to set up a customized notification message.

For additional information, refer to [Configuring Notification Messages on page 3-64](#).

Notifying NetApp Devices of New Update Components

When update downloads new components (scan engine and pattern) to the Scan Server, the Scan Servers will notify NetApp Device to flush the cache of previously scanned files. This ensures that all files are scanned with the latest virus pattern. Each NetApp Device will then begin rebuilding the cache of previously scanned files until a new update arrives from the update server.

For more information on downloading updates. See [Downloading Updates on page 3-34](#).

Managing ICAP Client List in Scan Server

A Scan Server with ICAP Scanner provides protection to the storage devices with ICAP client. You can configure Scan Server to accept a scan request from any ICAP client or only from those on the ICAP Client List.

Accepting a Scan Request from ICAP Clients

The following procedure describes how to accept a scan request from any ICAP client or from ICAP clients that exist in ICAP Client List only.

Procedure

1. Right-click a Normal Server, and then select **ICAP Client List** on the domain browser tree.

The **ICAP Client List** screen appears.

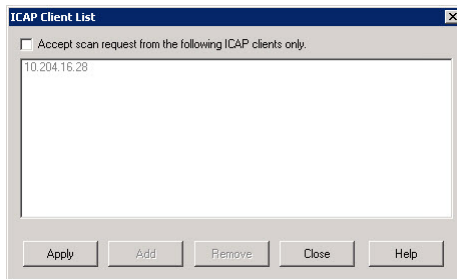


FIGURE 3-13. The ICAP Client List

2. Do one of the following:
 - To accept scan request from the ICAP clients that exist in the ICAP Client List only, select **Accept scan request from the following ICAP clients only** checkbox.
 - To accept a scan request from any ICAP clients, clear the **Accept scan request from the following ICAP clients only** checkbox.
3. Click **Apply**.

Adding an ICAP Client to ICAP Client List

Procedure

1. Right-click a Normal Server, and then select **ICAP Client List** on the domain browser tree.

The **ICAP Client List** screen appears.

2. Click **Add**.

The **Add ICAP Client Address** screen appears.

3. Do one of the following:

- Select **IP/Hostname** and type the IP address or the Hostname to add single ICAP Client.
- Select **IP Range** and type the IP range to add multiple ICAP clients.

4. Click **OK**.
-

Removing an ICAP Client or IP Range from ICAP Client List

Procedure

1. Right-click a Normal Server, and then select **ICAP Client List** on the domain browser tree.

The **ICAP Client List** screen appears.

2. Select an ICAP client or the IP range from the list. To select multiple entries, press the **CTRL** key as you select.

The **Add ICAP Client Address** screen appears.

3. Click **Remove**.
-

Configuring Updates

Trend Micro update server allows you to update ServerProtect components. The update process comprises downloading and deploying the updates.

Update Components

The following are the ServerProtect components that you can update:

- **Virus pattern file:** Trend Micro antivirus scan software uses a detection method called pattern matching. Files on a computer are examined and compared to the virus pattern file that contains the "electronic fingerprint" of thousands of known computer viruses. If a file on your computer matches one in the pattern file, the antivirus scan software detects it as being infected.
- **Spyware pattern file:** The spyware pattern identifies spyware/grayware in files, programs and modules in memory, Windows registry and URL shortcuts.
- **Scan engine (for 32-bit and 64-bit Windows and NetWare platform):** The scan engine is the software component that performs the actual virus detect operations.
- **Virus Cleanup Engine (for 32-bit and 64-bit Windows):** the Engine scans for and removes Trojans and Trojan processes. It supports 32-bit and 64-bit platforms.
- **Virus Cleanup Template:** The Virus Cleanup Template is used by the Virus Cleanup Engine to identify Trojan files and processes so the VCE can eliminate them.
- **Anti-Rootkit Driver (for 32-bit Windows only):** Anti-rootkit Driver is a kernel mode driver used by the Damage Cleanup Engine that provides functionality to bypass any potential redirection by rootkits.

How Updates Work

The following figure shows how ServerProtect deals with a typical request to download and deploy updates in a ServerProtect network.

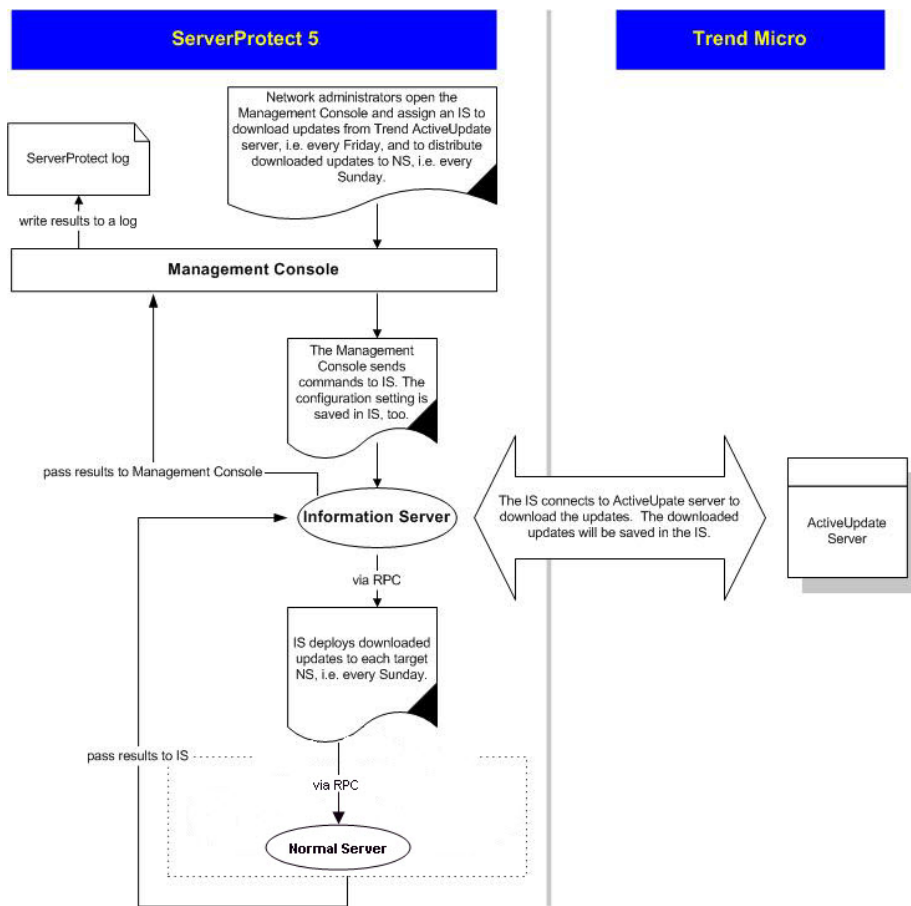


FIGURE 3-14. How Updates Work

Verifying the Current Version of Files

ServerProtect allows you to check the version of the virus pattern file and scan engine currently used by an Information Server.

To verify the current version do one of the following:

- Click **Update** > **Update** on the side bar.
- Click **Do** > **Update** on the main menu.

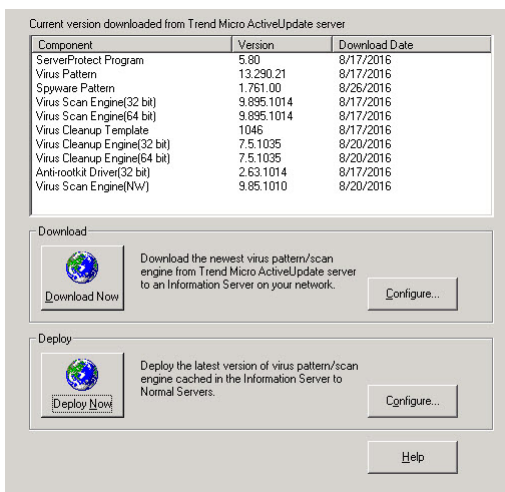


FIGURE 3-15. Trend Micro ServerProtect Update Main Screen

The following version information used by the system are shown at the top of the **Update** screen.

- ServerProtect version
- Virus Pattern version
- Spyware Pattern version
- Virus Scan Engine version (32-bit /64-bit)
- Virus Cleanup Template version

- Virus Cleanup Engine version (32-bit /64-bit)
- Anti-rootkit Driver version (32-bit only)

After installing ServerProtect for the first time, the version fields are displayed. Updated information will be displayed after you perform a successful update by clicking **Download Now** to download the latest updates from the Trend Micro update server.

Downloading Updates

We recommend that you regularly download updates from the Trend Micro update server to ensure continued protection. Trend Micro releases new virus pattern files several times each week. The scan engine files, on the other hand, are updated less frequently.

After downloading updates from the Trend Micro update server, you can designate a network drive to act as a download source (mirror) for other Information Servers on your network. This will avoid redundant downloads.

Downloading updates from a network drive is ideal for large networks (such as Intranets) with multiple Information Servers. Before attempting to download update files from another server, you must make sure the source server has the updated files.

Configuring a Download Source

You can download updated files from Trend Micro update server or copy the files from a location on your network. If you want to copy files from a location on your network, you must create a download source folder.

Setting Trend Micro Update Server as the Download Source

Procedure

1. Do one of the following:
 - Click **Update** > **Update** on the side bar.
 - Click **Do** > **Update** from the main menu.

2. Click **Configure** in the **Download** group to open the **Download Option** window.
3. Click **Internet** and then type the following URL to download the update files from the Trend Micro update server:

```
http://spfs60-p.activeupdate.trendmicro.com/activeupdate
```

4. Click **OK**. The downloaded files will be saved in the following directory of the Information Server:

```
\ProgramFiles\Trend\SProtect\SpntShare
```

Setting a Local or Network Drive as the Download Source



WARNING!

In order to download updates from a local or network drive, you must first create a download source folder. For details, see [Creating a Download Source Folder on page 3-36](#).

Procedure

1. Do one of the following:
 - Click **Update > Update** on the side bar.
 - Click **Do > Update** from the main menu.
2. Under **Download**, click **Configure**.
The **Download Option** window appears.
3. Click **From a local or network drive**.
4. Type the UNC path where the files are being kept to download the update files from another server on you network. Use UNC format, rather than mapped drive format to identify the source server.

For example:

```
\\servername\foldername
```

5. Type the **User name** and **Password** to access the source server. The server you are updating from must have previously downloaded a copy of the update files.
 6. Click **OK**.
-

Creating a Download Source Folder

Procedure

1. Execute an update from the Internet by clicking **Download Now**.
 2. Do one of the following:
 - Make the SpntShare folder, located under <drive>:\ProgramFiles\Trend\SProtect\ in the designated Information Server, a shared folder.
 - Create a shared folder on a network server and then copy all the files in the SpntShare folder to the mentioned shared folder.
-



Note

If you do not select the SpntShare folder as your download source, you need to copy all the files in the SpntShare folder of the designated Information Server to the mentioned shared folder every time you execute an update from the Internet.

Using Download Now

If updated components are available, you can initiate an immediate download of the latest virus pattern files and scan engine files from either the Trend Micro update server or another Information Server on your network.

Procedure

1. Do one of the following:

- Click **Update > Update** on the side bar.
 - Click **Do > Update** from the main menu.
2. Click **Download Now** on the **Update** main screen.

A progress bar appears to show the time remaining until the completion of the update.

**Note**

Before you use **Download Now** for the first time, you need to configure the download settings. Failure to do so, could prompt an "Source network generic failure" or "HTTP timeout" message when you click **Download Now**. For details, see [Configuring Download Settings on page 3-39](#).

ServerProtect logs the event in the Information Server logs.

Configuring a Scheduled Download

You can schedule ServerProtect to download the latest update files from Trend Micro or another server on your network.

Procedure

1. Do one of the following:
 - Click **Update > Update** on the side bar.
 - Click **Do > Update** from the main menu.
2. Under **Download**, click **Configure**.
The Download Option window appears.
3. Click the **Schedule Setting** tab.

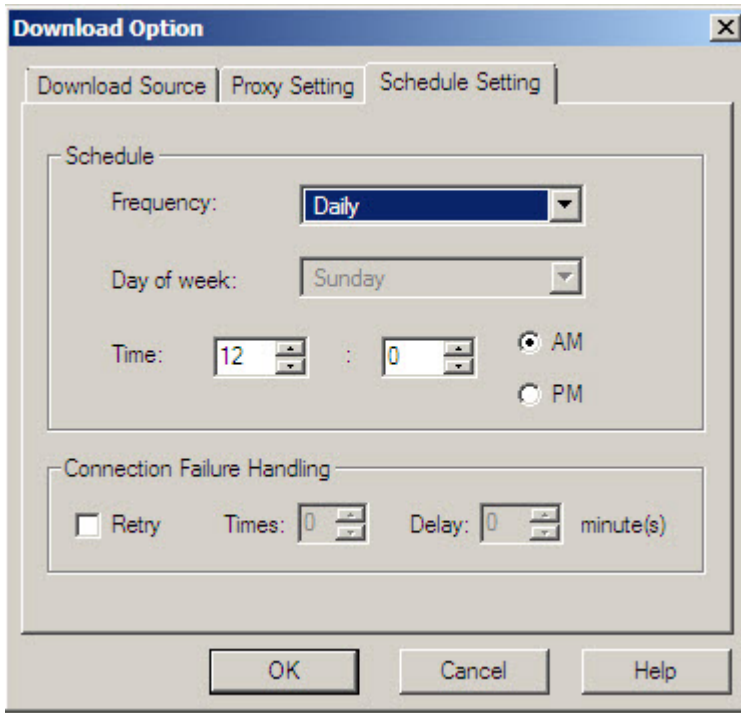


FIGURE 3-16. Download Option - Schedule Setting window

4. Under **Schedule** in the **Frequency** list, click a download frequency. You can select **None**, **Hourly**, **Daily** or **Weekly**. If you do not want to schedule a download, click **None**. If you click **Weekly**, in the **Day of Week** list, click a day.
5. In the **Time** box, type or select the time when you want to update the components, and then click **AM** or **PM**.
6. Select the **Retry** check box to instruct ServerProtect to attempt to reconnect to the download server if the initial download operation is unsuccessful. In the **Times** and **Delay** boxes, type or select the number of times and the delay you want between each retry.
7. Click **OK**.

The downloaded files will be saved under the following directory:

\Trend\SProtect\SptShare

Configuring Download Settings

The following steps describe how to download the update files.

Configuring the Download Settings

Procedure

1. Do one of the following:
 - Click **Update** > **Update** on the side bar.
 - Click **Do** > **Update** from the main menu.
2. Click **Configure** on the **Update** screen to change your download configuration.

The **Download Option** window appears.

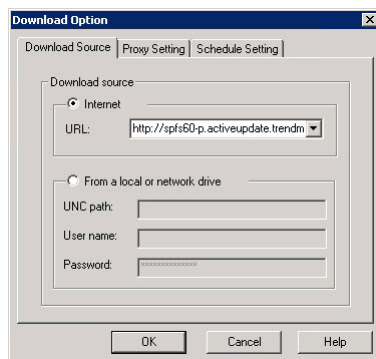


FIGURE 3-17. Download Option window

Configuring the Proxy Server Settings

You can configure ServerProtect to use your proxy server settings while connected to the Internet.

Procedure

1. Do one of the following:
 - Click **Update** > **Update** on the side bar.
 - Click **Do** > **Update** from the main menu.
2. Under **Download**, click **Configure**.
The **Download Option** window appears.
3. Click the **Proxy Setting** tab.

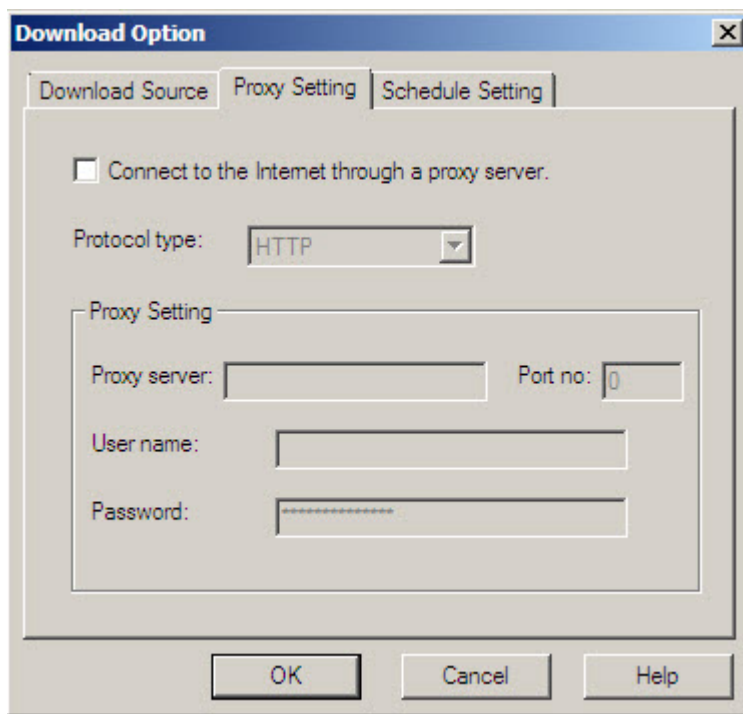


FIGURE 3-18. Download Option - Proxy Setting window

4. Select the **Connect to the Internet through a proxy server** check box.
5. In the **Protocol type** list, click the protocol used for downloading. The protocols supported are: HTTP and SOCK4.
6. Under **Proxy Setting** do the following:
 - In the **Proxy Server** and **Port no** text boxes, type the name of the proxy server and the port number used.
 - In the **User name** and **Password** text boxes, type the appropriate information for the proxy server.
7. Click **OK**.

