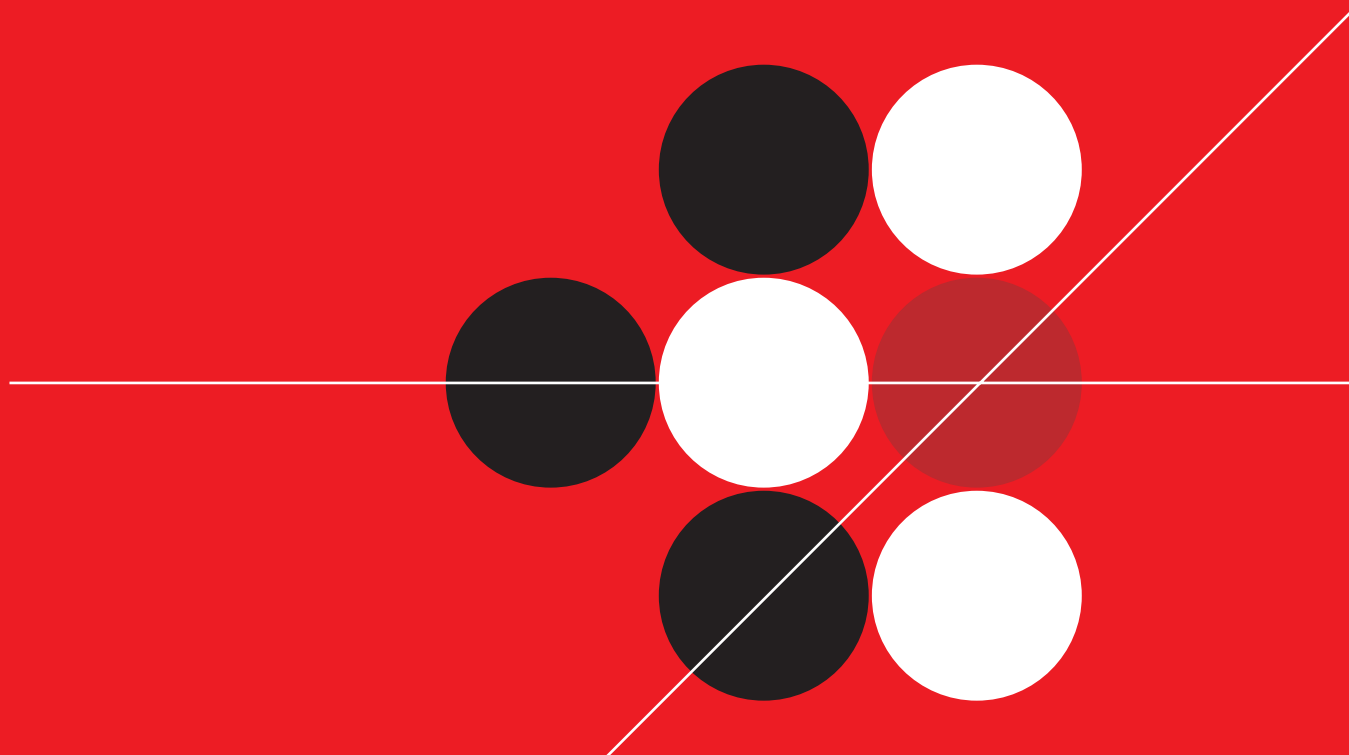
TREND MICRO™

Network VirusWall™ Enforcer 1200

Administrator's Guide



Document Part No. NVEM22856/60915

Release Date: January 2007

The user documentation for Trend Micro Network VirusWall Enforcer 1200 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site: http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Welcome to the Administrator's Guide for Trend Micro™ Network VirusWall™ Enforcer 1200. This book contains information about the tasks you need to configure Network VirusWall Enforcer 1200. This book is intended for novice and experienced users of Trend Micro Network VirusWall Enforcer 1200 who want to quickly configure, administer, and monitor the product.

The Network VirusWall Enforcer 1200 package includes the Trend Micro Solutions CD for Network VirusWall Enforcer 1200. If you are planning large-scale deployment of Network VirusWall Enforcer 1200 or have complex network architecture, refer to the *Network VirusWall Enforcer 1200 Getting Started Guide* PDF files on the Solutions CD.

This Preface discusses the following topics:

Network VirusWall Enforcer 1200 Documentation

The Network VirusWall Enforcer 1200 documentation consists of the following:

- Online Help—Web-based documentation that is accessible from the Network VirusWall Enforcer 1200 Web console.

  The Network VirusWall Enforcer 1200 Online Help contains explanations about the Network VirusWall Enforcer 1200 components and features.

- Upgrade Guide (UG)—PDF documentation that is accessible from the Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site.

  The UG contains explanations about upgrading from Network VirusWall 1200 1.5 and 1.8 to Network VirusWall Enforcer 1200.

- Getting Started Guide (GSG)—PDF documentation that is accessible from the Trend Micro Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site

  The GSG contains instructions on how to deploy Network VirusWall Enforcer 1200, a task that includes planning, testing, and preconfiguration.

- Administrator's Guide (AG)—PDF documentation that is accessible from the Trend Micro Solutions CD for Network VirusWall Enforcer 1200 or downloadable from the Trend Micro Web site

  This AG contains detailed instructions on how to configure and administer Network VirusWall Enforcer 1200 from the applicable management tools, as well as explanations on the Network VirusWall Enforcer 1200 concepts and features. See *About This Administrator's Guide* for chapters available in this book.

Note: Trend Micro recommends checking the Update Center for updates to the Network VirusWall Enforcer 1200 documentation and program file. You can download the latest versions of the *Upgrade Guide* and *Administrator's Guide* from the following location:
http://www.trendmicro.com/en/products/network/nvwe/evaluate/overview.htm

---

About This Administrator's Guide

The *Network VirusWall Enforcer 1200 Administrator's Guide*, which is in PDF, provides the following information:

- Overview of the product and its architecture, and description of all new features in Network VirusWall Enforcer 1200, see *Understanding Trend Micro™ Network VirusWall™ Enforcer 1200* on page 1-1
- Procedures to configure and administer Network VirusWall Enforcer 1200 from the applicable management tools, see *Configuring Policy Enforcement and Device Settings* on page 2-1
- Procedures to update Network VirusWall Enforcer 1200 components, see *Updating Components* on page 3-1
- Instructions to access antivirus information to evaluate your organization's virus protection policies and identify endpoints that are at a high risk of infection, see *Viewing Status, Logs, and Summaries* on page 4-1
- Troubleshooting tips for issues encountered during device administration, which includes debug and error logs interpretation, see *Troubleshooting and FAQs* on page 5-1
- Guidelines to obtain more information, see *Getting Support* on page 6-1

Audience

The Network VirusWall Enforcer 1200 documentation assumes a basic knowledge of security systems, including:

- Antivirus and content security protection
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Network devices and their administration
- Network configuration (such as the use of VLAN, SNMP)

Document Conventions

To help you locate and interpret information easily, the Network VirusWall Enforcer 1200 documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and Network VirusWall Enforcer 1200 tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

TABLE 1. Conventions used in the Network VirusWall Enforcer 1200 documentation

Chapter 1

Understanding Trend Micro™ Network VirusWall™ Enforcer 1200

This chapter introduces Trend Micro Network VirusWall Enforcer 1200 and provides an overview of its technology, capabilities, and hardware connections.

The topics discussed in this chapter include:

Trend Micro™ Network VirusWall Enforcer 1200

Trend Micro Network VirusWall Enforcer 1200 is an outbreak prevention appliance that helps organizations stop network viruses (Internet worms), block high-threat vulnerabilities during outbreaks, and quarantine and clean up infection sources including unprotected devices as they enter the network, using threat-specific knowledge from Trend Micro deployed at the network layer.