Deploying Updates

When an Information Server deploys updates to Normal Servers, it sends commands to each Normal Server, requesting them to obtain a copy of the updates. ServerProtect records both the connection and deployment process in a log file.

Configuring Deploy Now

The **Deploy Now** function is used to deploy the updates saved in an Information Server to other Normal Servers.

Procedure

1. Do one of the following:
 - Click **Update > Update** on the side bar.
 - Click **Do > Update** from the main menu.
2. Click **Deploy Now**. A confirmation window appears. Click **Yes** to proceed with the manual update deployment.

The **Deploy** window appears.

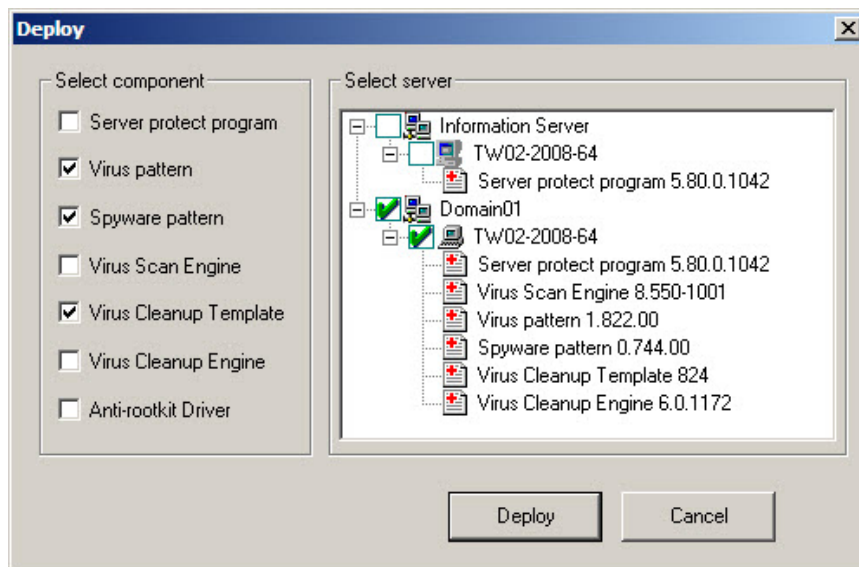


FIGURE 3-19. Deploy window

A number of check boxes in the **Select Component** group present those components readily to be deployed to the Normal Servers. The check boxes of **Virus pattern**, **Spyware** and **Virus cleanup Template** are selected at the application initiation stage as part of default configuration settings. In **Select server** pane, the version information of each downloaded ServerProtect antivirus elements is shown in the tree view UI element. For a 64-bit Window server, the available check boxes presented in the **Select Component** group are the **Server protect program**, the **Virus pattern**, the **Spyware pattern**, the **Virus Scan Engine**, the **Virus Cleanup Template** and the **Virus Cleanup Engine**. For a 32-bit Windows Server, an **Anti-rootkit Driver** check box, together with the six elements for 64-bit Windows described, is also presented.

3. To apply intended antivirus protections, set the check boxes corresponding to these components in **Select Component** Group, then

set the check boxes corresponding to those Normal Servers need to be deployed in the **Select server** tree view UI element.

4. Click **Deploy** to deploy the downloaded elements.
-

Configuring a Scheduled Deployment

After downloading updates on a scheduled basis, configure a scheduled deployment task to distribute the most recent updates to the Normal Servers.

ServerProtect creates a deploy task by default. See [Default Tasks on page 3-50](#).

For more information on how to configure a scheduled task, refer to [Creating Tasks on page 3-50](#).



Tip

When setting the time for downloading and deploying updates, be sure to set the download time before the deployment.

Procedure

1. Do one of the following:
 - Click **Update** > **Update** on the side bar.
 - Click **Do** > **Update** from the main menu.
2. Click **Configure** in the **Deploy** section.

The **Deploy Option** window appears.

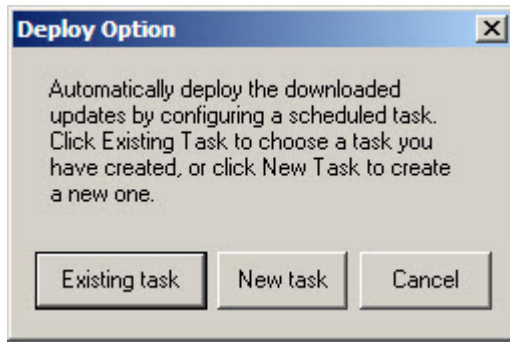


FIGURE 3-20. Deploy Options window

3. Do one of the following:
 - Click **New task**, to create a task.
 - Click **Existing task**, to edit a task.

See [Creating Tasks on page 3-50](#) and [Modifying an Existing Task on page 3-58](#) for information on how to create or edit a task.

Rolling Back the Previous Deployment Action

ServerProtect can roll back a deployed update action; reverting the system to the previous version of the updated file. Only the virus pattern and the virus scan engine can be rolled back. This is necessary when there is a software compatibility issue or when the update files were corrupted during the original download.



Note

If both the virus pattern and the scan engine files were originally deployed, you must roll both of them back.

Procedure

1. Do one of the following:
 - Click **Update** > **Rollback** on the side bar.
 - Click **Do** > **Rollback** from the main menu.

The **Rollback** screen appears.

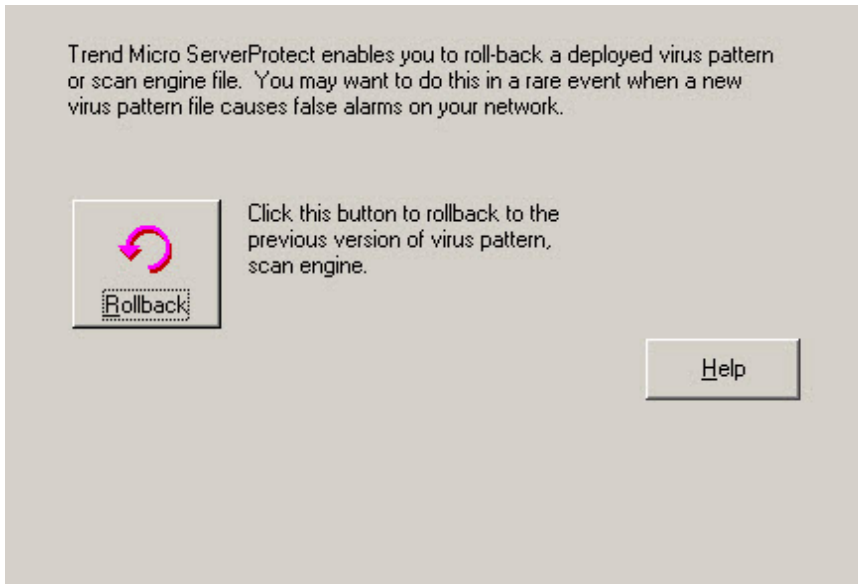


FIGURE 3-21. Roll Back Configuration window

2. Click **Rollback**.

The ServerProtect **Rollback** window appears.

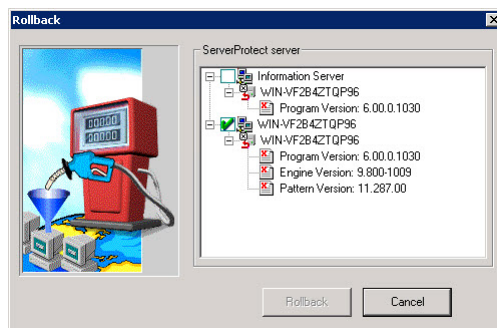


FIGURE 3-22. Rollback window

The screen displays information about the virus pattern file and scan engine that is currently being used by ServerProtect. The respective version and build numbers are also shown.

3. Select the check boxes of the items you want to roll back, and then click **Rollback**.



Note

You can only roll back the components which is most recently updated, The components can either be a virus pattern or a scan engine.

Managing Tasks

Tasks allow you to schedule Normal Servers to perform multiple functions simultaneously. Using tasks automates routine antivirus maintenance procedures on your network and improves the management of your antivirus policy.

You can define a task to run several procedures at one time in the same manner as macros automate word processing programs, or scripts automate routine network administration tasks.

Tasks are assigned to a "task owner" who is responsible for maintaining the task.

ServerProtect Task Wizard

The ServerProtect Task Wizard provides an intuitive interface for you to easily define a task. You can include the following functions in a task:

- **Real-time Scan setting:** Enables different Real-time Scan options for different tasks, for example, scanning incoming files only when the network performance is normal
- **Scan Now:** Checks whether your server is virus-free
- **Purge logs:** Defines which types of logs to purge from the database. You can enable the automatic purging of virus logs that are older than a preset age.
- **Export logs:** Exports logs as CSV files for use in other applications
- **Print logs:** Chooses a network printer to print logs that meet a certain criteria
- **Run statistics:** Compiles and displays statistics about virus scanning on your server
- **Deploy:** Defines when to distribute the updates of virus pattern and scan engine components to other ServerProtect servers

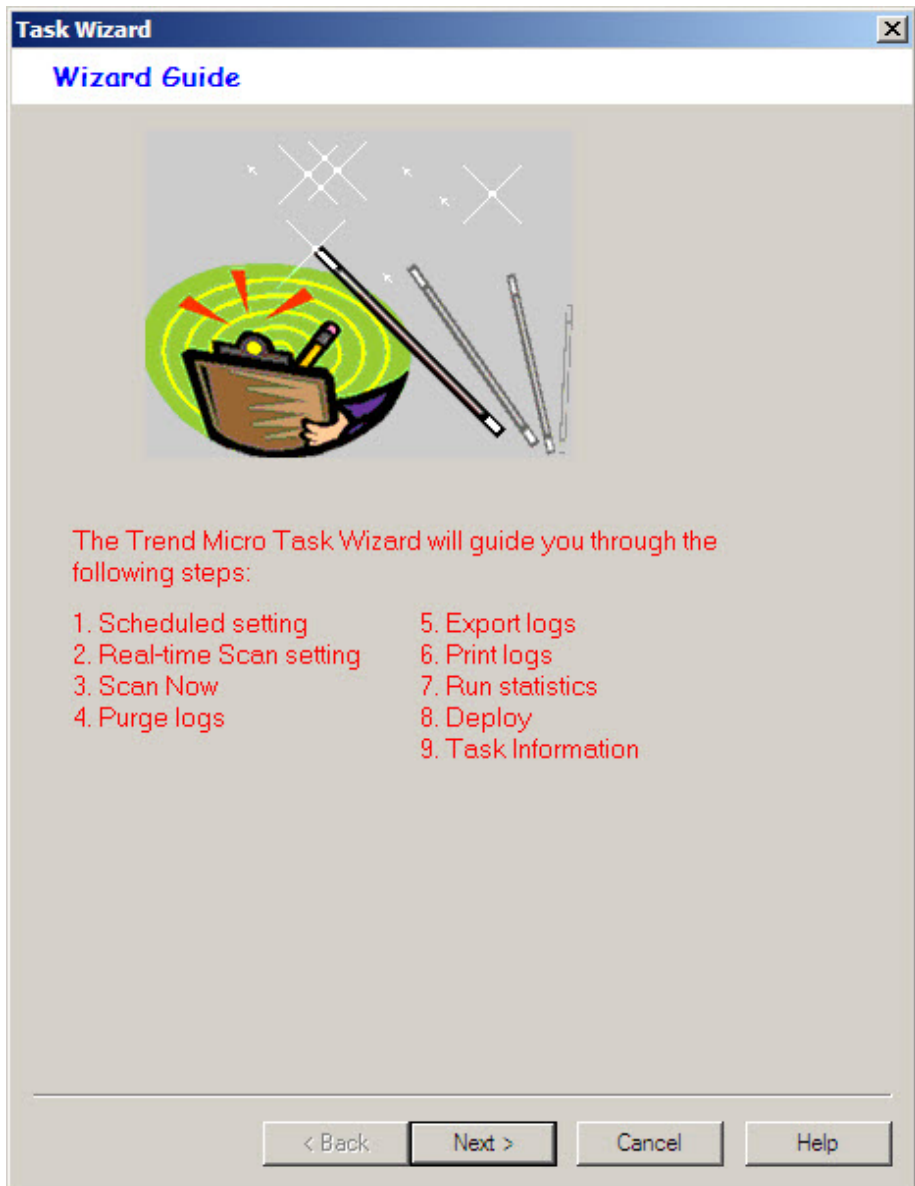


FIGURE 3-23. Task Wizard window

Default Tasks

Default tasks are created by ServerProtect with every Normal Server installation. When you install ServerProtect for the first time, you immediately have three default tasks: Scan, Statistics, and Deploy. You can edit default tasks, however, you cannot modify the task name or the task owner.

Creating Tasks

New tasks let you set up routine maintenance and configuration procedures.

Creating a Task

Procedure

1. Select the Information Server, domain, or Normal Server on the domain browser tree.
2. Do one of the following:
 - Click **Do** > **Create Task** on the main menu.
 - Click **Task** > **New Task** on the side bar.
3. Click **Create**.

The **Create New Task** window appears.

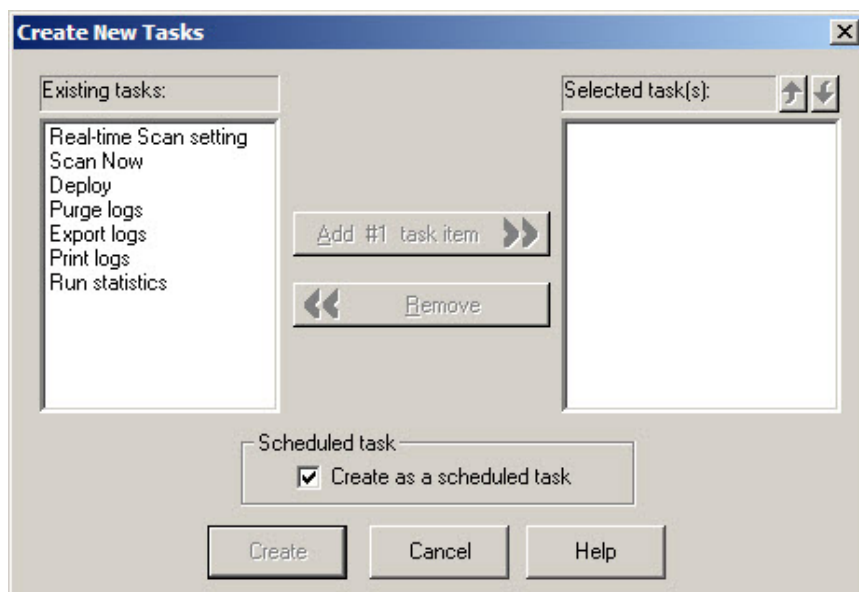


FIGURE 3-24. Create New Tasks window

4. Select the functions you want to include in this task in the **Existing tasks** list.
5. Click **Add #n Task Item** to add the selected function to the **Selected task** list. You can continue adding more functions. Alternatively, you can remove a previously selected function.



Tip

You can click the up or down arrow icons next to **Selected task(s)** to change the order in which the functions are performed. The Deploy function should always be the last one on the list.

6. Select the **Create as a scheduled task** check box if you want this task to be run according to a specified schedule. You can schedule tasks to run on an hourly basis.

7. Click **Create** to start the wizard and create a task with the selected functions. Click **Cancel** to close the **Create New** window without saving your changes.
-

Creating a Scheduled Task

Creating a scheduled task is easy to configure and save you time.