Unlike security solutions that only monitor threats or provide threat information, Network VirusWall Enforcer 1200 helps organizations take precise outbreak security actions and proactively detect, prevent or contain, and eliminate outbreaks. By deploying Network VirusWall Enforcer 1200 in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden. Network VirusWall Enforcer 1200 supports the Trend Micro™ Enterprise Protection Strategy.

Network VirusWall Enforcer 1200 monitors network packets and events that could indicate an attack against a network. Endpoint security prevents endpoints from becoming sources of network outbreaks. The device scans all the traffic to guard against security risks from passing between segments. Deploy Network VirusWall Enforcer 1200 in a switch or router environment.

Functions and Capabilities

From the Web console, you can accomplish the following administrative tasks:

- *View a Summary of Your Network's Protection Against Viruses*
- *Enforce Antivirus Policies*
- *Update Your Protection*
- *Analyze Your Network's Protection Against Viruses*
- *Perform Administrative Tasks*

View a Summary of Your Network's Protection Against Viruses

Use the Summary and Real-time status screens to help you monitor your network's protection against viruses.

View the following from the **Summary** screen:

- Policy Enforcement Status—Use this information to determine statistics on policy compliance and violations. Click the number under Violations to view the Endpoint History for more information.
- Top 5 Policies with Violations—Use this information to determine the most common or largest number of policy violations. Click the number under Violations to view additional information.
- AV Product Detection Status—Use this information to determine statistics on detected Protected Endpoints, Undetectable Endpoints (includes endpoints that do not have antivirus software and endpoints that can't be assessed), Total Endpoints, Virus Protection Ratio (the percentage of endpoints with antivirus software in relation to the total number of detected endpoints). Click Export to save the information to a file.
- Component Status—Use this information to determine whether your Network VirusWall Enforcer 1200 components are current. After an update use this information to determine if all components are current.

View the following from the **Real-time Status** screen:

- LED Status—Use this information to help determine the state of the device. Network VirusWall Enforcer 1200 has three light-emitting diodes (LEDs) that indicate the SYSTEM, POLICY, and OUTBREAK status.
- Performance Status—Use this information to determine the device resource usage. You can view CPU usage, memory usage, and concurrent connections.
- Interface Configuration Status—use this information to determine the configuration of the ports. View connection mode, port speed, and port type.

Enforce Antivirus Policies

Network VirusWall Enforcer 1200 monitors endpoints and determines the status of their antivirus protection. Based on this information, configure antivirus policy settings to block, monitor, or redirect traffic, including traffic from specified TCP and UDP ports. In this release, you can specify multiple policies for each segment in your network by configuring network zones.

Specify Damage Cleanup as a remedy when an endpoint is infected with a virus. Damage Cleanup performs the following:

- Removes unwanted registry entries created by worms or Trojans
- Removes memory resident worms or Trojans
- Removes garbage and viral files dropped by viruses
- Repairs system file configurations (such as system.ini), after they have been altered or infected by malicious code
- Returns the system to an active and clean state

Update Your Protection

Virus writers write and release new viruses through different media every day, especially the Internet. To help ensure your protection against the latest threats is current, periodically update Network VirusWall Enforcer 1200 components, including the network virus pattern file, network scan engine, file virus pattern, file virus scan engine, vulnerability assessment pattern, vulnerability engine, Damage Cleanup engine, Damage Cleanup pattern, program file, and Pattern Release History.

Analyze Your Network's Protection Against Viruses

Network VirusWall Enforcer 1200 generates various types of logs, including security and event logs. Use these logs to verify module updates and network outbreaks and view viruses found in network packets.

Perform Administrative Tasks

Network VirusWall Enforcer 1200 supports Simple Network Management Protocol (SNMP) v2 and can send traps to specific network management stations. For added security, you can require network management stations to authenticate before gaining access to the Network VirusWall Enforcer 1200 Management Information Base (MIB).

Network VirusWall Enforcer 1200 Architecture

This section describes the Network VirusWall Enforcer 1200 components and antivirus defenses, which includes discussion about its antivirus technology and types of network threats.

Components

Two major components make up a Network VirusWall Enforcer 1200 system:

- *Device(s)*
- *Management*

Device(s)

Unlike security solutions that only monitor threats or provide threat information, Network VirusWall Enforcer 1200 helps organizations take precise outbreak security actions and proactively detect, prevent or contain, and eliminate outbreaks. By deploying Network VirusWall Enforcer 1200 devices in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden. Refer to the Network VirusWall Enforcer 1200 Getting Started Guide for information about ports.

Management

Network VirusWall Enforcer 1200 provides the following management tools:

- Preconfiguration console (Serial Console/SSH)
- Web console (HTTP/HTTPS)
- LCD module (also known as LCM console)

Preconfiguration Console

The Preconfiguration console allows you to perform the network configuration and set the device settings by directly connecting to the Network VirusWall Enforcer 1200 device using a terminal communication application.

You can view the Preconfiguration console by using either a console connection to Network VirusWall Enforcer 1200 or using SSH. There are certain settings you cannot alter if you log on using SSH. The setting you cannot alter using SSH include disabling SSH connection from the **Access Control** menu. Due to this difference, the corresponding numbers for features may be different depending on the method you use to connect to the Preconfiguration console.

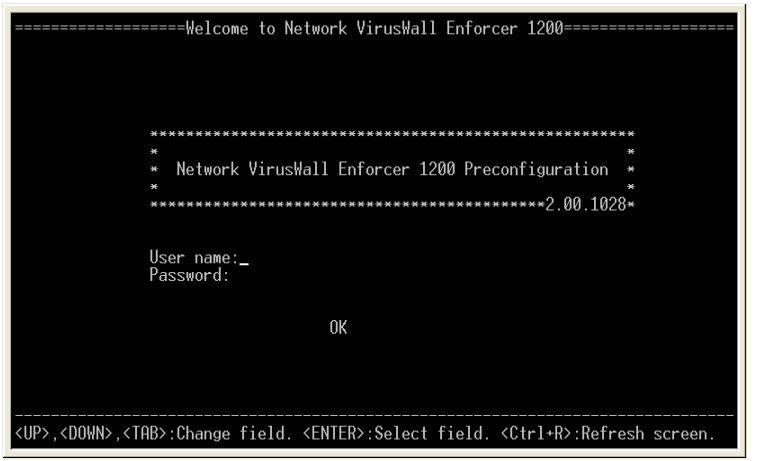


FIGURE 1-1. The Preconfiguration console login screen

Note: If you access the Preconfiguration console using SSH, type `root` at the **login as** prompt. You do not need a password to access the Network VirusWall Enforcer 1200 login screen.

Web Console

The Network VirusWall Enforcer 1200 Web console provides central management of Network VirusWall Enforcer 1200 devices. The Web console gives you the tools to configure and enforce antivirus policies for an entire organization. This enables you to react quickly to network virus emergencies from nearly anywhere using the Web console.