Procedure

1. Follow steps 1 through 6 in [Creating a Task on page 3-50](#). Make sure you select the **Create as a scheduled task** check box under **Scheduled task**.

The **Task Wizard** window appears.

2. Click **Next**.

The **Schedule Settings** window appears.

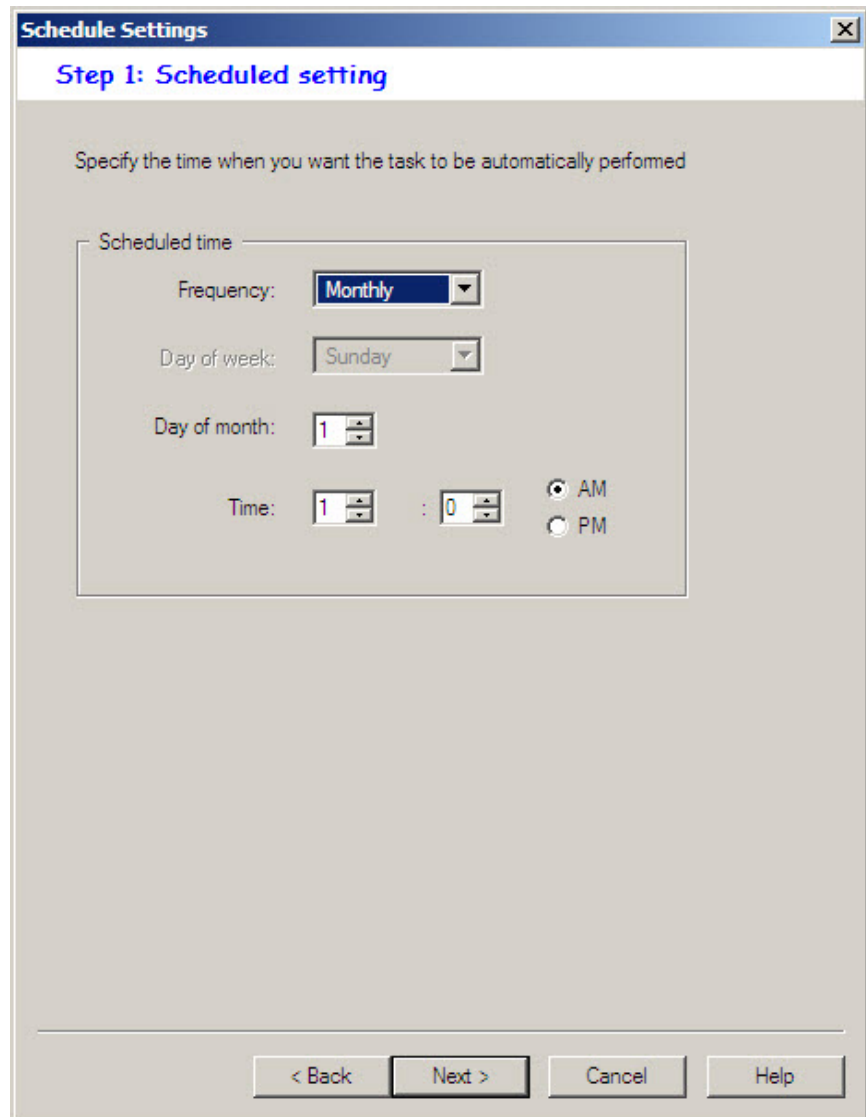


FIGURE 3-25. Schedule Settings window

3. Under **Scheduled time** in the **Frequency** list, click a download frequency. You can select **Monthly**, **Weekly**, **Daily**, or **Hourly**. If you selected **Weekly**, click a day in the **Day of Week** list. Alternatively, if you selected **Monthly**, click a day in the **Day of month** list.
 4. In the **Time** box, type or select the time when you want to update the components, and then click **AM** or **PM**.
 5. Click **Next** to proceed with the task wizard configuration.
-

Specifying a Target for Scan Now

Scan tasks must be run on specific drives. When defining the target drive, you are initially given the option to scan all local drives or specific drives

and/or directories. The latter option also allows you to scan another drive on the network.

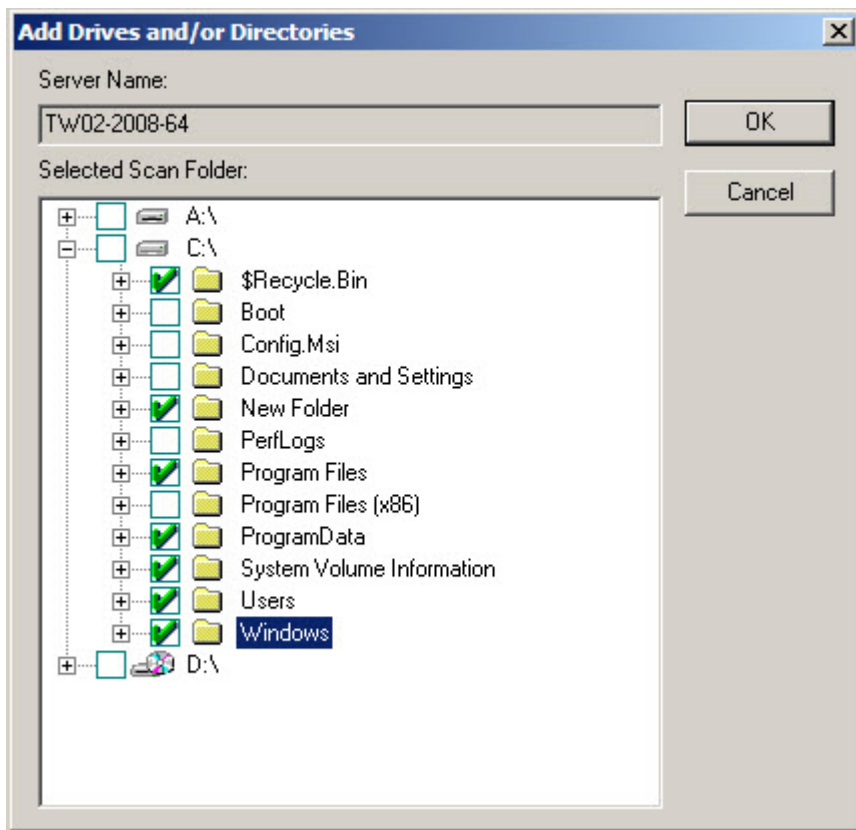
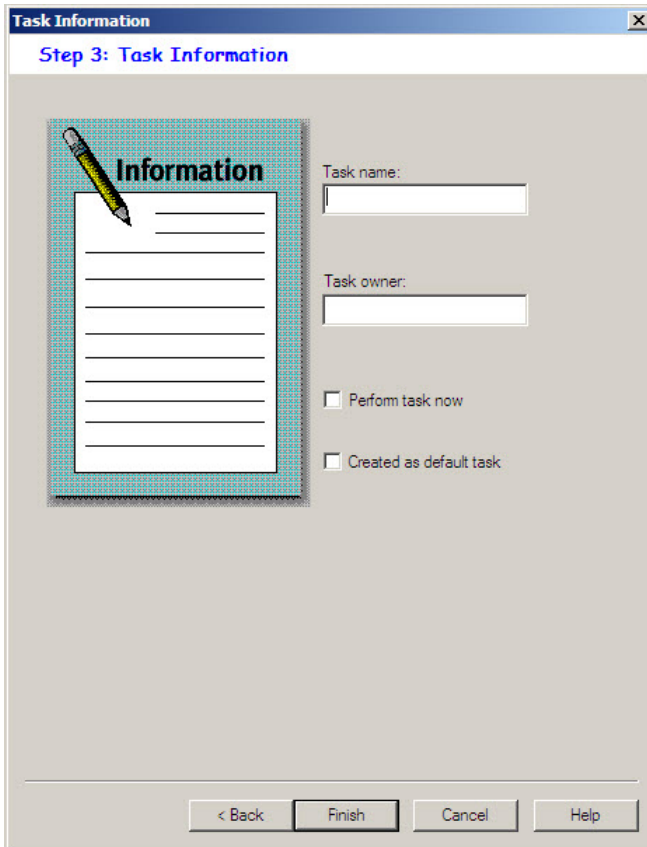


FIGURE 3-26. Add Drives and/or Directories window

Creating a Default Task

You can define a default task in the last screen of the task wizard, the **Task Information** window, where you define the name and owner of the task.

Default tasks affect all Normal Servers managed by an Information Server which means if you add a Normal Server, it will inherit existing default tasks.



The screenshot shows a window titled "Task Information" with a subtitle "Step 3: Task Information". On the left, there is a notepad icon with the word "Information" and a pencil. To the right of the notepad are two text input fields: "Task name:" and "Task owner:". Below these fields are two checkboxes: "Perform task now" and "Created as default task". At the bottom of the window, there are four buttons: "< Back", "Finish", "Cancel", and "Help".

FIGURE 3-27. Task Information window

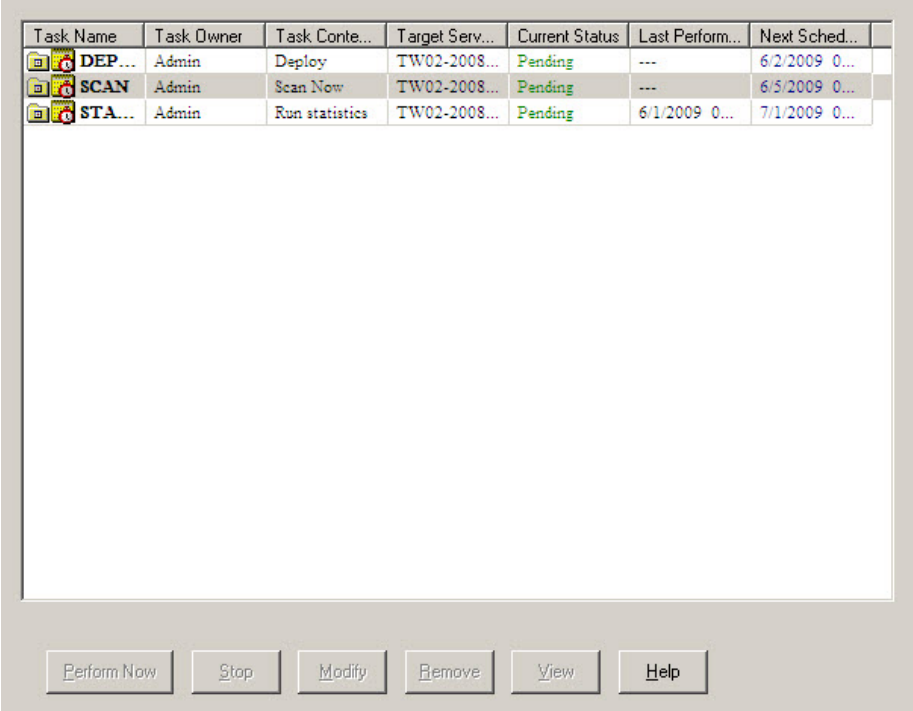
Opening the Existing Task List




The **Existing Task** list displays information about the tasks that have been created. You can use the **Existing Task** list to perform, modify, delete, or view the task definition.

To open the existing task list, do one of the following:

- Click **Task > Existing Task** on the side bar.
- Click **Do > Existing Task** on the main menu.

The **Existing Task** list is displayed in a table format. The following figure displays the different fields. Note that you can sort the list by clicking on the heading of each field.



Task Name	Task Owner	Task Conte...	Target Serv...	Current Status	Last Perform...	Next Sched...
 DEP...	Admin	Deploy	TW02-2008...	Pending	---	6/2/2009 0...
 SCAN	Admin	Scan Now	TW02-2008...	Pending	---	6/5/2009 0...
 STA...	Admin	Run statistics	TW02-2008...	Pending	6/1/2009 0...	7/1/2009 0...

Perform Now Stop Modify Remove View Help

FIGURE 3-28. Viewing Existing Tasks table



Note

If the servers to which a task is applied are located in different time zones, the time/date displayed in the **Last Perform Time** and **Next Schedule** fields will reflect the local time for each server.

Running an Existing Task

The **Existing Task** list displays information about all the tasks that have been defined. You can use the **Existing Task** list to perform a task.

Procedure

1. Do one of the following:
 - Click **Task** > **Existing Task** on the side bar.
 - Click **Do** > **Existing Task** on the main menu.

The **Existing Task** list displays all of the tasks that are currently defined within ServerProtect.

2. Select the task that you want to run, and click **Perform Now**.
-

Modifying Existing Tasks

Modifying existing tasks saves you valuable configuration time. This way, you do not need to spend time configuring new tasks.

Modifying an Existing Task

Procedure

1. Do one of the following:
 - Click **Task** > **Existing Task** on the side bar.
 - Click **Do** > **Existing Task** on the main menu.

The **Existing Task** list appears.

2. Click the task in the **Existing Task** list that you want to modify.
3. Click **Modify**.

The **Modify Task** window appears.

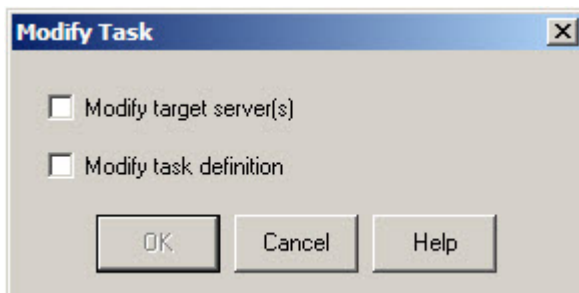


FIGURE 3-29. Modify Task window

4. Do one of the following:
 - Select the **Modify target server(s)** check box to change the servers, on which the task is configured to run.
 - Select the **Modify task definition** check box to change the procedures that were used to define the task.
5. Click **OK**.

Modifying a Target Server for an Existing Task

Procedure

1. In the **Select Servers to Apply Tasks** window, select and add the server on which you want to run the task.
2. Click **Add**.

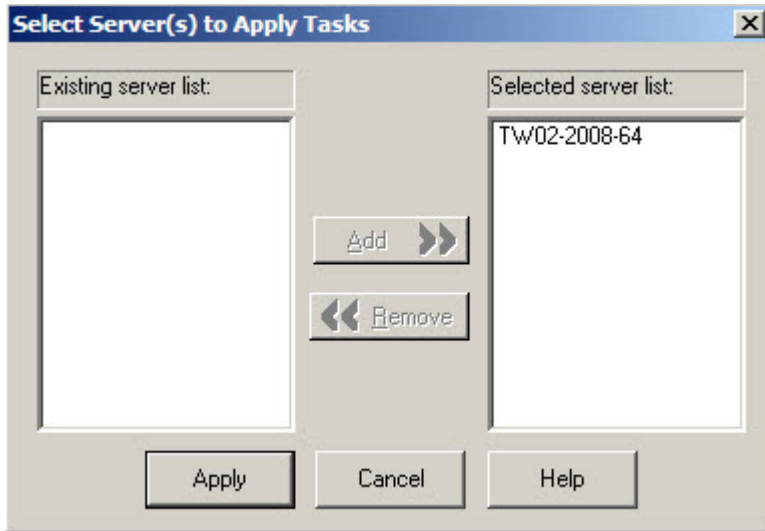


FIGURE 3-30. Select Servers to Apply Tasks window

3. Click **Apply**. To close the window without saving your changes, click **Cancel**.
-

Modifying a Task Definition for an Existing Task

Procedure

1. Select each function you want to include in this task in the **Existing Tasks** list.

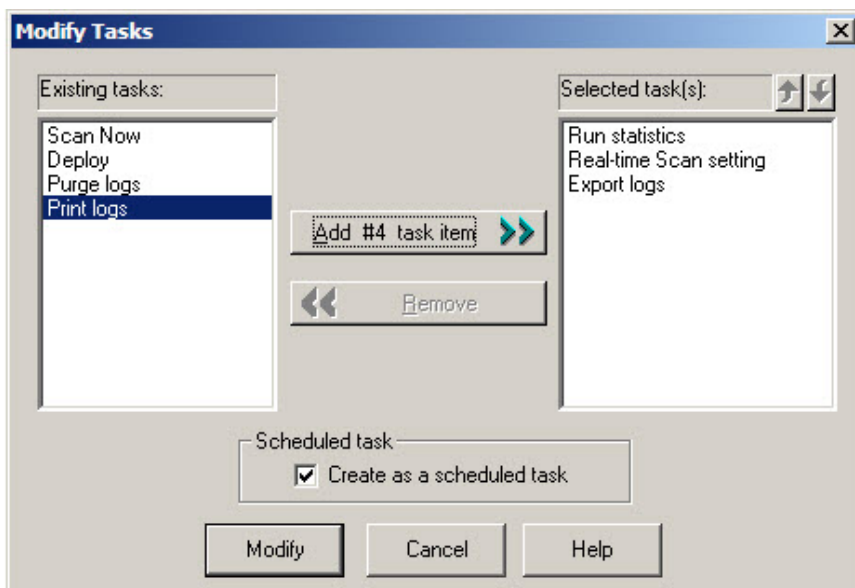


FIGURE 3-31. Modify Tasks window

2. Click **Add #n Task Item** to add the function you selected to the **Selected task** list.

If you want this task to be scheduled to run, make sure that you select the **Create as a scheduled task** check box.