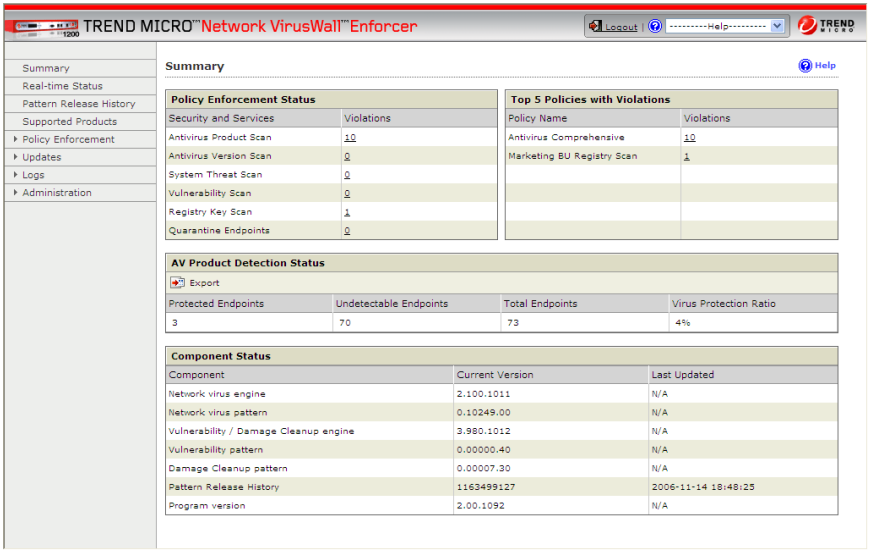


FIGURE 1-2. Network VirusWall Enforcer 1200 Web console

After preconfiguration, the Web console enables you to perform the following Network VirusWall Enforcer 1200 administrative tasks:

- Analyze your network's protection against viruses
- View the Pattern Release History
- View the Supported Products list
- Update Network VirusWall Enforcer 1200 components and settings
- Enforce antivirus policies
- View and manage logs

- Manage Network VirusWall Enforcer 1200

LCD Module

This document uses the term "LCD module (LCM or LCM console)" to refer to the Liquid Crystal Display (LCD) and the control panel Network VirusWall Enforcer 1200 front panel elements collectively. The best use of the LCM console is for simple, on-the-spot Network VirusWall Enforcer 1200 settings adjustments, as well as for viewing system information.

FIGURE 1-3. LCD and Control Panel make up the LCD module

The LCM console allows you to perform the following basic configuration:

- Configure device settings

  Device settings such as the Network VirusWall Enforcer 1200 IP address, netmask, gateway, and primary and secondary DNS servers, as well as the Control Manager IP address.

- View system information

  Use the LCM console to view the Network VirusWall Enforcer 1200 memory and CPU usages, as well as its concurrent activities.

The following table lists the differences between the management tools:

USAGE	PRECONFIG-URATION CONSOLE	WEB CONSOLE	LCD MODULE
Configure advanced device settings	●		
Configure device settings	●	●	●
Configure Endpoint Notifications		●	
Configure interface speed and duplex mode	●		
Configure IP Address Settings	●	●	●
Configure Policy Exceptions		●	
Configure Proxy Settings		●	
Create and manage Policies		●	
Manage Access Control	●	●	
Manage Administrative Accounts		●	
Monitor device events, status, and summaries		●	
Perform System Rollback/Restore of program file	●		
Register the device to Control Manager 3.5	●		●
Restart device	●	●	●
Update and deploy components		●	
View device information (for example, CPU usage, memory usage)	●	●	●
View network configuration	●	●	
View Pattern Release History		●	

TABLE 1-1. Comparison of the Network VirusWall Enforcer 1200 management tools

Antivirus Technology

Network VirusWall Enforcer 1200 is equipped with state-of-the-art antivirus technology that targets network viruses. Because it was designed to act as shield for a segment of your network, it not only can scan and drop infected network packets before they reach your endpoints, but also prevent vulnerable or infected endpoints from accessing the public network.

The number and complexity of virus threats are on the rise. Many organizations have put in place multi-layer virus protection in the form of a "security suite"– several antivirus installations that provide a patchwork virus defense. This type of virus protection, however, is effective only after servers or endpoints detect a virus; in other words, when a virus is already on your network.

Trend Micro has specially designed Network VirusWall Enforcer 1200 to recognize network viruses, drop infected packets before they enter the network, and prevent future attacks on your network caused by network virus infections. See *Understanding Security Risks* for more information on viruses, including network viruses.

In addition to network virus scanning capabilities, Network VirusWall uses PEAgent to perform assessments of endpoint. PEAgents can scan for file viruses, vulnerabilities, antivirus software, and registry keys to help ensure that endpoints are secure.

Understanding Security Risks

Tens of thousands of viruses exist, with more coming into existence each day. Although once most common in DOS or Windows, computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and Web sites.

In general, computer viruses fall into the following categories:

- **ActiveX malicious code—**resides in Web pages that execute ActiveX controls
- **Boot sector viruses—**infects the boot sector of a partition or a disk
- **COM and EXE file infectors—**executable programs with *.com or *.exe extensions
- **Joke programs—**virus-like programs that often manipulate the appearance of things on a computer monitor
- **Java malicious code—**operating system-independent virus code written or embedded in Java
- **Macro viruses—**encoded as an application macro and often included in a document
- **Trojan horses—**executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter
- **VBScript, JavaScript or HTML viruses—**reside in Web pages and downloaded through a browser
- **Worms—**a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the malware mentioned above, such as worms, are actually network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of endpoint machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

Vulnerabilities

The principle function of Vulnerability Scan is to assess an organization's network's vulnerability to various threats. Vulnerability Scan helps prevent attacks by detecting major threats associated with vulnerabilities in Microsoft operating systems.

Trend Micro assesses the risks posed by vulnerabilities by considering the significance of Internet threats that use them, the vulnerability's potential and actual impact, and the difficulty or ease by which vulnerability can be used—also known as exploitability. Vulnerabilities are considered low, moderate, important, critical, or highly critical based on the described criteria.

The following is a list of the vulnerability risk ratings:

- Highly Critical Risk—Vulnerabilities considered highly critical are vulnerabilities associated with at least ten Internet threats, regardless of how destructive the associated Internet threats are. Systems and networks not patched against these vulnerabilities will likely become infected due to the prevalence or sheer variety of associated Internet threats.
- Critical Risk—All vulnerabilities utilized by known Internet threats are critical. Vulnerabilities that remain unused by Internet threats, but that can facilitate the propagation of Internet threats across different systems, also fall under this category.
- Important Risk—Vulnerabilities that compromise vital information and allow unauthorized access to passwords and other valuable data are automatically important. Vulnerabilities that compromise the integrity or availability of system resources are similarly important.
- Moderate Risk—Vulnerabilities, whose exploitability reduces by factors such as default configuration, auditing, or difficulty of exploitation are moderate-risk.
- Low Risk—Low-risk vulnerabilities either have minimal impact on affected systems or are very difficult to exploit.

Protection Principle

The principle function of Network VirusWall Enforcer 1200 is to separate a segment of the network from the rest of public network (that is, the Internet, other LAN segments, and so on).

Tip: Trend Micro recommends deploying a Network VirusWall Enforcer 1200 device between switches or routers. Although the exact location of the device depends on the network topology, position the device between level 2 (L2) switches or level 3 (L3) routers.

Figure 1-4 depicts a representation of the Network VirusWall Enforcer 1200 protection.

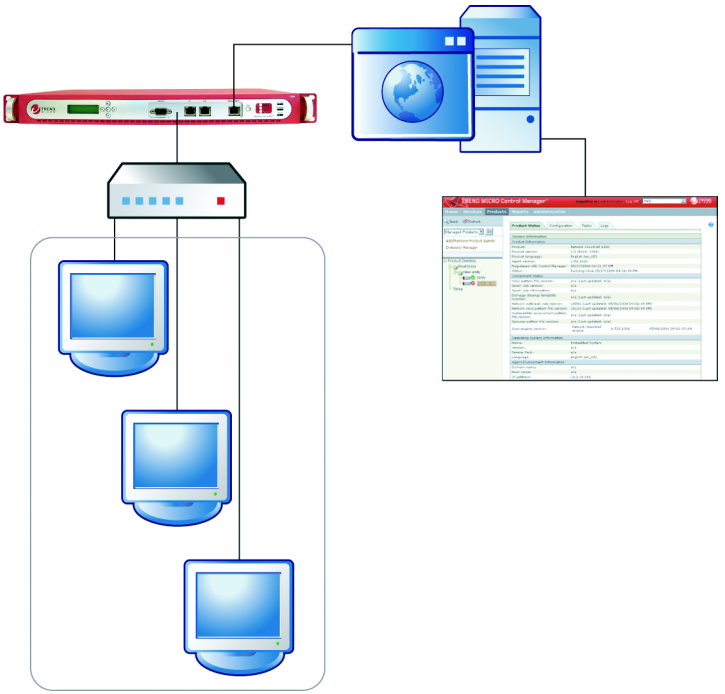


FIGURE 1-4. Network Protection

Network VirusWall Enforcer 1200 accomplishes these tasks:

- Scan network traffic to and from endpoints
- Assess vulnerability on endpoints
- Block endpoints they do not conform to the security policies of your organization
- Isolate infected endpoints to prevent viruses from spreading

Protecting Your Network

Network VirusWall Enforcer 1200 protects an organization through Policy Enforcement configured to assess:

- Endpoint Security
- Network Threat Detection
- Network Management

Policy Enforcement

Network VirusWall Enforcer 1200 is capable of identifying a packet source, and then determining if it complies with the current antivirus and vulnerability-elimination policies. The device can determine if the packet source (the endpoint where the packet originated) has antivirus protection, service packs, security patches installed, and so on. It helps ensure that machines sending inter-segment traffic comply with the policies you configure.

Policy Enforcement assesses endpoints that send traffic through a Network VirusWall Enforcer 1200 device to ensure the endpoints have:

- Active antivirus protection
- No security threats on their computer
- Required security patches installed
- Required and prohibited software on their computer

Policy Enforcement assesses the status of endpoint antivirus installations and vulnerabilities by using the following components:

- Exception list

  Network VirusWall Enforcer 1200 does not monitor endpoints belonging to the Policy Enforcement exception list for policy violations. Network VirusWall Enforcer 1200 monitors endpoints that do not belong to the exception list based on the traffic volume and connection rules. See *Global Endpoint Exceptions List* on page 1-17 for details about endpoints belonging to the exception list.

- Endpoint Security

  Network VirusWall Enforcer 1200 can scan endpoints to help prevent security risks from entering the network. Network VirusWall Enforcer 1200 uses PEAgent to perform assessments of endpoints. The device deploys PEAgent and the agent registers itself as a Windows service and runs in the background.

  You can configure policies to do the following:

  - scan endpoints to ensure the installation of antivirus software
  - scan network packets to prevent security threats from entering the network
  - ensure vulnerabilities are updated before allowing access to the network
  - specify required and prohibited registry keys to require or prohibit software on endpoint computers

  Configure Endpoint Notifications to send Windows Messenger Messages or HTTP Messages to instruct Policy Enforcement to display endpoint notifications.

  - Web Notifications— use this feature to notify endpoints using a browser.
  - Windows Messenger Service—use this feature to notify Windows-based endpoints that are using any type of protocol (that is, HTTP, FTP, telnet, and so on) to access a public network resource

---

Note: This type of Network VirusWall Enforcer 1200 endpoint notification uses the **Windows Messenger Service**. This feature does not require a Windows messaging server (for example, Windows Messenger Server or Live Communications Server) or instant messaging application (for example, Windows Messenger or MSN Messenger) to send popup notifications. If you use this feature, ensure that you have not disabled this service on endpoints.

- Network Virus Policy

  Configure Network Virus Policy to scan for network viruses and to help prevent network outbreaks. If a network virus is detected, Network VirusWall Enforcer 1200 can monitor (allow the packet to reach it's destination), drop the packet, or quarantine the endpoint computer. Use damage cleanup to repair the damage that viruses do to endpoint computers.

- Network Application Policy

  Configure Network Management Services to assess specific protocol, instant messenger, and file transfer traffic. Monitor, reject, or drop packets that Network VirusWall Enforcer 1200 detects. If you configure the action to reject the packet, the action is different based on the protocol or layer 7 service. The device sends a TCP RESET for TCP protocol related packets and ICMP Port Unreachable for ICMP and UDP packets. The drop action filters out the selected network type packets.

Viewing Logs to Assess Policy Enforcement

Logs provide information to help you monitor Policy Enforcement on your network. Configure log settings from the Logs > Log Settings screen. You can also configure the device to send the Endpoint History log to the Control Manager server from the Log Settings screen. The device sends Endpoint History logs according to the time you specify in Log Settings. Network Virus logs and Event logs are sent immediately to Control Manager if the device is registered to a Control Manager server.

Event Log—Provides information on the Policy Enforcement configuration modification.

Network Virus Log—Provides information on viruses detected in your network.

Endpoint History—Provides information on compliant endpoints, endpoints with violations, and endpoints that are quarantined. (This information is sorted by IP address and not by Date/Time.)

See the following pages to:

- Configure Policy Enforcement, *page 2-3*
- Configure the Global Endpoint exception list, *page 2-14*
- Enable Windows Messenger Service popup message, *page 2-15*

Understanding Endpoints

A packet source (a machine or a device) can have more than one network interface card (NIC) and therefore can have more than one IP address. Network VirusWall Enforcer 1200 considers each IP and MAC address pair a unique endpoint.

The following types of endpoints may exist depending on policy configuration:

- Global endpoint exceptions
- Quarantined endpoints
- Endpoints that violate a policy

Global Endpoint Exceptions List

Network VirusWall Enforcer 1200 does not monitor these endpoints for policy violation. Therefore, the device never performs an assessment of these endpoints. Since these endpoints are not scanned, they are also not protected from security threats. Potential exempted endpoints may include trusted machines owned by the organizations CEO which should not be delayed. Manage Global Endpoint Exceptions from the Web console.

Quarantined Endpoints

You can configure the device to quarantine endpoints that violate the Network Virus Policy. Quarantined endpoints are endpoints identified as a source or destination of an infected packet. After an endpoint is quarantined, the device drops all network requests by the quarantined endpoint. The only traffic the quarantined endpoint receives is the quarantine notification and the remedy you specify from the Web console. View and manage quarantined endpoints from the Endpoint History page accessible from the Web console.

Endpoints that Violate a Policy

Network VirusWall Enforcer 1200 allows you to block endpoints that violate enforcement policies. You can configure the device to block and prevent endpoints from accessing the network if the endpoint violates a policy.

If you configure the device to monitor endpoints when the device detects a policy violation, the endpoint displays as an endpoint that violates a policy. However, endpoint can still access the network with no restrictions to network traffic.

See the following pages to:

- Configure Network VirusWall Enforcer 1200 Policy Enforcement setting, *page 2-3*
- View Network VirusWall Enforcer 1200 log information, *page 4-3*

IP Address Settings

Configure the Management IP Address, Bridge IP Address, and Static Routes to minimize transfer of data through an external router.

Management IP Address

Configure the device IP address. This is the IP address you use to access the Web console to manage the device.

Bridge IP Address

Configure bridge IP addresses to allow packets to pass directly back to the device from endpoints. This list supports up to 32 entries.

An Example of When a Bridge IP Address is Necessary

In an environment where the Network VirusWall Enforcer 1200 Management IP address and the endpoint IP addresses are in the same network segment, configuring Bridge IP addresses is not necessary. See *Figure 1-5* for an example. In *Figure 1-5*, Endpoint 1 and the Management IP address belong to the same network segment. So, the Policy Enforcement Agent assessment completes as expected.