Tip

You can click the up or down arrow icons next to **Selected task(s)** to change the order in which the functions are performed. The Deploy function should always be the last one on the list.

3. Click **Modify** to start the wizard that will help you create a task with the functions that you have chosen. Click **Cancel** to close the **Create New Task** window without saving your changes.

Viewing an Existing Task

The attributes of any existing task can be viewed from the **Existing Task** window. This enables you to know exactly what the task will do before executing it.

Procedure

1. Do one of the following:
 - Click **Do > Existing Task** on the main menu.
 - Click **Task > Existing Task** on the side bar.
2. Select the task in the **Existing Task** list that you want to view.
3. Click **View** at the bottom of the configuration area. Alternatively, you can double-click the task's record entry in the **Existing Task** table. The **View Task Information** window appears.

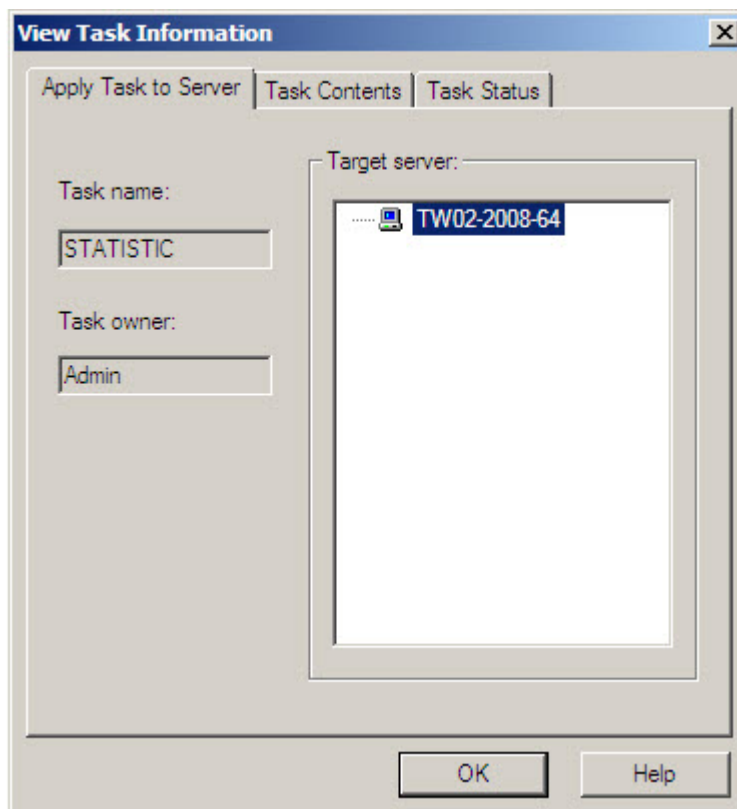


FIGURE 3-32. View Task window

This screen contains three tabbed sections labeled **Apply Task to Server**, **Task Contents**, and **Task Status**.

- **Apply Task to Server:** The **Task name** and **Task owner** are displayed on the left side of the tab. The **Target server** displays all the servers on your network that the task will run on.
- **Task Contents:** All of the functions that make up the task are displayed. Click a function in the **Task sequence** list and the function definition will appear in the task definition table on the right.

- **Task Status:** The **Target Server** displays all of the servers on your network on which the task will run. The **Current Status**, **Last Perform Time**, and **Next Schedule** fields display the status of the task and the last time it was run.

4. Click **OK** to close the **View Task Information** window.
-

Removing an Existing Task

The **Existing Task** list displays information about all tasks that have been defined. You can use the **Existing Task** list to delete a task definition.

Procedure

1. Do one of the following:
 - Click **Do > Existing Task** on the main menu.
 - Click **Task > Existing Task** on the side bar.
 2. In the **Existing Task** list, select the task you want to remove.
 3. Click **Remove**.
-

Configuring Notification Messages

Antivirus software is quite useful if it alerts a user or an administrator when a virus is detected. ServerProtect enables you to configure both notifications and to whom they will be sent.

ServerProtect notifications comprise of standard and outbreak alerts. Alerts can be delivered in various ways. See [Setting Alert Methods on page 3-69](#) for all available delivery options.

Standard Alerts

A standard alert is generated whenever a selected event is detected on the designated server. You can append additional text to a notification message.

Notification Events

You can configure ServerProtect to notify you when the following events occur.

- **Virus/Malware detected:** an infected file on the server was detected
- **Spyware/Grayware Detected:** Detection of a Spyware-infected file on the server
- **Attempt to change write-protected file:** Any attempt to change the write-protected settings
- **Real-time configuration change:** Changes to the configuration settings of Real-time Scan
- **Service load/unload:** To stop/start the ServerProtect
- **Device RPC connection success/failure:** Status of an RPC connection to a NetApp Device
- **Virus pattern out-of-date:** Expiration of the virus pattern file
- **Spyware pattern out-of-date:** Expiration of the Spyware pattern file

Configuring a Standard Alert

Procedure

1. Select the Information Server domain, or a Normal Server on the domain browser tree.
2. Do one of the following:
 - Click **Configure** > **Notifications** > **Standard Alert** on the main menu.
 - Click **Set Notification** > **Standard Alert** on the side bar.

The **Standard Alert** screen appears.

FIGURE 3-33. ServerProtect Standard Alert Configuration window

3. Select the event type check box(es).
4. Click **Configure Message** for each selected event.

The **Configure Alert Message** window appears.

5. Type your desired settings, and then click **OK** to close the window.
6. Click **Set Alert Method** to select the way that you want to be notified. Refer to [Setting Alert Methods on page 3-69](#) for additional information.



Note

To find out more on configuring alert messages, refer to the related topic in the online help.

Outbreak Alerts

Virus outbreaks have a high potential for damage on a corporate network. Whenever the number of virus events exceeds the threshold, an outbreak alert is triggered to notify the system administrator.

This ensures that system administrators or other individuals who need to know about the virus outbreak are notified and can then take action against them. A customized message will be used to alert of an outbreak.

Configuring an Outbreak Alert

Procedure

1. Select the Information Server domain, or a Normal Server on the domain browser tree.
2. Do one of the following:
 - Click **Set Notification > Outbreak Alert** on the side bar.
 - Click **Configure > Notifications > Outbreak Alert** on the main menu.

The **Outbreak Alert** screen appears.

Signal an outbreak alert when the number of viruses found exceeds within hours.

Set alert methods

- Message box
- Printer
- Pager
- Internet email
- SNMP trap
- Windows event log

FIGURE 3-34. ServerProtect Outbreak Alert Events Configuration Window

3. Define the outbreak threshold. Specify the number of viruses to be exceeded, and the period of consideration, in hours, in the boxes provided.
4. Select the notification methods that the alert uses.

5. Click **Configure** to access the notification settings for the selected methods. For additional information about each modification method, refer to *Setting Alert Methods on page 3-69*.
 6. Under **Alert Message**, click **Configure Message** to modify the message that will be displayed when there is a virus outbreak.
 7. Click **Apply** to save your settings.
-

Setting Alert Methods

When a virus outbreak occurs, ServerProtect can notify system administrators, and other people you designate using the following methods:

- **Message box:** A standard Windows pop-up message box is displayed on the administrator's computer.
- **Printer:** A document is sent to a local or network printer.
- **Pager:** A message is sent to a pager. This feature requires a modem to be connected to the server that is hosting Trend Micro ServerProtect.
- **Internet Mail:** An email message is sent on detection of viruses.
- **SNMP Trap:** An alert message is sent to network administrators by SNMP. This integrates with other SNMP-compatible management tools that may be deployed within your company.
- **Windows Event Log:** The detection of the virus is written to the Windows event log.

You can configure one or several notification methods. Instructions to configure email notifications are provided in this document. For other forms of notification, refer to the online help.

Configuring an Alert to be Sent by Internet Mail

Procedure

1. Click either the Information Server domain, or a Normal Server on the domain browser tree.

2. Do one of the following:
 - To configure an outbreak alert:
 - Click **Set Notification** > **Outbreak Alert** on the side bar.
 - Click **Configure** > **Notifications** and then **Outbreak Alert** on the main menu.
 - To configure a standard alert:
 - Click **Configure** > **Notifications** > **Standard Alert** on the main menu then click **Set Alert Method**.
 - Click **Set Notification** > **Standard Alert** on the side bar and then click **Set Alert Method**.
3. Select the **Internet mail** check box, and then click **Configure**.

The **Configure Internet Mail** window appears.

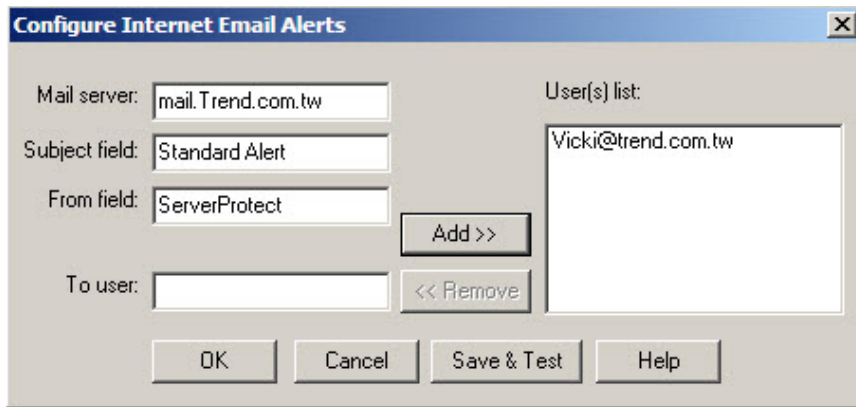


FIGURE 3-35. Configure Internet Email Alerts window

4. Do the following:
 - a. Type the name of the mail server in the **Mail Server** text box.
 - b. Type the subject of the message in the **Subject field** text box.
 - c. Type the name of the sender in the **From field** text box.

5. Type each recipient of this email message in the **To user(s)** text box and then click **Add**. You can remove a recipient by selecting the user, and then clicking **Remove**.
6. Click **Save & Test** to ensure that the configuration settings are working. If successful, the users that you specified receive a test email message.
7. Click **OK** to save your configuration changes and return to the **Set Alert Method** window.

**Note**

To find out more about configuring alert messages, refer to the related topic in the online help.

Scanning Viruses for Normal Server

ServerProtect provides three scan modes for detecting viruses: Real-time Scan, Scan Now (Manual scan), and Scheduled scan.

Real-time Scan checks all incoming and outgoing files on the server for signs of infection. Scan Now scans on-demand, allowing you to check a server for virus exposure immediately. Scheduled scan checks for infected files on selected ServerProtect servers at predetermined times.

There are five actions for dealing with infected files: Bypass (Ignore), Delete, Rename, Quarantine (Move), and Clean.

You can do the following:

- Choose the type of files to scan.
- Prevent users from modifying or deleting selected directories/files using the Deny Write list. For more information about configuring the Deny write list, see the related topic in the online help.



Note

The results of each scan are available in the Scan Result logs. You can take action on the infected files directly from the Scan Result window. This provides a convenient way to take appropriate actions during a virus infection event. For more information, refer to the **Viewing Scan Result Information** topic in the online help.

Defining Actions Against Viruses

ServerProtect lets you configure the kind of action(s) to take against infected files that are found on your network during a Real-time Scan or Scan Now.

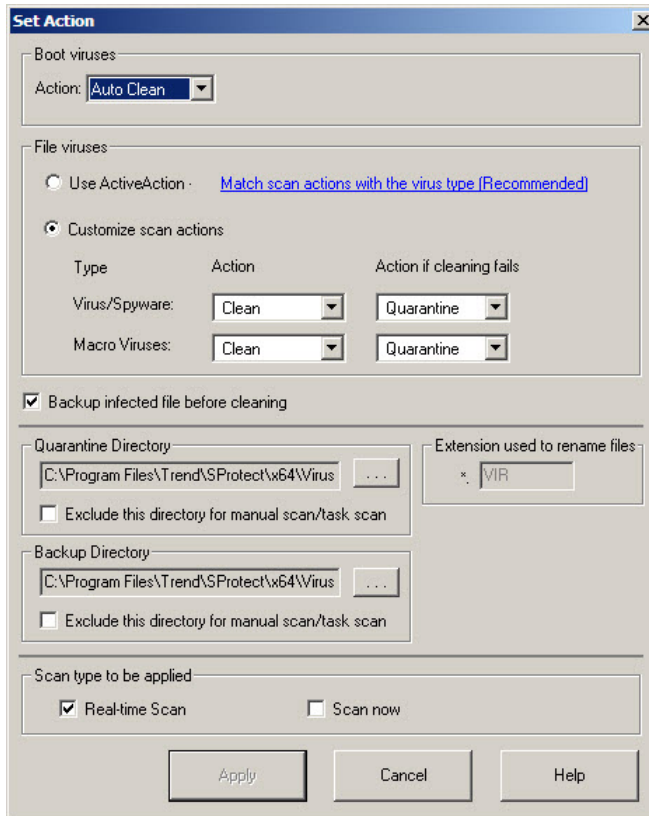


FIGURE 3-36. Set Virus Action window

Procedure

1. Click **Set Action** from the **Scan Now** or **Real-time Scan** configuration area. The Set Virus Action window appears.

**Note**

Spyware doesn't support clean action. If the action of virus is clean/delete, for spyware virus it will only do delete operation.

2. Under **Boot Viruses** in the **Action** list, click the virus action you want ServerProtect to take when it finds a boot virus. You can select **Auto Clean** or **Bypass**.
 3. Under **File Viruses**, do one of the following:
 - Click **Use ActiveAction** to set Trend Micro recommended virus actions. Beware that the action can be taken to handle spyware infection is limited to **Bypass**, and that the action **Clean** is not supported to handle spyware infection. Applying **Clean** action to a spyware infected file results the deletion of the file.
-

**Note**

When using ActiveAction, spyware action will be bypass/bypass.

- Click **Customize scan actions**, to select the appropriate action to take against the file and macro viruses in the **Action** and **Action if cleaning fails** lists. See [When ServerProtect Finds a Virus \(Virus Actions\) on page 1-20](#). For more information about ActiveAction, see [IntelliScan on page 1-28](#).
-

**Note**

If you selected a **Clean** action, we recommend that you select the **Backup infected file before cleaning** check box. The virus cleaning process can, on rare occasions, damage files and make them unusable.

You should exclude both the backup and quarantine directories from scanning. Refer to the **Directory Exclusion List** topic in the online help for more information. The selected scan type is displayed under **Scan type to be applied**.

4. Click **Apply** to start using these settings.

**Note**

The EMC CAVA Scanner protects storage devices using Real-time Scan. If the Normal Server is an EMC CAVA Scanner, the configuration of Real-time Scan will also be applied to the EMC CAVA Scanner.

Scanning Profiles

Real-time Scan and Scan Now configurations can be saved as scanning profiles that can then be used to create or modify tasks. Alternatively, you can delete profiles if they are no longer needed. Scanning profiles can be applied when configuring Scan Now and Real-time Scan tasks. For more information, see **Choosing a scan profile** in the online help.

For scheduled scans, that is, scheduled scan tasks, you can either choose an existing scanning profile or create your own. See [Modifying an Existing Task on page 3-58](#).

Saving a Scanning Profile

Procedure

1. Configure a Real-time Scan or Scan Now.

See [Configuring Real-Time Scan on page 3-81](#) and [Configuring Scan Now on page 3-85](#).

2. Click **Save As/ Delete Profile**.

The **Save/Delete Profile** window appears.

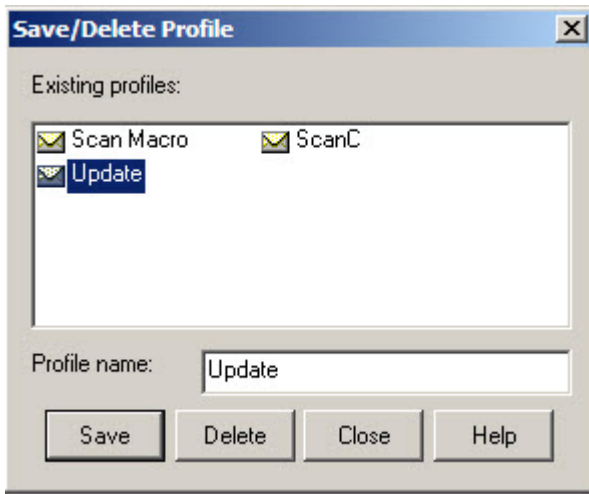


FIGURE 3-37. Save/Delete Profile window

3. Type a profile name in the **Profile name** text box.
4. Click **Save** to save the new profile. Alternatively, click **Close** to close the window without saving it.

Deleting a Scanning Profile

Procedure

1. Do one of the following:
 - Click **Scan Now** > **Scan Now** on the side bar.
 - Click **Do** > **Scan Now** on the main menu.
 - Click **Set Scan option** > **Real-time Scan** on the side bar.
2. Click **Save As/ Delete Profile**.

The **Save/Delete Profile** window appears.

3. Click the profile you want to delete in the **Existing Profiles** list.
 4. Click **Delete** to delete the profile. Alternatively, click **Close** to close the window without deleting it.
-

Scanning Viruses for Storage Devices

ServerProtect for Storage provides three kinds of scanners for detecting viruses for storage devices: RPC Scanner, EMC CAVA Scanner and ICAP Scanner.

There are five actions for dealing with infected files in RPC Scanner and EMC CAVA Scanner: Bypass (Ignore), Delete, Rename, Quarantine (Move), and Clean. And there are only two actions for dealing with infected files in ICAP Scanner.

Defining Actions Against Viruses in RPC Scanner and EMC CAVA Scanner

ServerProtect with EMC CAVA Scanner and RPC Scanner lets you configure the kind of action(s) to take against infected files that are found on a storage device.

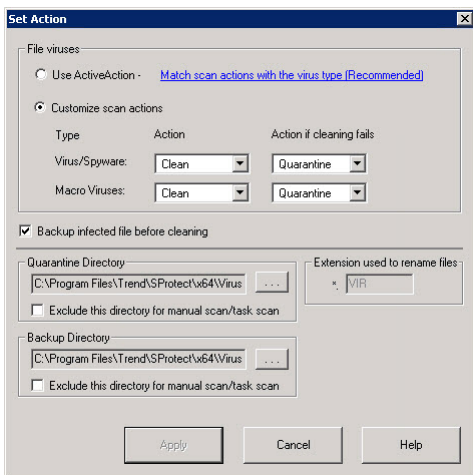


FIGURE 3-38. Set Action dialog for RPC and EMC CAVA Scanner

Procedure

1. Click **Set Action** from the **Storage Scanner** configuration area. The **Set Action** dialog appears.
2. Under **File Viruses**, do one of the following:
 - Click **Use ActiveAction** to set Trend Micro recommended virus actions. Beware that the action that can be taken to handle spyware infection is limited to **Bypass**, and that the action **Clean** is not supported to handle spyware infection. Applying the **Clean** action to a spyware infected file will delete the file.
 - Click **Customize scan actions**, to select the appropriate action to take against the file and macro viruses in the **Action** and **Action if**

cleaning fails lists. See [When ServerProtect Finds a Virus \(Virus Actions\) on page 1-20](#). For more information about ActiveAction, see [IntelliScan on page 1-28](#).



Note

If you selected a **Clean** action, Trend Micro recommends selecting the **Backup infected file before cleaning** check box. The virus cleaning process can, on rare occasions, damage files and make them unusable.

You should exclude both the backup and quarantine directories from scanning. Refer to the *Excluded Directory List* topic in the online help for more information. The selected scan type is displayed under **Scan type to be applied**.

3. Click **Apply** to start using these settings.



Note

The EMC CAVA Scanner protects storage devices using Real-time Scan. If the Normal Server is an EMC CAVA Scanner, the configuration of EMC CAVA Scanner will also be applied to Real-time Scan.

Defining Actions Against Viruses in ICAP Scanner

ServerProtect with ICAP Scanner lets you configure the kind of action(s) to take against infected files that are found on a storage device.

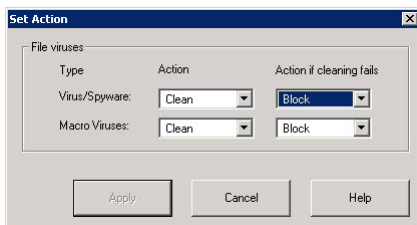


FIGURE 3-39. Set Action dialog for ICAP Scanner

Procedure

1. Click **Set Action** from the **Storage Scanner** configuration area. The **Set Action** dialog appears.
 2. Under **File Viruses**, select the appropriate action to take against the file and macro viruses in the **Action** and **Action if cleaning fails** lists. See [When ServerProtect Finds a Virus \(Virus Actions\) on page 1-20](#) for more information.
 3. Click **Apply** to start using these settings.
-

Using Real-Time Scan

Real-time Scan constantly scans all files that are accessed and provides powerful virus protection that runs in the background. All incoming/outgoing files are monitored, thus infected files are prevented from being copied to or from a server.

The following scan options are specific to Real-time Scan:

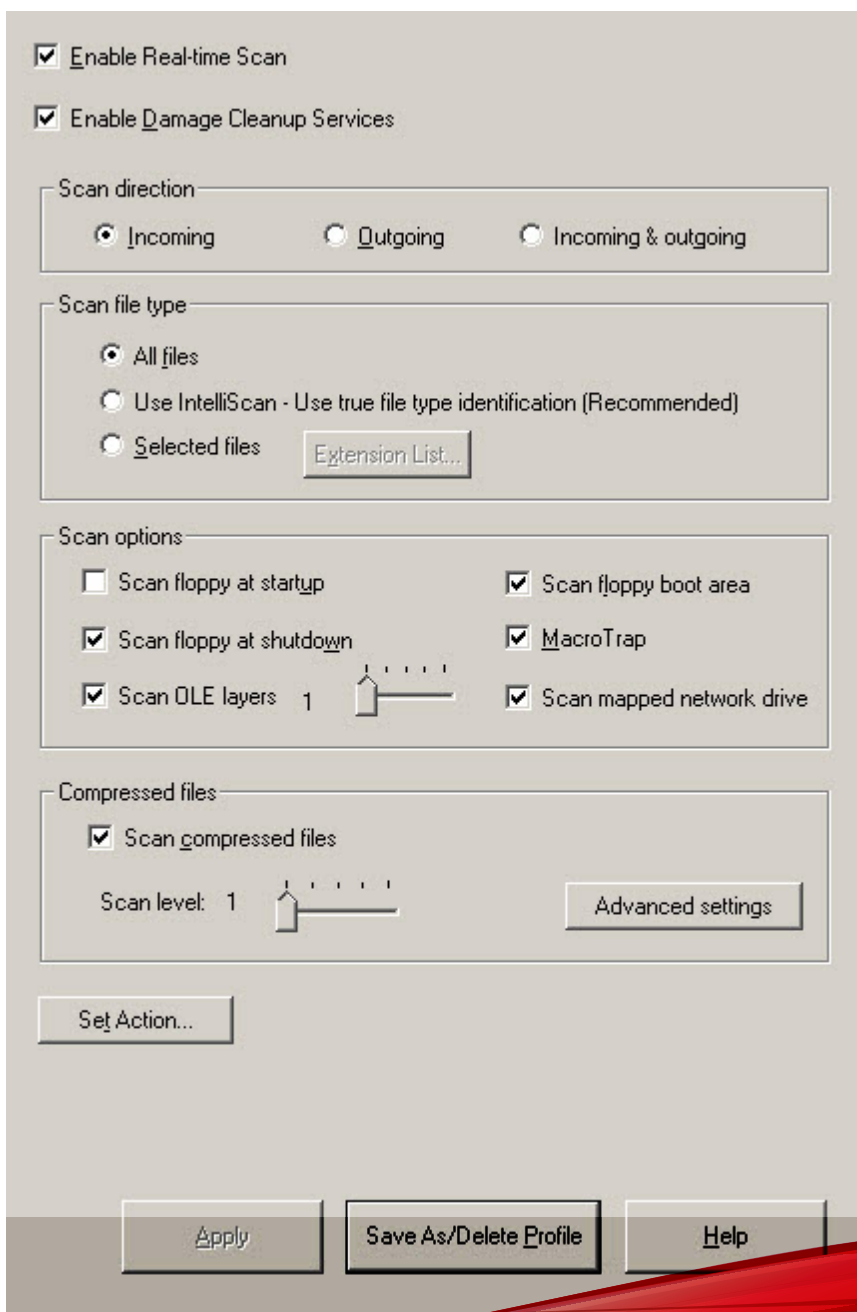
- **Scan floppy at startup:** Your floppy disk drive is scanned for boot viruses when you turn your computer on. Any diskette inside your floppy disk drive is also scanned. This prevents you from booting your computer with an infected diskette.
- **Scan floppy at shutdown:** Your computer's floppy disk drive is checked for boot viruses when the computer is shut down and any diskette inside it is also scanned.
- **Scan floppy boot area:** This option scans the floppy boot area of your computer. This feature protects against Master Boot Record viruses.
- **MacroTrap:** ServerProtect includes patented MacroTrap™ technology to guard against macro viruses in Microsoft™ Office files and templates.
- **Scan OLE layers:** This option scans embedded files. OLE layer scan offers five layers of protection. See [OLE Layer Scan on page 1-27](#) for more information.

- **Scan mapped network drive:** This option scans any mapped network drive. You should have an existing network mapped drive for this option to work.

Configuring Real-Time Scan

Procedure

1. Select the Information Server, domain, or a Normal Server on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option > Real-time Scan** on the side bar.
 - Click **Configure > Scan Options > Real time Scan** on the main menu.



3. Select the **Enable real-time scan** check box.
4. Set the **Enable Damage Cleanup Services** check box so that the Virus Cleanup engine scans for and removes Trojans and Trojan processes. It supports 32-bit and 64-bit platforms. Clear the check box to disable the service.
5. Under **Scan direction**, choose one of the following:
 - **Incoming:** Scans files copied to the server
 - **Outgoing:** Scans files being copied from the server
 - **Incoming and Outgoing:** Scans all incoming and outgoing files on the server
6. Under **Scan file type**, choose one of the following:
 - **All files:** Scans all file types
 - **IntelliScan:** Scans files using true file type identification
See [IntelliScan on page 1-28](#).
 - **Selected files:** Scans only specified files
If you choose **Selected files**, click **Extension List** to define the file types that you want to scan. Refer to [Selecting File Types to Scan on page 3-101](#).
7. Under **Scan options**, select one or more from the following check boxes:
 - Scan floppy at start up
 - Scan floppy at shutdown
 - Scan OLE layers
 - Scan floppy boot area
 - MacroTrap
 - Scan mapped network drive

See [Using Real-Time Scan on page 3-80](#) for additional information on each scan option.

8. Select the **Scan compressed files** check box to scan compressed files and then move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the **Compressed file scan** topic in the online help.



Note

If you choose to scan selected file types in step 5, make sure you select the extensions of compressed files in the extension list.

9. Click **Set Action** to configure how ServerProtect acts on infected files. See [Defining Actions Against Viruses on page 3-73](#).
10. Click **Apply** to save your changes or click **Save As Profile** to recall your configuration settings at a later time.



Note

The EMC CAVA Scanner protects storage devices using Real-time Scan. If the Normal Server is an EMC CAVA Scanner, the configuration of Real-time Scan will also be applied to EMC CAVA Scanner.

Using Scan Now (Manual Scan)

Scan Now performs a scan on demand. Use Scan Now if you suspect a server has been infected.

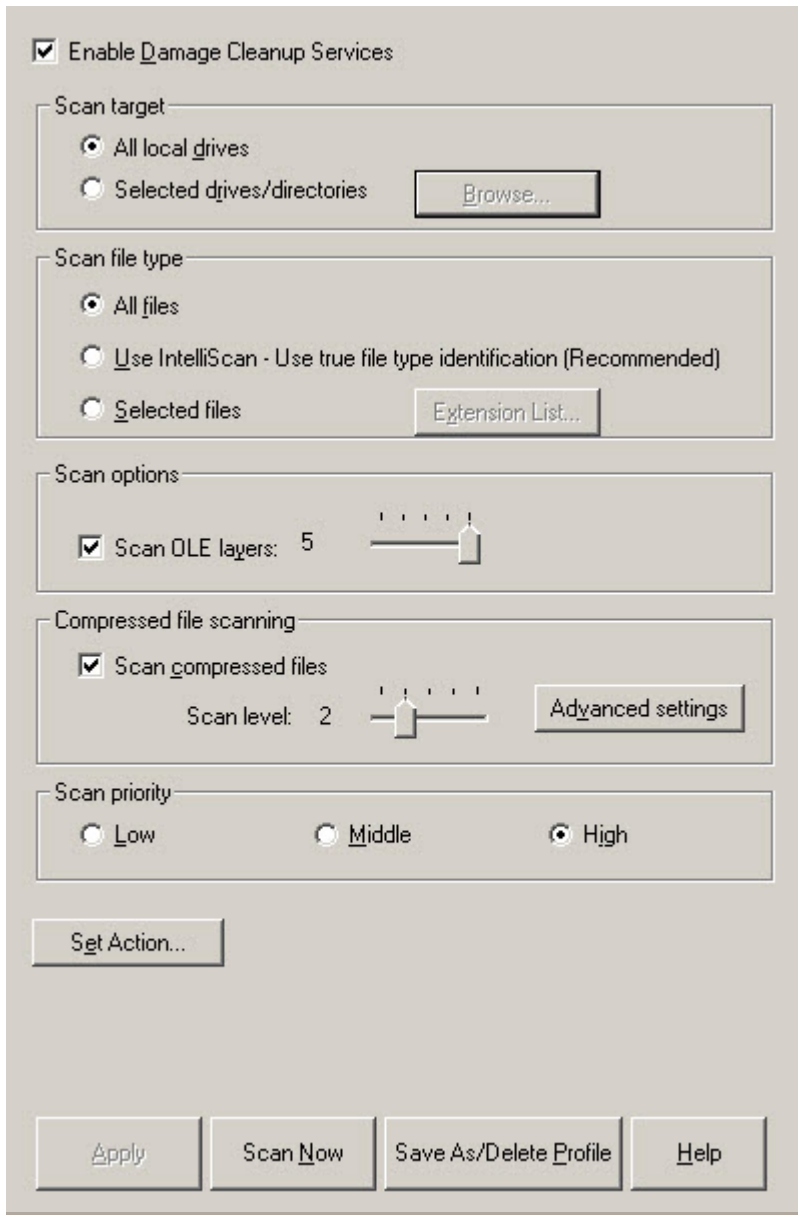
You can configure the following for Scan Now:

- Scan target
- Scan file type
- Scan options
- Compressed file scanning
- Scan priority
- Scan action

Configuring Scan Now

Procedure

1. Click the Information Server, domain, or a Normal Server on the domain browser tree.
2. Do one of the following to bring about the configuration pane for Scan Now operation:
 - Click **Scan Now** > **Scan Now** on the side bar.
 - Click **Do** > **Scan Now** from the main menu.

**FIGURE 3-41. Scan Now Configuration window**

3. Set **Enable Damage Cleanup Service** check box to enable the service. Clear it to disable the service.
4. Under **Scan target**, choose one of the following:
 - **All local drives:** Scans all drives in a server
 - **Selected drives/directories:** Scans specific drives or directories on a server

Click **Browse**. The **Add Drives and/or Directories** window appears. Select the check box(es) for the drives or directories you want to scan, then click **OK** to close the window.