However, if the Management IP address and the endpoint IP addresses do not belong to the same network segment, policy enforcement assessment enters an infinite loop. For example, in *Figure 1-5*, Endpoint 2 and the Management IP address belong to different network segments so the assessment enters an infinite loop.

What happens:

1. Network VirusWall Enforcer (NVWE) receives traffic with Endpoint 2's IP and MAC addresses. The path of the traffic is: Endpoint 2 -> L2 Switch -> NVWE.
2. Network VirusWall Enforcer (NVWE) sends the blocking page and deploys Policy Enforcement Agent to Endpoint 2. The path of the traffic is: NVWE -> L3 Switch -> NVWE -> L2 Switch -> Endpoint 2.
3. After performing an assessment, Policy Enforcement Agent sends the results to Network VirusWall Enforcer. The path of the traffic is: Endpoint 2 -> L2 Switch -> NVWE -> L3 Switch -> NVWE.

   Network VirusWall Enforcer receives Endpoint 2's IP address and L3 Switch's MAC addresses because L3 Switch forwards the results.
4. Network VirusWall Enforcer adds a new record with Endpoint 2's IP address and L3 Switch's MAC addresses after receiving the results.
5. Endpoint 2 tries to refresh the page to continue, but remains in the assessment stage because the wrong data (Endpoint 2's IP address and the L3 Switches MAC addresses) was stored.

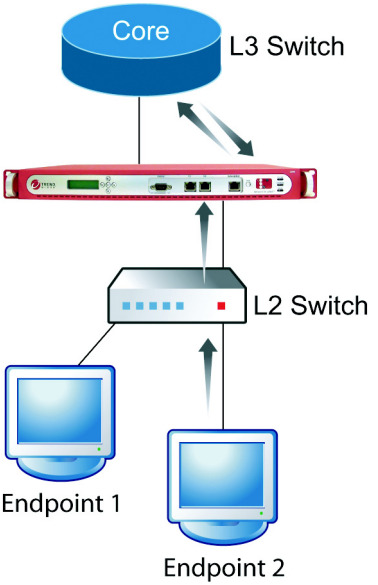


FIGURE 1-5. An Example of When a Bridge IP Address is Necessary

The solution:

Add a Bridge IP address and bind the address to a bridge port using the Web console. You can add Bridge IP addresses from Administration -> IP Address Settings | Bridge IP Address(es).

What happens after you add the Bridge IP Address:

1. Network VirusWall Enforcer receives Endpoint 2 traffic.
2. Network VirusWall Enforcer (NVWE) sends the blocking page and deploys Policy Enforcement Agent to Endpoint 2 through the bridge IP address. The path of the traffic is: NVWE -> L2 Switch -> Endpoint 2.
3. After performing an assessment, Policy Enforcement Agent sends the results to Network VirusWall Enforcer through the bridge IP address.
4. Network VirusWall Enforcer receives the results and updates the state of Endpoint 2 successfully.

Static Routes

Configure static routes to allow packets to pass through the device to different segments in your network. This list supports up to 25 entries.

An Example of When a Bridge IP Address and Static Route is Necessary

You need to configure a Bridge IP address and Static Route if you have an environment where: the Network VirusWall Enforcer 1200 Management IP address and the endpoint IP addresses do not belong to the same network segment, there is a router between the device and the endpoint, and the device and endpoint belong to the same VLAN. See *An Example of When a Bridge IP Address is Necessary* on page 1-18 for an explanation of why a Bridge IP address is necessary.

In the example illustrated by *Figure 1-6*:

- Endpoint 1 and Router 1's interface 1 belong to the same network segment.
- Endpoint 2 and Router 1's interface 2 belong to the same network segment.
- All devices and endpoints belong to VLAN 3.

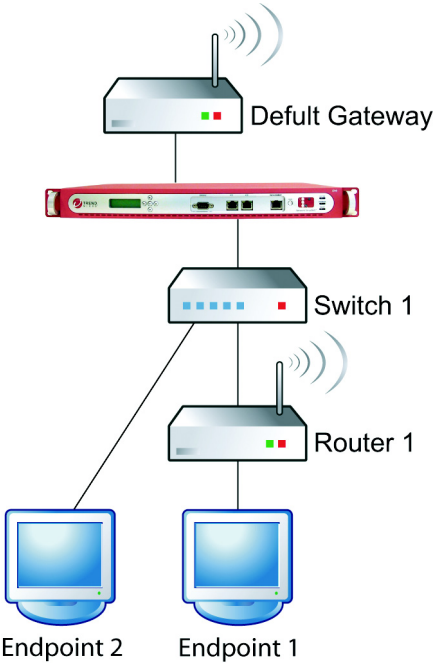


FIGURE 1-6. An Example of When a Bridge IP Address and Static Route is Necessary

What happens and when the Bridge IP address and Static Route are used:

1. Network VirusWall Enforcer (NVWE) receives traffic with Endpoint 1's IP and Router 1's MAC addresses. The path of the traffic is: Endpoint 1-> Router 1-> Switch1 -> NVWE.
2. Network VirusWall Enforcer (NVWE) needs to send packets to Endpoint 1, but they belong to different network segments. So, we add a Bridge IP address bound to VLAN 3 that is in the same network segment as Endpoint 2 and Router 1's interface 2. This allows Network VirusWall Enforcer to send packets to Endpoint 1using the Bridge IP address. The path of the traffic is: NVWE -> Default Gateway -> NVWE -> Switch 1-> Router 1-> Endpoint 1.

3. The Bridge IP address and Router 1's interface 1 belong to different network segments, so the traffic sends to the default gateway first. However, traffic between NVWE and the default gateway is unnecessary. We add a Static Route and bind it to Bridge.VLAN 3. The path of the traffic is: NVWE -> Switch 1-> Router 1-> Endpoint 1.

SNMP

Simple **N**etwork **M**anagement **P**rotocol (SNMP) is set of communications specifications for managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

In the SNMP management architecture, one or more computers on the network act as a network management station (NMS) and poll the managed devices to gather information about their performance and status. Each managed device has a software module, known as an agent, which communicates with the NMS.

Security

Managed devices can protect their MIBs by granting only specific network management stations access. One way of doing this is through authentication. Managed devices can require that all NMS's belong to a community, the name of which acts as a password that the managed devices use to authenticate management stations attempting to gain access. Additionally, the settings for a community can include access privileges, such as READ-ONLY and READ-WRITE, that are granted to network management stations.

Table 1-2 and *Table 1-3* enumerate the supported Network VirusWall Enforcer 1200 SNMP specifications:

VERSION	**v2c**
ACCESS PRIVILEGES	**READ ONLY (the GET command)**
MANAGEMENT INFORMATION BASE (MIB)	**MIB II, with the following standard objects:** • System group • Interfaces group • Enterprise group, including system status and memory utilization
ACCEPTED COMMUNITY NAMES	**Community names with the following characteristics:** • Default name– public • Access privileges- READ ONLY (the get command) • Maximum number of community names- 5 • Maximum length of community name- 33 alphanumeric characters
TRUSTED NETWORK MANAGEMENT STATIONS (NMS)	**Allows up to 255 specific network management station IP addresses to access the agent**

TABLE 1-2. Supported SNMP Agent specifications

COMMUNITY NAMES	**One community name allowed**
DESTINATION NETWORK MANAGEMENT STATION (NMS) IP ADDRESSES	**One NMS IP address allowed per community name**

TABLE 1-3. Supported SNMP Traps specifications

SNMP Trap Limitations

The following SNMP traps limitations exist:

- **Version supported:** 2c
- **Community Names:** one community name allowed
  - **Community name character limitations:** 1–33 alphanumeric characters (including underscore: "_")
- **Destination Network Management Station (NMS) IP addresses:** one NMS IP address allowed per community name
- **System location and System contact:** 0–254 characters (ASCII 32–126, excluding "&")

SNMP Traps

In addition to the standard SNMP traps, Network VirusWall Enforcer 1200 defines the following additional traps:

- Cold start—Enable SNMP.
- Link down—Remove connection from LAN port.
- Link up—Connection to LAN port established.
- Authentication failure—Login to the Web console or Preconfiguration console was not successful.
- Shutdown—Shutting down Network VirusWall Enforcer 1200.
- Boot to previous partition—Boot to previous partition by typing. This sends an SNMP trap after booting to the previous partition.
- Turn on/off OPP—If Control Manager sends an OPP command to Network VirusWall Enforcer 1200, an SNMP trap sends to notify whether OPP is on or off.

SNMP Agent Messages

In addition to the standard SNMP agent messages, Network VirusWall Enforcer 1200 defines the following additional agent messages:

- nvwScanCurrConn—Concurrent scan connections.
- nvwScanCurrMem—Current memory use for scans.

- nvwPolicyCurrConn—Concurrent number of endpoints with Policy Enforcer Agent (PEAgent).

VLAN

A **V**irtual **L**ocal **A**rea **N**etwork (VLAN) is a network consisting of endpoints that are not on the same segment of a Local Area Network (LAN) but behave as if they are on the same segment. These endpoints comprise a network in a virtual sense, through software residing on a networking device, such as a switch, which filters traffic using endpoint MAC addresses (layer 2) or IP addresses (layer 3). VLANs reduce network congestion by managing the flow of traffic between endpoints that communicate often, even if they are not on the same network segment.

Tagged and Non-tagged Frames

When a local switch on the network receives a packet, it can use the destination port, destination MAC address, or protocol to determine to which VLAN the packet belongs. When other switches receive the packet, they determine VLAN membership either implicitly (using the MAC address) or explicitly (using a tag that the first switch added to the MAC address header).

Network VirusWall Enforcer 1200 recognizes both tagged and non-tagged of IEEE 802.1Q VLAN frames, thereby preserving the VLAN structure on your network.

Tip: If you use Control Manager and the Control Manager server on your network belongs to a VLAN, bind Network VirusWall Enforcer 1200 to the same VLAN (tagged or non-tagged). This will help ensure effective communication between the Control Manager server and Network VirusWall Enforcer 1200.

Network VirusWall Enforcer 1200

Network VirusWall Enforcer 1200 is a device added to the Network VirusWall product line. This model provides the following new features:

- Network VirusWall Enforcer 1200 Web console

Failopen

The failopen or LAN bypass solution involves one Network VirusWall Enforcer 1200 device. Failopen is a fault-tolerance solution that allows the Network VirusWall Enforcer 1200 device to continue to pass traffic in an event when a software or hardware failure occurs within the device.

In addition to previously supported cards, this release of Network VirusWall Enforcer 1200 supports 10/100M copper ports that support link-state failover.

Applying a failopen solution requires the completion of the following task:

1. Establishment of Network VirusWall Enforcer 1200 connection to other network devices. By default, failopen is enabled on Network VirusWall Enforcer 1200.

Failopen Considerations

Consider the following points when implementing a failopen-based solution:

- If the switches on your network do not support auto MDI/MDI-X, use a crossover and non-crossover cable combination to enable failopen. Invalid cable combinations prevent Network VirusWall Enforcer 1200 from using failopen and can result in network issues. Refer to device documentation to determine whether your L2 switches support auto MDI/MDI-X.
- The total length of the network cable connecting ports 1 and 2 to other devices must not exceed 100 meters (328 feet) for copper port connections.

Note: This constraint only applies to failopen deployments. The network cable connecting port 1 should not exceed 50 m. Also, the network cable connecting port 2 should not exceed 50 m. A cable that is longer than the maximum length prevents failopen from working because the natural electrical resistance of a copper wire greater than that slows down the signal too much.

- Resetting a Network VirusWall Enforcer 1200 device with failopen enabled temporarily blocks the network connection.

  Table 1-4 describes the behavior of failopen ports during a device reset.

Note: The thirty-second (30s) delay occurs only when resetting the device. Powering on or off the device does not cause this delay.

TIME (SECONDS)	PROCESS	PORTS 1 AND 2 STATUS (FAILOPEN ENABLED)	PORTS 1 AND 2 STATUS (FAILOPEN DISABLED)
2	Restart the device	Disconnected	Disconnected
35	Loading Grand Unified Bootloader (GRUB)	Connected	Disconnected
	Rescue Mode	Connected	Disconnected
	Validating the boot partition flag	Connected	Disconnected
	Validating the system configuration file	Connected	Disconnected
	Booting the device	Connected	Disconnected
20	Disabling failopen and bridge learning	Disconnected	Disconnected
n/a	Preconfiguring the device	Connected	Connected

TABLE 1-4. Ports 1 and 2 status when resetting a device

Policy Prioritization and Creation

Network VirusWall Enforcer 1200 allows you to create multiple policies directed at different network segments and different types of endpoints and traffic. Network VirusWall Enforcer 1200 follows a first-match rule—once the device matches a policy to an endpoint it stops searching for additional policy matches to the endpoint down the policy list.

First-match Rule

Keep policies with broad settings at the bottom of the policy list and policies with specific settings higher in the list. Once an endpoint matches a policy, that is the only policy that Network VirusWall Enforcer 1200 applies.

For example, consider the following three policies in the table:

Priority	Endpoint	Destination	Scan Feature
1	RD, Marketing	Sales	Antivirus Program Scan, System Threat Scan, Vulnerability Scan, Network Virus Policy
2	RD, Marketing	*	Antivirus Program Scan, Network Virus Policy
3	*	*	Network Virus Policy

TABLE 1-5. Example of correctly prioritized policies

In *Table 1-5*, prioritizing policies with broad settings lower in the list prevents situations where all endpoints match the policy with broad settings. Since Network VirusWall Enforcer 1200 applies only one policy to an endpoint, once a policy matches an endpoint, no further matches are made.

In *Table 1-6*, using the same policies from above, if you rearrange the priorities and place polices with broad settings higher in the priority list, lower priority policies may never be applied to endpoints.

Priority	Endpoint	Destination	Scan Feature
1	*	*	Network Virus Policy
2	RD, Marketing	*	Antivirus Program Scan, Network Virus Policy
3	RD, Marketing	Sales	Antivirus Program Scan, System Threat Scan, Vulnerability Scan, Network Virus Policy

TABLE 1-6. Example of incorrectly prioritized policies

In *Table 1-6* specifying the policy with a setting of any source (Endpoint) and any destination as the first priority means that policies with priorities 2 and 3 are never applied. The any source (Endpoint) and any destination policy matches all endpoints and the other two policies with specific settings are never applied. Even if the first policy in *Table 1-6* is removed, the third policy is still never applied since the destination of the third policy is more specific than the second policy.

Policy Enforcement Considerations

- Carefully set policy priority based on the first-match rule.
- Traffic from endpoints must pass through Network VirusWall Enforcer 1200 or the device will not detect the endpoint.
- To minimize endpoint disruption and to monitor activity, select **Remote login** for the **Endpoint installation method, Monitor** for the **Endpoint Action**, and disable the detecting page. However, if Remote login is unsuccessful ActiveX is used.
- If you use a proxy server, include the Proxy port in HTTP Detection settings and the port number in the policy **Authentication and Network Zones**.
- If you select ActiveX for the **Endpoint Installation Method**, ActiveX needs to be enabled on the endpoint.
- If you select Remote Login, ActiveX for the **Endpoint Installation Method**, configure Remote Login Accounts and for Endpoints with Windows XP

operating systems, ensure that the firewall setting allows installation through remote login.