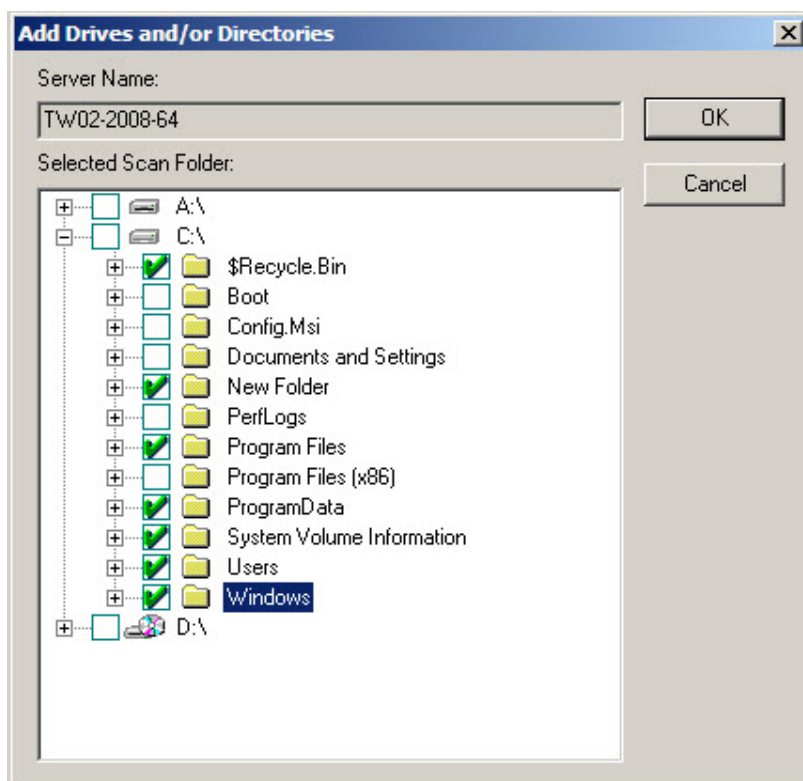


FIGURE 3-42. Add Drives and/or Directories window

5. Under **Scan file type**, choose one of the following:
 - **All files:** Scans all file types
 - **Use IntelliScan:** Scans files using true file type identification
See [IntelliScan on page 1-28](#).
 - **Selected files:** Scans only specified files
Click **Extension List** to define the file types that you want to scan.
Refer to [Selecting File Types to Scan on page 3-101](#).
6. Under **Scan options**, select **Scan OLE layers**. Move the **Scan OLE layers** slider to set the number of OLE layers. ServerProtect can scan up to five layers.
7. Under **Compressed file scanning**, select the **Scan compressed files** check box. Move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.

**Note**

If you choose to scan selected file types in step 4, make sure you include the extensions of compressed files in the extension list.

8. Under **Scan priority**, click **Low**, **Middle**, or **High**. A high scan priority consumes more CPU resources, but can complete scan jobs faster.
 9. Click **Set Action** to configure how ServerProtect acts on infected files. See [Defining Actions Against Viruses on page 3-73](#).
 10. Click **Apply** to save the changes or click **Save As Profile** to recall the configuration settings at a later time.
-

Running the Scan Now Tool on Windows Normal Servers

Use the Scan Now tool to scan servers of Microsoft Windows Server family without accessing the Management Console. Scan Now performs the scan

according to the Scan Now configurations you have set in the Management Console (for example, Scan target, Scan file type).

Running the Scan Now Tool

Procedure

1. Click **Start > Programs > Accessories > Windows Explorer** on the Normal Server.

The **Windows Explorer** window appears.

2. Click the folder where you installed ServerProtect.

The default location for a 32-bit operating system is:

C:\Program Files\Trend\SProtect

The default location for a 64-bit operating system is:

C:\Program Files\Trend\SProtect\x64

3. Double-click **ScanNow.EXE**.

A Scan Now is performed.

Stopping the Scan Now Tool

Procedure

1. Click **Start > Run** on the Normal Server. The Run window appears.

2. Click **Browse** and locate the ScanNow.EXE file.

The default location for a 32-bit operating system is:

C:\Program Files\Trend\SProtect

The default location for a 64-bit operating system is:

C:\Program Files\Trend\SProtect\x64

3. Run the tool with the "stop" switch as shown below:

For a 32-bit operating system:

```
C:\Program Files\Trend\SProtect\ScanNow.exe /STOP
```

For a 64-bit operating system:

```
C:\Program Files\Trend\SProtect\x64\ScanNow.exe /STOP
```

4. Click **OK**.

Scan Now stops.



Note

You must include a space between the file name and the Stop switch.

Scheduled Scanning

A scheduled scan scans files at the time and frequency configured. Use scheduled scans to automate routine scans on your Normal Servers. You can create a scheduled Scan Now or Real-time Scan by using a scheduled task.

Configuring a Scheduled Scan

You can configure a scheduled Scan Now or Real-time Scan by using a scheduled task. Refer to [Creating Tasks on page 3-50](#) for more information.



Note

When a ServerProtect server is installed, ServerProtect automatically applies a Scan task to the server. The default Scan task is set to scan all your local directories every Friday.

If the existing task does not suit your needs, you can either edit the default task, or create a new one. The **ServerProtect Task Wizard** guides you through the process of creating new tasks.

Using RPC Scanner

Use RPC Scanner if the storage supports RPC mode for virus scanning.

Configuring RPC Scanner

You can configure the following for RPC Scanner:

- Scan file type
- Scan options
- Compressed file scanning
- Scan action

Procedure

1. Click a Normal Server with RPC Scanner on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option** > **Storage Scanner** on the side bar.
 - Click **Do** > **Storage Scanner** on the main menu.

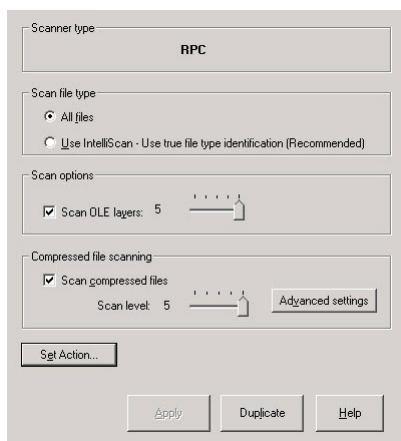


FIGURE 3-43. RPC Scanner Configuration dialog

3. Under **Scan file type**, choose one of the following:
 - **All files**: Scans all files
 - **Use IntelliScan**: Scans files using true file type identification. See [IntelliScan on page 1-28](#).
 4. Under **Scan options**, select **Scan OLE layers**. Move the **Scan OLE layers** slider to set the number of OLE layers. ServerProtect can scan up to five layers.
 5. Under **Compressed file scanning**, select the **Scan compressed files** check box. Move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.
 6. Click **Set Action** to configure how ServerProtect acts on infected files. See [Defining Actions Against Viruses in RPC Scanner and EMC CAVA Scanner on page 3-78](#).
 7. Click **Apply** to save the changes.
-

Duplicating RPC Scanner Configuration

Procedure

1. Click a Normal Server with RPC Scanner on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option** > **Storage Scanner** on the side bar.
 - Click **Do** > **Storage Scanner** on the main menu.
3. Click **Duplicate**.

The **Select Server(s) to Duplicate Configuration to** screen appears.

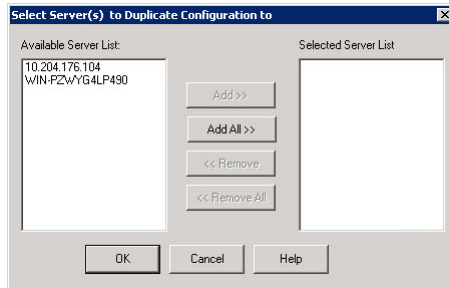


FIGURE 3-44. Duplicate configuration dialog

4. Select one or more Normal Servers in **Available Server List**. To select multiple Normal Servers, press the **CTRL** key as you select.



Note

The scanner type of Normal Server(s) shows in **Available Server List** is the same with the scanner type of the source Normal Server.

5. Do one of the following:
 - Click **Add** to add the selected Normal Server(s) to **Selected Server List**.
 - Click **Add All** to add all the Normal Server(s) in **Available Server List** to **Selected Server List**.
6. Click **OK**.



Note

This procedure does not duplicate the quarantine directory and backup directory.

Using EMC CAVA Scanner

Use EMC CAVA Scanner if the storage supports EMC CAVA or Huawei Antivirus Agent for virus scanning. EMC CAVA/Huawei Antivirus Agent triggers Real-time Scan once receiving the following events from a storage device:

- A file was renamed on the storage device.
- A file was copied or saved to the storage device.
- A file was modified and closed on the storage device.

If you want to define stricter conditions to trigger Real-time Scan, refer to the documentation of your storage device.

Configuring EMC CAVA Scanner

You can configure the following for EMC CAVA Scanner:

- Enable Real-time Scan
- Enable Damage Cleanup Services
- Scan direction
- Scan file type
- Scan options
- Compressed file scanning
- Scan action



Note

The EMC CAVA Scanner protects storage devices using Real-time Scan. If the Normal Server is an EMC CAVA Scanner, the configuration of EMC CAVA Scanner will also be applied to Real-time Scan.

Procedure

1. Click a Normal Server with EMC CAVA Scanner on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option > Storage Scanner** on the side bar.
 - Click **Do > Storage Scanner** on the main menu.

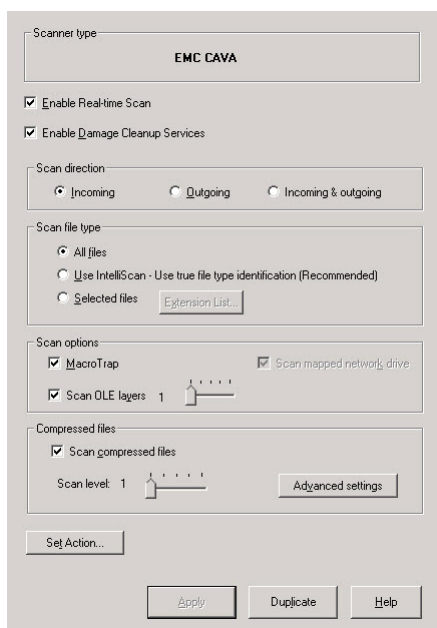


FIGURE 3-45. EMC CAVA Scanner Configuration dialog

3. Select the **Enable real-time scan** check box.
4. Set the **Enable Damage Cleanup Services** check box so that the Virus Cleanup engine scans for and removes Trojans and Trojan processes. It supports 32-bit and 64-bit platforms. Clear the check box to disable the service.

5. Under Scan direction choose one of the following:
 - **Outgoing:** Scans files being copied from the server
 - **Incoming and Outgoing:** Scans all incoming and outgoing files on the server

**Note**

The **Incoming** option is not supported by EMC CAVA/Huawei Antivirus Agent. Trend Micro recommends selecting **Incoming and Outgoing**, which scans files in both directions.

6. Under **Scan file type**, choose one of the following:
 - **All files:** Scans all file types
 - **IntelliScan:** Scans files using true file type identification. See [IntelliScan on page 1-28](#).
 - **Selected files:** Scans only specified files

If you choose **Selected files**, click **Extension List** to define the file types that you want to scan. Refer to [Selecting File Types to Scan on page 3-101](#).
7. Under **Scan options**, select one or more from the following check boxes:
 - Scan OLE layers
 - MacroTrap
 - Scan mapped network drive

See [Using Real-Time Scan on page 3-80](#) for additional information on each scan option.
8. Select the **Scan compressed files** check box to scan compressed files and then move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.

**Note**

If you choose to scan selected file types in step 5, make sure you select the extensions of compressed files in the extension list.

9. Click **Set Action** to configure how ServerProtect acts on infected files. See [Defining Actions Against Viruses in RPC Scanner and EMC CAVA Scanner on page 3-78](#).
10. Click **Apply** to save your changes.

Duplicating EMC CAVA Scanner Configuration

Procedure

1. Click a Normal Server with EMC CAVA Scanner on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option** > **Storage Scanner** on the side bar.
 - Click **Do** > **Storage Scanner** on the main menu.
3. Click **Duplicate**.

The **Select Server(s) to Duplicate Configuration to** screen appears.

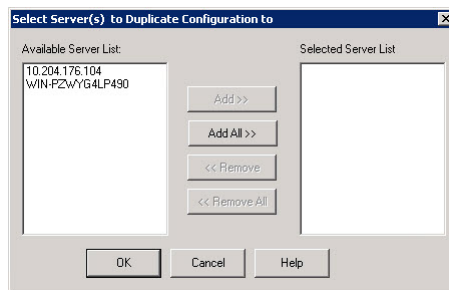


FIGURE 3-46. Duplicate configuration dialog

4. Select one or more Normal Servers in **Available Server List**. To select multiple Normal Servers, press the **CTRL** key as you select.



Note

The scanner type of Normal Server(s) shows in **Available Server List** is the same with the scanner type of the source Normal Server.

5. Do one of the following:
 - Click **Add** to add the selected Normal Server(s) to **Selected Server List**.
 - Click **Add All** to add all the Normal Server(s) in **Available Server List** to **Selected Server List**.
 6. Click **OK**.
-



Note

This procedure does not duplicate the quarantine directory and backup directory.

Using ICAP Scanner

Use ICAP Scanner if the storage supports ICAP mode for virus scanning.

Configuring ICAP Scanner

You can configure the following for ICAP Scanner:

- Scan file type
 - Scan options
 - Compressed file scanning
 - Scan action
 - Options
-

Procedure

1. Click a Normal Server with ICAP Scanner on the domain browser tree.

2. Do one of the following:
 - Click **Set Scan Option > Storage Scanner** on the side bar.
 - Click **Do > Storage Scanner** on the main menu.

The screenshot shows the 'ICAP Scanner Configuration' dialog box. It is organized into several sections:

- Scanner type:** ICAP
- Scan file type:**
 - All files
 - Use IntelliScan - Use true file type identification (Recommended)
- Scan options:**
 - Scan OLE layers: 5 (with a slider)
- Compressed file scanning:**
 - Scan compressed files
 - Scan level: 2 (with a slider)
 - Advanced settings button
- Options:**
 - Port number: 1344
 - Enable "X-Virus-ID" ICAP header
 - Enable "X-Infection-Found" ICAP header
 - Enable "X-Violations-Found" ICAP header

At the bottom of the dialog are buttons for 'Set Action...', 'Apply', 'Duplicate', and 'Help'.

FIGURE 3-47. ICAP Scanner Configuration dialog

3. Under **Scan file type**, choose one of the following:
 - **All files:** Scans all file types
 - **IntelliScan:** Scans files using true file type identification. See [IntelliScan on page 1-28](#).
4. Under **Scan options**, select **Scan OLE layers**. Move the **Scan OLE layers** slider to set the number of OLE layers. ServerProtect can scan up to five layers.
5. Under **Compressed file scanning**, select the **Scan compressed files** check box. Move the **Scan level** slider to set the number of compressed layers that you want to scan. For information on advanced settings, refer to the *Compressed file scan* topic in the online help.

6. Under **Options**, do the following:
 - Type the port number in **Port Number**. Scan Server uses this port number to listen for ICAP server connections from ICAP Clients.
 - Select **Enable "X-Virus-ID" ICAP Header**. If ServerProtect detects a virus, it adds the **X-Virus-ID** ICAP extension header in the ICAP response.
 - Select **Enable "X-Infection-Found" ICAP Header**. If ServerProtect detects a virus, it adds the **X-Infection-Found** ICAP extension header in the ICAP response.
 - Select **Enable "X-Violations-Found" ICAP Header**. If ServerProtect detects a virus, it adds the **X-Violations-Found** ICAP extension header in the ICAP response.
 7. Click **Set Action** to configure how ServerProtect acts on infected files. See [Defining Actions Against Viruses in ICAP Scanner on page 3-79](#).
 8. Click **Apply** to save the changes.
-

Duplicating ICAP Scanner Configuration

Procedure

1. Click a Normal Server with CAP Scanner on the domain browser tree.
2. Do one of the following:
 - Click **Set Scan Option** > **Storage Scanner** on the side bar.
 - Click **Do** > **Storage Scanner** on the main menu.
3. Click **Duplicate**.

The **Select Server(s) to Duplicate Configuration to** screen appears.

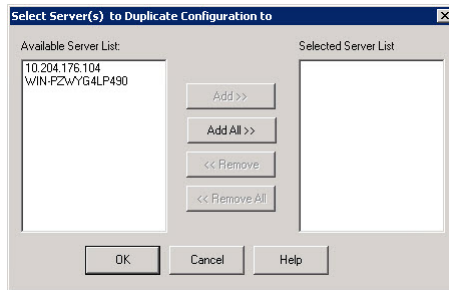


FIGURE 3-48. Duplicate configuration dialog

4. Select one or more Normal Servers in **Available Server List**. To select multiple Normal Servers, press the **CTRL** key as you select.



Note

The scanner type of Normal Server(s) shows in **Available Server List** is the same with the scanner type of the source Normal Server.

5. Do one of the following:
 - Click **Add** to add the selected Normal Server(s) to **Selected Server List**.
 - Click **Add All** to add all the Normal Server(s) in **Available Server List** to **Selected Server List**.
6. Click **OK**.



Note

This procedure does not duplicate the port number.

Selecting File Types to Scan

While configuring a Real-time Scan, Scan Now, or scheduled scan (task scan), ServerProtect lets you choose what kinds of files to scan by choosing

the file extensions. Since only certain kinds of files can contain viruses, you can benefit from this function by only scanning those file types that are more likely to be infected.