- If you disable endpoint detection for endpoints with unidentifiable operating systems, the device will not assess endpoints with firewall software or devices, such as routers.
- If you select user authentication, you must configure LDAP settings.
- If you select **Instant messaging detection**, ensure you add the corresponding ports to the **Authentication and Network Zones** settings page. See*Table 1-7* for the default ports to add to the **Authentication and Network Zones** settings page.

Instant Messenger	All Activities	File Transfer
Tools	TCP	TCP
MSN™	1863, 443, 80	1863 (MSN server), random (P2P), 80 (server)
Yahoo!™	5050, 80, 3478	5050 (file negotiation), 80 (data)
ICQ™	5190, 80	random (P2P), 80 (server)
AIM™	5190, 80	random (P2P), 80 (server)
IRC™	6667	

TABLE 1-7. Instant Messenger Ports

Note: The ICQ and AIM information listed are from the default settings. However, these ports can be easily changed.

- If you enable only the ActiveX and select to only assess Trend Micro products, then the Policy Enforcement Agent (PEAgent) will not install on endpoints.
- If you want to access the URL Exception page, do not type TCP port 80 in **Application Protocol Detection**.
- If you select the **Reject packet** action in **Application Protocol Detection** the following occurs for:
  - TCP: TCP reset
  - UDP: ICMP Destination Port unreachable
  - ICMP: ICMP Destination Port unreachable

- If you select the **Drop packet** action in **Application Protocol Detection**, packets are dropped and may cause certain applications to stall.
- If you select the **File Transfer Detection** service:
  - HTTPS is not scanned.
  - ASP upload is not scanned
  - If the action is **Reject Packet**, FTP downloads a file name with zero bytes.
  - If CIFS connections exist at the time of policy creation, the action may not function correctly.
  - Inform endpoints of policy requirements prior to blocking them from accessing the network. If you deploy a policy that requires endpoints to have the latest vulnerability patch installed moments after the patch is released, the majority of the endpoints on your network will violate this policy.
  - Selecting the monitor action for all new policies helps locate problem areas without disrupting endpoints. This is a good way to begin deploying new policies on your network.
  - If you select **Enable the detecting page** and select a short reassessment time interval, endpoints will frequently see the detecting page and have to wait to access the network. Consider disabling the detecting page to allow scans to run in the background instead.

Sample Policy Creation

Network VirusWall Enforcer 1200 architecture is different from previous releases of the Network VirusWall product line. In Network VirusWall Enforcer 1200, administrators create policies to detect whether any or a group of endpoints sending traffic through the device violate or comply with these policies. Configuring a policy to determine whether any or a group of endpoints violate or comply with security settings is a major feature in Network VirusWall Enforcer 1200. See *First-match Rule* on page 1-30 for more information.

Before you create policies, consider the services you want to apply to an endpoint and the type of endpoints to assess. For example, endpoints in Group A need to have antivirus software (the corresponding service is **Antivirus Program Scan**) and endpoints in Group B need to update all security patches to prevent vulnerabilities (the corresponding service is **Vulnerability Scan**).

Policy Scenario 1: Authenticated users need to have antivirus software and Guest users need to have a certain registry key.

This example requires three policies: one for authenticated users, one for guest users, and one catchall.

Sample Policy 1: Authenticated users

For the first policy, a network zone that includes all IP addresses in the network is necessary. We add the "Internal Endpoint" network zone to the Network Zones list from the Web console.

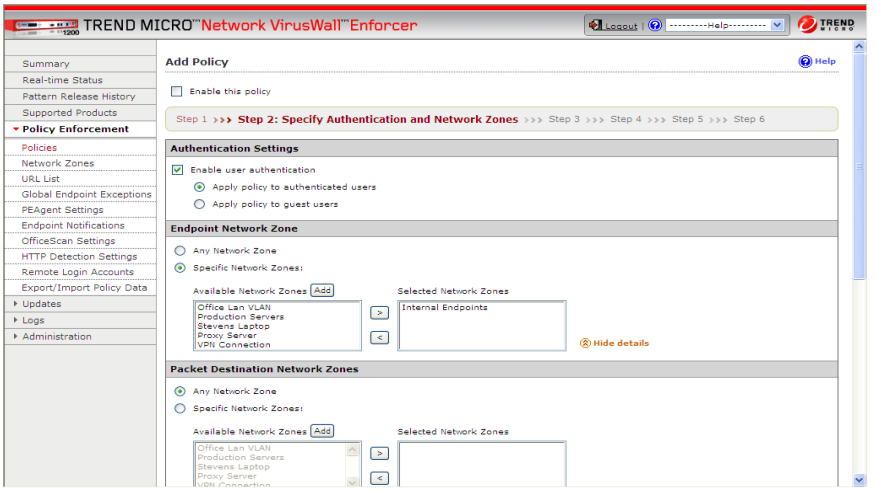


FIGURE 1-7. Sample Policy 1: Authenticated users Step 2

In **Step 2**:

- Select **Enable user authentication** and **Apply policy to authenticated users** to apply this policy to authenticated users.
- Specify the "Internal Endpoints" network zone as the **Source**.
- Select **Any destination**.

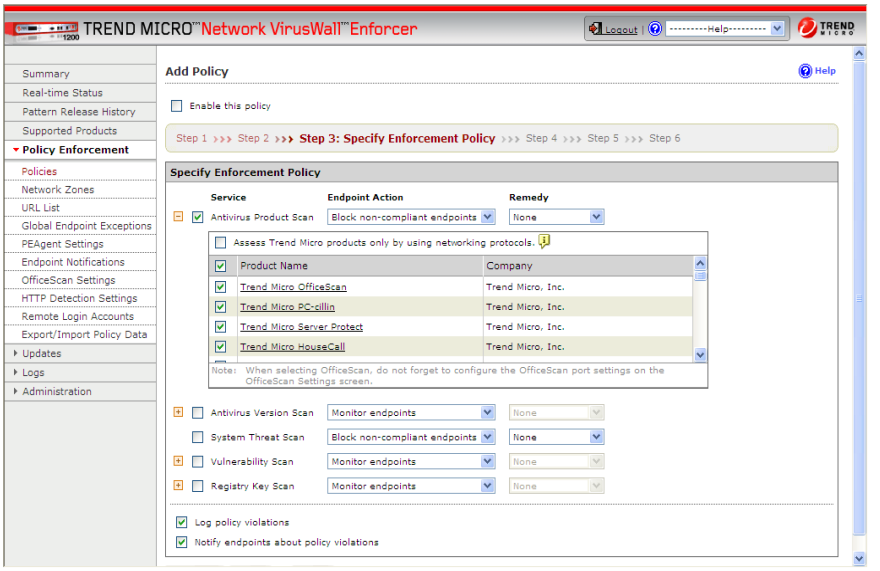


FIGURE 1-8. Sample Policy 1: Authenticated users Step 3

In **Step 3**:

- Select **Antivirus Program Scan** and all of the antivirus applications in the list.
- Select to **Block non-compliant endpoints** to block endpoints that do not have any of these applications installed.
- Select **Log policy violation** and **Notify endpoints about policy violations** to record and send a blocking page to the endpoint with a notification message.