Procedure

1. In the **Real-time Scan** or **Scan Now** configuration area, under **Scan file type**, click **Selected files**, and then click **Extension List** to define the file types you want to scan.

The **Select File for Scanning** window then appears.

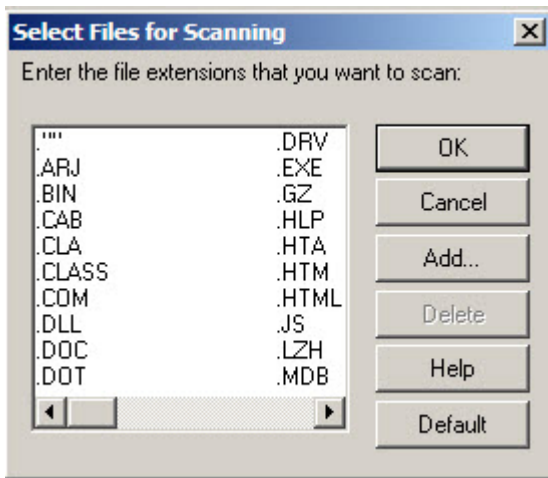


FIGURE 3-49. Select Files for Scanning window

2. Do one of the following:

- Click **Add**. The **Add Program File Extension** window appears.

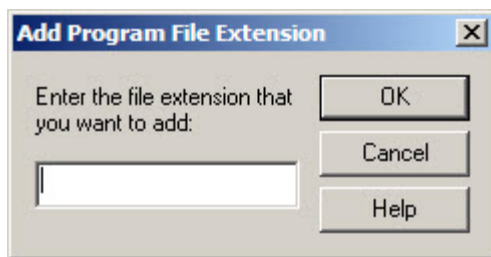


FIGURE 3-50. Add Program File Extension window

Type the file extension that you want to add in the text box, and then click **OK** to add the extension to your list. Alternatively, click **Cancel** to close the window without saving your changes. Finally, click **OK** to close the **Select files for Scanning** window.

- Click **Default** to add all the default file extensions and then click **OK** to close the **Select files for Scanning** window. Any customized extensions will be lost.

The default setting provides sufficient protection for most environments. For more information, see [Supported File Extensions for Scanning on page 3-103](#).

- Select the file extension you want to delete, and then click **Delete**.

Supported File Extensions for Scanning

ServerProtect supports the following default file extensions for scanning:

- .ARJ
- .CLASS
- .DOT
- .HLP
- .JS

- .MPT
- .OVL
- .PPT
- .SHS
- .VSD
- .XLT
- .BIN
- .COM
- .DRV
- .HTA
- .LZH
- .MSG
- .PIF
- .RAR
- .SYS
- .VST
- .Z
- .CAB
- .DLL
- .EXE
- .HTM
- .MDB
- .OCX
- .POT

- .RTF
- .TAR
- .XLA
- .ZIP
- .CLA
- .DOC
- .GZ
- .HTML
- .MPP
- .OFT
- .PPS
- .SCR
- .VBS
- .XLS

Excluding a File Extension from Scanning

Procedure

1. Select **Set Scan Option Exclusion List** from the left side bar.
2. Click **Configure > Scan Options > Exclusion List** on the main menu.
3. Under **Excluded file extension list**, click **Add**. The **Add Program File Extension** dialog box appears.

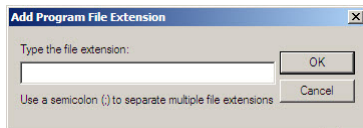


FIGURE 3-51. Add Program File Extension dialog

4. Type the file extensions that you want to exclude from being scanned. You can add multiple file extension separated by a semicolon (;).
 5. Click **OK**.
 6. To delete a previously typed file extension, select the file name from the **Excluded file extension list**, and then click **Remove**.
 7. Click **Apply**.
-

Chapter 4

Upgrading Existing ServerProtect

ServerProtect supports the product upgrading and migration from the previous versions of the product. The configuration settings of older versions can be migrate and stay effective in the new version of application.

The version 6.0 installation program can detect the existence of ServerProtect components, including the Normal Server, the Information Server and Management Console. The upgrading and migration feature is an integral part of the ServerProtect installation program. This chapter introduces the key concepts and presents to the user how to use the feature.

This chapter also introduces the troubleshooting for ServerProtect for Storage.

The topics included in this chapter are:

- *Overview of ServerProtect Upgrade Feature on page 4-2*
- *Use the Installation Package to Upgrade ServerProtect Locally on page 4-3*
- *Use the Installation Package to Upgrade ServerProtect Remotely on page 4-4*
- *Perform a Silent Mode Installation to Upgrade the Normal Servers on page 4-5*
- *Upgrading the ServerProtect Evaluation Copy on page 4-9*
- *Troubleshooting ServerProtect for Storage with RPC Scanner on page 4-9*

Overview of ServerProtect Upgrade Feature

Many users of the ServerProtect have a previous version of product already installed on their network server system, such as ServerProtect 5.8. The upgrade feature integrated in ServerProtect 6.0 offers a number of upgrade options for the users to choose, whichever the most effective will be to serve the purpose. This overview explains each of the options and introduces the related key concepts.

1. ServerProtect 6.0 Information Server can manage ServerProtect 5.8 Normal Server. Therefore, you can upgrade the Information Server and you will still be able to manage the older Normal Server.

**Note**

You cannot add an existing normal server by selecting "Add a Normal Server" or "Move a Normal Server".

2. Launch the ServerProtect installation and make proper selection to install an Information Server of the latest version of ServerProtect 6.0. To upgrade an existing Information Server, simply select the same target server during the course of installation. See [Use the Installation Package to Upgrade ServerProtect Locally on page 4-3](#) for details.
3. The next move is to install the Management Console component if the latest version one is not yet in place. See [Use the Installation Package to Upgrade ServerProtect Locally on page 4-3](#) for detailed information.
4. At this point the Management Console and the Information Server are ready. The Normal Server can be upgraded by the following methods:
 - Use the installation package to perform the upgrade locally.
 - Use the installation package to perform the upgrade remotely across the network.
 - Use silent mode installation to perform the upgrade. The silent mode installation should be used to upgrade the machine only with Normal Server installed. If the silent installer detects that other components are installed, it will terminate and do nothing. We recommend that this method be the only one to upgrade the

Normal Servers. It can prevent upgrading Information Server on the remote target machine by accident.

The rest of this chapter will focus on presenting comprehensive information. While the major attention is to describe how to perform Normal Server upgrading, the upgrade details for other components, together with related key concepts, will also be presented in aiding the users to achieve an effective and smooth program upgrade.

Use the Installation Package to Upgrade ServerProtect Locally

Because the Upgrade feature is an integral part of the ServerProtect installation program, no differences exist at all in term of user interface appearances and program behaviors. Upgrading the ServerProtect locally is by far the most straight-forward and reliable option. It is also the only way to install or upgrade a Management Console component.

To initiate a local upgrade session, use the installation package to launch the installation session in the local computer. See [Installing ServerProtect on page 2-12](#) for detailed information. The installation program will the user through the whole procedure. At the **ServerProtect Select Component** window as shown in the following:

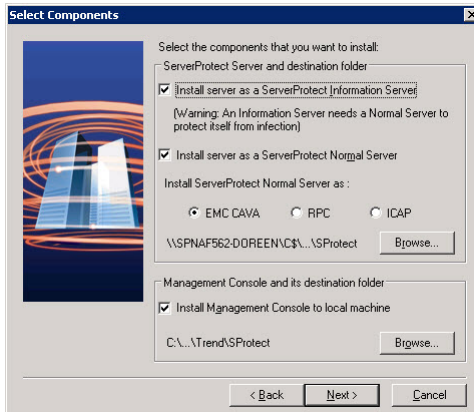


FIGURE 4-1. The ServerProtect Select Component Window

**Note**

Always keep in mind that all those components known to be existing in the system must be selected to achieve a successful upgrade.

Set the check box corresponding to those options need to be upgraded and click **Browse...** to bring up **ServerProtect Installation Path Selection** window. See step 3 in *Installing an Information Server on page 2-17*. Navigate to the target folder which needs to be upgraded on the local computer. The installation program will complete the upgrade after copying the program files and starting all related services.

**Note**

When make the selection to upgrade one ServerProtect component, keep in mind to select all the existing components, including those of the latest version already. Otherwise the installation program will pop up message box, stating that other components must be choose to continue, and bring the user back to the **ServerProtect Selection Component** window and request the user to redo the selection

**Note**

If Trend Micro Control Manager Agent is installed, it should be upgraded after the Information Server is installed.

Use the Installation Package to Upgrade ServerProtect Remotely

The way to remotely upgrade the ServerProtect is not very different to that of doing it locally. After launching the ServerProtect installation program, accepting the agreement terms and submitting the correct serial number, The ServerProtect Select Component window will be brought up. When choosing a Normal Servers as the upgrade candidate using **Browser...** button to locate the target server, instead of exploring in the local computer, the user can navigate to the connected server network system, locate the Normal Server or Information Server need to be upgraded and perform the upgrade

operation just as doing it locally. See [Installing ServerProtect on page 2-12](#) for detailed information.

**Note**

ServerProtect does not support installing or upgrading the Management Console component remotely.

Perform a Silent Mode Installation to Upgrade the Normal Servers

It is well known that, under Microsoft Windows environment, executing program by running it in DOS command line window has certain advantages. The Windows shell is capable of interpreting commands which compose a script file. One can compose such a file to automate certain tasks. In ServerProtect 6.0, capable of launching the installation program in silent mode let the users to enjoy such advantages.

**Note**

The silent install should be used to upgrade the server only with normal server exists. When silent installer detects the other components, it will quit and do nothing.

Installing ServerProtect in Silent Mode

Procedure

1. Install an Information Server.
2. Locate the SMS folder in the default installation path, and share it.

**Note**

Share the SMS folder with read and write permissions.

Make sure the target servers you want to install as Normal Servers can access the folder. If you want to perform more than one silent installation, map the SMS folder on the target servers.

3. At the target server, navigate to the SMS folder or drive that is mapped to the folder, open the file `Setup.ini`, and then add one of the following lines at the end of the file to specify the scanner type:

- To install Normal Server as NetApp RPC Scanner:

```
[CommonSection]  
NormalServerType=1
```

- To install Normal Server as ICAP Scanner:

```
[CommonSection]  
NormalServerType=2
```

- To install Normal Server as EMC CAVA Scanner:

```
[CommonSection]  
NormalServerType=4
```

**Note**

If the `NormalServerType` in `Setup.ini` is not specified, the setup installs the Normal Server as EMC CAVA Scanner by default.

4. At the target server, open a command prompt, go to the SMS folder or drive that is mapped to the folder, and then enter the following command:

```
<drive>:\setup -SMS -s -m"SPFS"
```

Example:

- a. At the target server, map the SMS folder to drive `"M"`.
- b. Open a command prompt.
- c. Go to drive M: by typing `"M: "`.

d. Type the following:

```
M:\setup -SMS -s -m"SPFS"
```

e. Press **Enter**.

Silent install will proceed and the target server will be registered with the Information Server.

For a silent installation, Normal Servers are installed in the "SMS" domain. There is no way to change the domain name during the silent installation. You can, however, rename the SMS domain after all the Normal Servers have been installed.

You can also specify a path to which ServerProtect is installed. For example, to install ServerProtect to the path `D:\Utility\AntiVirus\SProtect`, do the following:

- a. Locate the `Setup.ini` file in the source folder.
- b. Add the following lines:

```
[CommonSection]
```

```
ServerTargetUNCPath=D$\Utility\AntiVirus\SProtect
```

Where:

`ServerTargetUNCPath`: Sets the location where the Normal Server is installed.

To license the installed Normal Server, add the following lines to the `Setup.ini` file in the source folder.

```
[CommonSection]
```

```
ServerTargetSN=XXXX-XXXX-XXXX-XXXX-XXXX
```

Where:

`XXXX-XXXX-XXXX-XXXX-XXXX`: Represents the legal serial number.

You may not be able to register a Normal Server under the "SMS" domain due to the use of a domain controller on the Information Server. To resolve this issue, configure an IP address before using silent install.

To configure an IP address, do the following:

- a. Go to the Setup.ini file in the SMS folder.
- b. Replace the host name with its IP address next to AgentName then save the file.



Note

During the course of perform upgrade in silent mode, caution should be excised when sharing with others the SMS folder so that all those target servers needs to be upgraded are included. See [Installing ServerProtect in Silent Mode on page 2-28](#) for detailed information to use this powerful tool.

Upgrading ServerProtect for NetApp or EMC Celerra

If you are currently using an older version of ServerProtect for NetApp or EMC Celerra, you can upgrade to this new version. The procedure for upgrading ServerProtect for NetApp and EMC Celerra is the same as for ServerProtect for Windows.



Note

After upgrading to this version from ServerProtect for NetApp or EMC Celerra, all configuration options from your previous installation will remain unchanged.

To upgrade from previous versions of ServerProtect for NetApp or EMC Celerra, do the following:

1. Verify the system requirements for this new version.
2. See [Overview of ServerProtect Upgrade Feature on page 4-2](#).

Upgrading the ServerProtect Evaluation Copy

To enjoy the benefits of automatic software updates and technical support, upgrade to a registered version of ServerProtect for Storage. Refer to the appendix for detailed instructions on how to upgrade your evaluation copy to the full version of ServerProtect.

Troubleshooting ServerProtect for Storage with RPC Scanner

This section contains troubleshooting information and may assist you in finding a solution to frequently asked questions.

NetApp Devices do not recognize ServerProtect for NetApp Scan Servers

Description:

After a power cycle on the NetApp Device, the ServerProtect for NetApp Scan Server returns event 213, which is described as follows:

Cannot add a connection to NetApp Device. The network path was not found. Running the "**vscan scanners**" command on the NetApp Device returns the following message:

```
"No virus scanners are registered with the device."
```

The ServerProtect for Storage with RPC Scanner still manage to obtain pattern updates from Trend update servers.

Solution:

Confirm the following conditions exist:

- Remote Procedure Call (RPC) is enabled on the servers
- Vscan is turned "On" on the NetApp Device
- The Common Internet File System (CIFS) default share (C\$) still exists

After confirming these conditions, do the following:

1. Right-click a Scan Server, and then select **Device List** on the domain browser tree. The **Device List** screen appears.

2. Select one or more NetApp Devices from the list. To multi-select several NetApp Devices, press the **CTRL** key as you select.
3. Click **Logon Info**. The **Logon Information** screen appears.
4. Verify the information is correct. Otherwise, reenter it.
5. Click **OK**.

After completing these steps, repeat the registration of the Scan Server in the NetApp Device. If the password for the administrator account was recently changed, the changes may not take effect until a start up/power-cycle of the NetApp Device occurs.

The Scan Server completed scan on a file but original request was not found when scanning large files on the NetApp Device

Description:

When scanning large files on the NetApp Device in ServerProtect for Storage with RPC Scanner, the following message appears:

```
"[Server] completed scan on [FileName] but original request was not found."
```

Solution:

This situation occurs because the scan period encountered a time out due to the large size of the file. Resolve this issue by extending the Time Out period between the NetApp Device and the Scan Server.

To extend the Time Out period between the NetApp Device and the Scan Server, perform the following steps on the Scan Server:

1. Run Regedit.
2. Browse to the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect  
\CurrentVersion\Engine\Devices
```
3. Set the Value Data to the desired TimeOut period in the ScanDeviceTimeOut DWORD.

The unit of `ScanDeviceTimeout` is in seconds; this is the timeout value for the Scan Server to scan a file.

**Note**

Default timeout period for ServerProtect is 24 seconds.

To disable this warning, add the `ScanTimeoutLog` DWORD Value to the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect  
\CurrentVersion\Engine\Devices
```

Possible values for `ScanTimeoutLog`:

- 1 - Enable logging of files not scanned due to time out
- 0 - Disable logging of files not scanned due to time out

Configuring the ServerProtect for Storage with RPC Scanner to scan all file types

Description:

How to configure ServerProtect for NetApp to scan all file types?

Solution:

To scan all files placed on the NetApp Device, change the extension table of the NetApp Device so it supports all file extensions.

To make sure the extension table of the NetApp Device supports all file extensions, type the following at the NetApp Device command prompt:

```
device> vscan extensions add ???
```

**Note**

The above command will make the NetApp Device scan all file types regardless of their extension. The NetApp Device wild card is a question mark (?) and not an asterisk (*).

To add any file extension into the NetApp Device's extension table, type the following at the NetApp Device command prompt:

```
device> vscan extensions add vbs
```

The above command will make the NetApp Device scan file with a ".VBS" extension. You can replace vbs with any three-letter file extension.

Scanning all files can degrade the NetApp Device's performance and slow down virus scanning. It is recommended to scan files that are prone to viruses.

Chapter 5

Managing ServerProtect with Trend Micro Control Manager

**Note**

Trend Micro Control Manager are now renamed Trend Micro Apex Central. All the Control Manager features and settings mentioned in this document are applicable to Apex Central.

To benefit from the information the ServerProtect server can provide, register your ServerProtect server to Control Manager. ServerProtect communicates to Control Manager through the Trend Micro Management Communication Protocol (MCP) agent that is installed on the same computer along with the Information Server service.

The topics included in this chapter are:

- *[Control Manager Integration Summary on page 5-2](#)*
- *[Registering With Trend Micro Control Manager on page 5-3](#)*
- *[Verifying ServerProtect status in Control Manager on page 5-6](#)*
- *[Unregistering from Control Manager on page 5-6](#)*

Control Manager Integration Summary

This topic discusses the extent of integration between Control Manager 7.0 and this ServerProtect version.

See the Control Manager documentation for details about the features and functions described in the table below.

TABLE 5-1. Integration Summary

INTEGRATION FEATURE	FUNCTION DETAILS
Registration	From the ServerProtect management console (through the MCP agent)
Single sign-on	Not supported
License management	Not supported
Command tracking	Supported
Components deployed from Control Manager	All components
Policies managed and deployed from Control Manager	None
Information shown in User/Endpoint Directory	None
Ad-hoc query	Select any of the following data views while performing an ad-hoc query to view product information and logs: <ul style="list-style-type: none"> • Product Status Information • Product Event Information • Virus/Malware Information • Spyware/Grayware Information
Dashboard widgets specific to product	None
Dashboard widgets shared with other managed products	None
Static report templates	None

INTEGRATION FEATURE	FUNCTION DETAILS
Custom report templates (predefined)	<ul style="list-style-type: none"> • TM-Managed Product Connection/ Component Status • TM-Overall Threat Summary • TM-Spam Detection Summary • TM-Spyware/Grayware Detection Summary • TM-Suspicious Threat Detection Summary • TM-Virus/Malware Detection Summary
Event notifications	None
Data Loss Prevention (DLP) incident management	Not applicable
Suspicious object and IOC file management	Not applicable

Registering With Trend Micro Control Manager

To enable ServerProtect integration with Control Manager, you must register the product with Control Manager.

Procedure

1. Click **Start > ServerProtect Management Console**.
2. Do one of the following:
 - Click **CM Agent Setting** on the side bar.
 - Click **Do > Control Manager (CM) Agent Setting** on the main menu.

The **CM Agent Setting** screen appears. The server **Registration Status** is **Not Registered with Control Manager**.

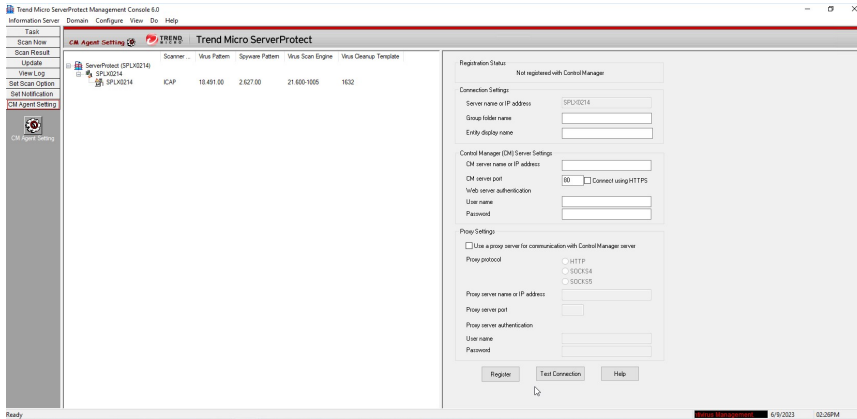


FIGURE 5-1. CM Agent Setting screen

3. Under **Connection Settings** section on the right pane, configure the following fields:
 - **Group folder name:** Type a descriptive name that identifies ServerProtect in the Control Manager product tree. The maximum length of Group folder name is 19.
 - **Entity display name:** Type the name of the ServerProtect Information Server. Choose this name carefully because this is the name that will display on the Control Manager server Product Directory to identify the ServerProtect Information server. A unique and meaningful name will help you to quickly identify the ServerProtect server in the Product Directory of Control Manager. The maximum length of Entity display name is 64 characters.



Note

The **Server name or IP address** field automatically fills the host name or the IP address of the computer on which you have installed ServerProtect.

4. Under **Control Manager (CM) Server Settings** section, specify the following:
 - **CM server name or IP address:** Type the Control Manager (CM) server name or IP address in this field.
 - **CM server port:** Type the Control Manager (CM) server port number that the MCP agent uses to communicate with Control Manager.
 - Select **Connect using HTTPS**, if you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products) or high (Only HTTPS communication is allowed between Control Manager and the MCP agent of any managed products).
 - **User name and Password:** If your network requires authentication, type the authentication information for your Internet Information Services (IIS) server.

**Note**

If you use IIS server authentication, you cannot set ServerProtect to update components from Control Manager. You must specify the URL of an update server (either the Trend Micro ActiveUpdate server or the one you set up) as the download source in the **Scheduled Update** or **Manual Update** screen.

5. If you use a proxy server to access the Trend Micro Control Manager server, select **Use a proxy server for communication with Control Manager server** under **Proxy Settings** section, and then configure the following:
 - **Proxy Protocol:** Select a proxy protocol.
 - **Proxy server name or IP address:** Type the proxy server name or its IP address.
 - **Proxy server port:** Type the proxy server's port number.

- **User name** and **Password** fields: If the proxy server requires authentication, type the user name and password for the proxy server.
6. Click **Test Connection** to verify that ServerProtect can connect to the Control Manager server using the information you have provided. If ServerProtect is unable to connect to the Control Manager server, check the settings that you have provided. Also, check the connection between the ServerProtect computer and the Control Manager server.
 7. Click **Register** to save the settings and register ServerProtect.
-

Verifying ServerProtect status in Control Manager

Procedure

1. In a Web browser, navigate to the following URL:
`https://<Control Manager server name>/Webapp/login.aspx`
Where *<Control Manager server name>* is the IP address or host name of the Control Manager server.
 2. On the menu bar, click **Products**.
 3. From the tree, expand the group folder name that you provided while registering ServerProtect with Control Manager.
 4. Verify if the server you had registered, appears in the list.
-

Unregistering from Control Manager

If you want to switch to a different Control Manager server, first unregister ServerProtect from its current Control Manager server and then register it to the new server.

Procedure

1. Click **Start > ServerProtect Management Console**.

2. Do one of the following:
 - Click **CM Agent Setting** on the side bar.
 - Click **Do > Control Manager (CM) Agent Setting** on the main menu.
The **CM Agent Setting** screen appears.
 3. Click **Unregister**.
-

Chapter 6

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting Trend Micro on page 6-3*
- *Sending Suspicious Content to Trend Micro on page 6-4*
- *Other Resources on page 6-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <https://success.trendmicro.com>.
 2. Select from the available products or click the appropriate button to search for solutions.
 3. Use the **Search Support** box to search for available solutions.
 4. If no solution is found, click **Contact Support** and select the type of support needed.
-



Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/smb-new-request>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<https://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<https://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://servicecentral.trendmicro.com/en-us/ers/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<https://success.trendmicro.com/solution/1112106>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<https://success.trendmicro.com/solution/1059565>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<https://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<https://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<https://docs.trendmicro.com/en-us/survey.aspx>

Appendix A

Converting the ServerProtect Trial Version

A 30-day trial version of ServerProtect will be installed if no serial number is entered. This version will be fully functional but after 30-days virus scanning will be disabled. After this, you should either purchase the product or remove it.

After purchasing a license, refer to the following topics to update the serial number.

The topics included in this chapter are:

- *The Software Evaluation Period Window on page A-2*
- *Viewing the Serial Number List on page A-2*
- *Updating a Serial Number on page A-4*
- *Frequently Asked Questions (FAQs) on page A-5*

The Software Evaluation Period Window

If you install the trial version of ServerProtect, the **Software Evaluation Period** window appears every time you open the Management Console. The **Software Evaluation Period** window shows which Normal Servers are using the trial version and the number of days remaining until they expire.

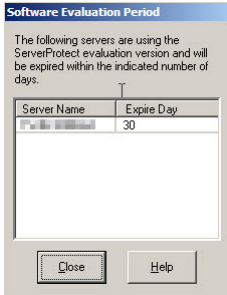


FIGURE A-1. Software Evaluation Period window

Viewing the Serial Number List

Using the Management Console, you can view the serial number of all the ServerProtect Normal Servers.

Procedure

1. Click **Help** > **About** on the main menu.

The **About ServerProtect Management Console** window appears.

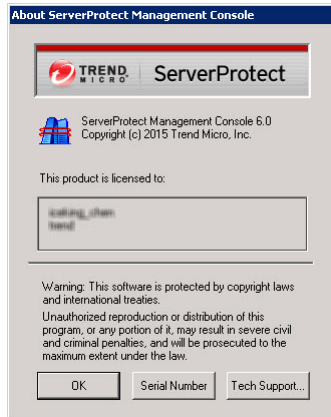


FIGURE A-2. About ServerProtect Management Console window

2. Click **Serial Number**.

The **Serial Number List** window appears showing you all the ServerProtect Normal Servers on your network, along with their respective serial numbers.

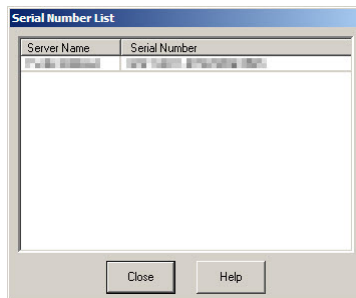


FIGURE A-3. ServerProtect Serial Number List Window

3. Click **Close** to close the **Serial Number List** window, and then click **OK** to close the **About ServerProtect Management Console** window.

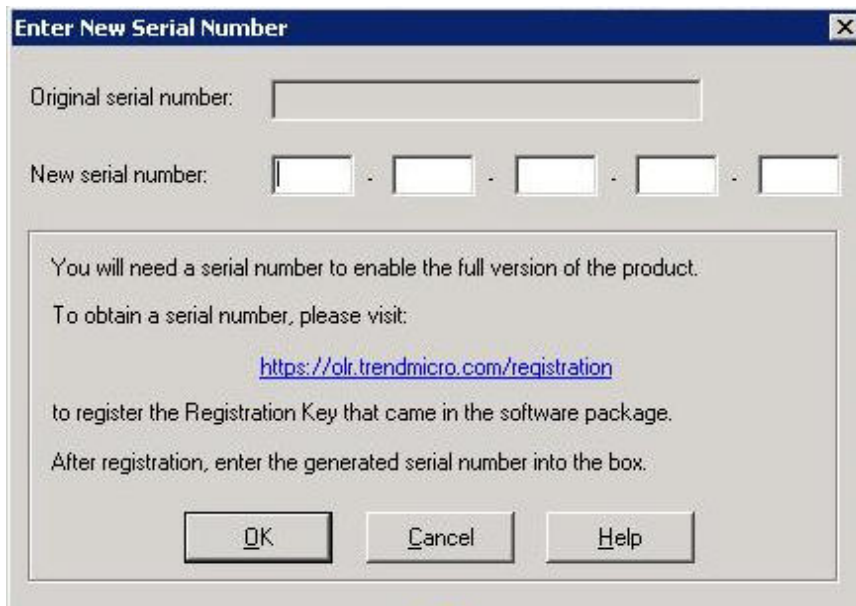
Updating a Serial Number

After you have purchased a ServerProtect license, you can update the serial number of installed ServerProtect software directly from the Management Console without reinstalling ServerProtect.

Procedure

1. Select the Normal Server you want to update the serial number for in the domain browser tree.
2. Click **Do > Update Serial Number** on the main menu.

The **Enter New Serial Number** window appears.



Enter New Serial Number

Original serial number:

New serial number:

You will need a serial number to enable the full version of the product.
To obtain a serial number, please visit:
<https://olr.trendmicro.com/registration>
to register the Registration Key that came in the software package.
After registration, enter the generated serial number into the box.

FIGURE A-4. Enter New Serial Number window

3. Type the new serial number in the **New serial number** text boxes.

4. Click **OK**. Otherwise, click **Cancel** to close the window.
-

Frequently Asked Questions (FAQs)

Virus Scan for NetApp Device

- Why ServerProtect cannot detect viruses in NetApp Device but can detect them in other locations?

File extensions that you want to scan for viruses are need to be specified on NetApp Device. You can check the current registered file extensions using command **vscan** on NetApp Device's console.

- Why ServerProtect scan the directories/files that I have already added to Exclusion List?

ServerProtect scans all the files that are requested by NetApp Devices, even if the directories/files are added to Exclusion List on NetApp Devices.

- Why I cannot scan any virus on NetApp Devices even though I am connected to the Devices?

Check whether **Vscan** is enabled on NetApp Device or not. Enabling **Vscan** also enables scanning for viruses on all Vfilers.

- How can I enable scanning for viruses on each Vfiler?

Check whether **Vscan** is enabled on NetApp Devices or not. Enabling **Vscan** also enables scanning for viruses on all Vfilers.

Upgrading ServerProtect

- Can I rollback ServerProtect to the previous version?

No. You cannot rollback ServerProtect to the previous version after the upgrade.

**Note**

To receive the latest virus protection, it is highly recommended to update your virus pattern files and virus scan engine immediately after the installation. Also, you should modify the default Deploy task, and add the Spyware pattern, Virus Cleanup Template, Virus Cleanup Engine, and Anti-rootkit Driver as the update components.

ServerProtect Virus Scan

- Why the file name and file path in Scan Result are not displayed correctly and appears to be truncated; and the Restore button is inactive?

The entry field for the file name and file path in **Scan Result** window can display the file name (including file path) up to 256 characters. If it exceeds 256 characters, the file name or file patch will be truncated and the Restore button will be inactive.

- Why the Deny Write List does not work?

The Deny Write List does not work if Real-time Scan is disabled. Enable the Real-time scan to activate Deny Write List.

- Why the pop-up notification messages do not appear, even though I have set the alert method to display pop-up message box for notifications?

Since Windows Server 2008, Windows does not support Messenger service. Therefore, the pop-up message notification will not work after Windows Server 2008.

- Why the Result in Log detail information shows the virus as cleanable, even if it is not a cleanable virus?

If the Action is set to **Clean** in the **Set Action** window, the virus will be correctly shown as cleanable or uncleanable. However, if the **Action** is not set to "**Clean**", the virus will always be shown as cleanable in Log detail information.

Miscellaneous

- Why there are old logs in Control Manager when installing CMAgent? Where did they come from?

After Control Manager agent is installed, ServerProtect sends all pre-existing logs to the Control Manager Server. However, this may generate additional network traffic. To avoid redundancy, purge all logs from the Management Console before installing the CMAgent.

- I have installed Information Server in the computer system, which is having multiple network cards belonging to different network segments. Why the Information Server could not be displayed in the Information Server list when Management Console is open, and the link between Information Servers and Normal Servers is broken?

The Information Server could not be displayed in the Information Server list because when Information Server/Normal Server attempts to connect to the correct network, it could not reach the network. To resolve the problem, uninstall both the Information Server and the Normal Server and reinstall them

- Why I can not see the Normal Server's icons in the system tray?

If you use a remote desktop connection, the Normal Server's icons may not be displayed in the system tray.

- Why I cannot see the Pattern and Engine of Normal Server?

Normal Server Pattern and Engine and other related information will not be displayed in the Management Console if the Normal Server is disconnected from the Information Server. A cross sign will be displayed in the Management Console status window if the link between Normal Server and Information Server is broken.

- Why I cannot register words in the exception list even when I enable "ExcludeUNCPath" in Admin.ini?

The configured setting may not be reflected to the Management Console when User Access Control (UAC) is enabled even though ExcludeUNCPath is enabled in Admin.ini.

- Why ServerProtect displays the login failure error if the Windows log-in password is blank?

Since Microsoft Windows has user account restriction, it requires a password for remote log-in. Therefore, if the password is not set, it will result in ServerProtect displaying login failure error.

Index

D

documentation feedback, 6-5

S

support

 resolve issues faster, 6-3



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: SPEM68262/180507