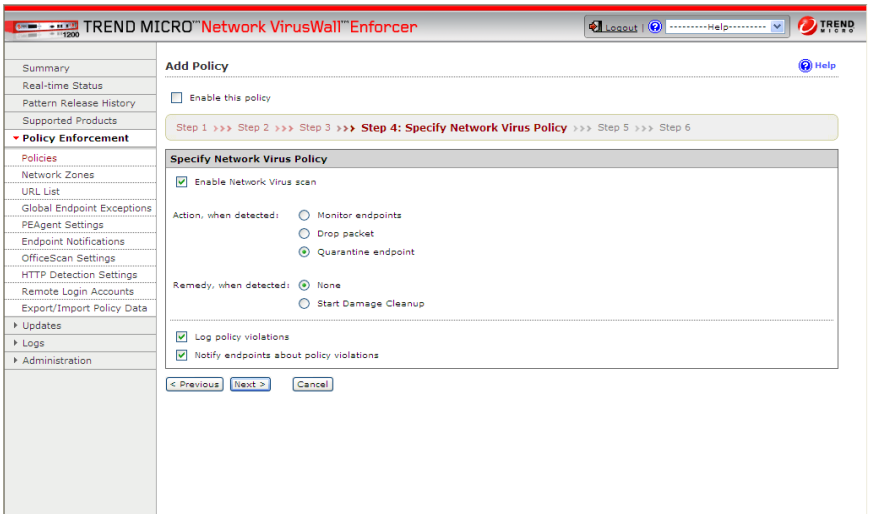


FIGURE 1-9. Sample Policy 1: Authenticated users Step 4

In **Step 4**:

- Select **Enable Network Virus Scan.**
- Select **Log policy violation** and **Notify endpoints about policy violations** to record and send a blocking page to the endpoint with a notification message.

Sample Policy 2: Guest users

For the second policy, specify the required registry key if guest users try to access endpoints belonging to the network.

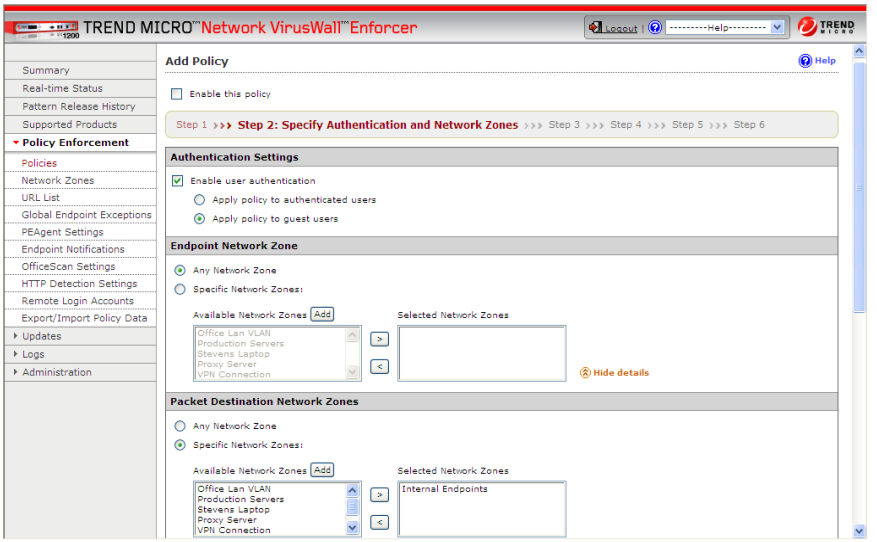


FIGURE 1-10. Sample Policy 2: Guest users Step 2

In **Step 2**:

- Select **Enable user authentication** and **Apply this policy to guest users**.
- Select **Any source**.
- Select "Internal Endpoints" as the **Packet Destination** for specific network zones.

Note: "Internal Endpoints" represents all the endpoints present on your network. You specify this value by clicking **Add** in the **Available Network Zones** list or going to **Policy Enforcement > Network Zones > Add**.

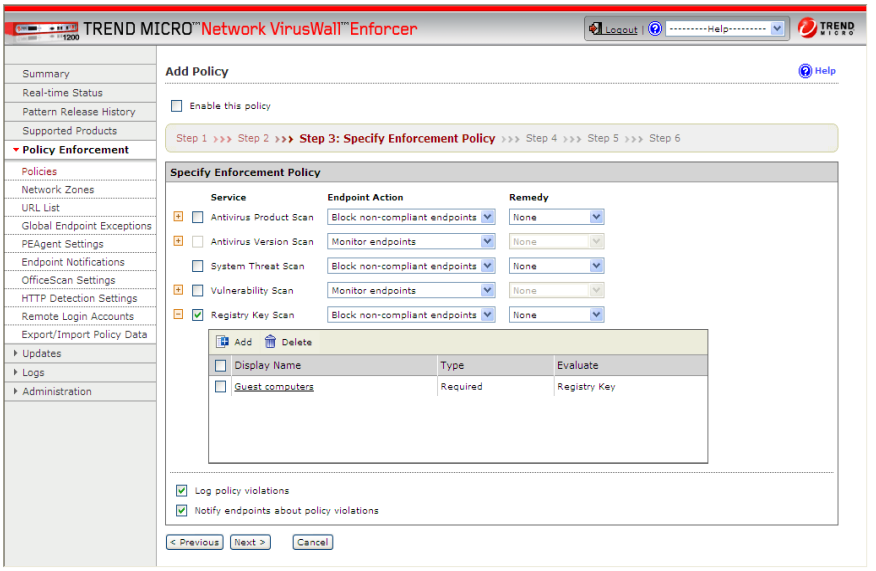


FIGURE 1-11. Sample Policy 2: Guest users Step 3

In **Step3**:

- Select **Registry Key Scan** and add the registry key as required.
- Select to **Block non-compliant endpoints** to block endpoints that do not have any of these applications installed.
- Select **Log policy violation** and **Notify endpoints about policy violations** to record and send a blocking page to the endpoint with a notification message.

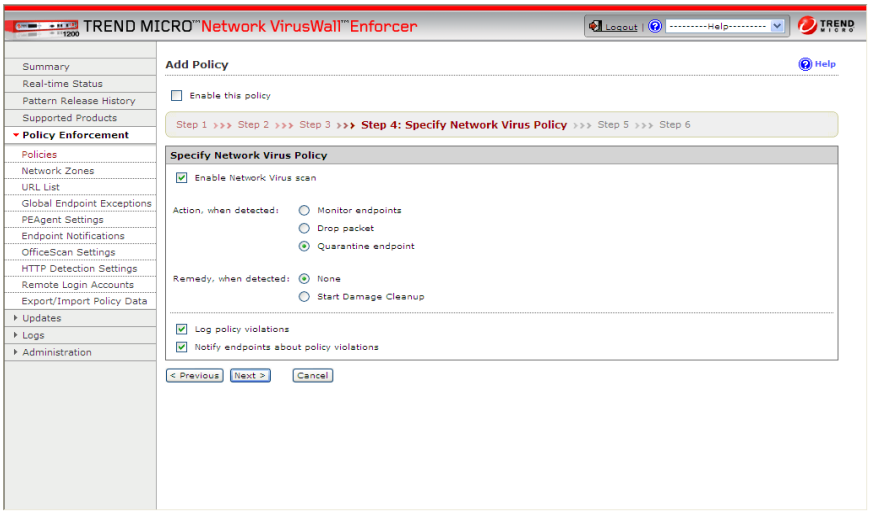


FIGURE 1-12. Sample Policy 2: Guest users Step 4

In **Step 4**:

- Select **Enable Network Virus Scan**.
- Select **Log policy violation** and **Notify endpoints about policy violations** to record and send a blocking page to the endpoint with a notification message.

Sample Policy 3: Catchall

When you create this policy, do not select **Enable user authentication** in **Step 2** and ensure that settings are configured to **Any** or **All**. Select all of the **Services** from Policy 1 and Policy 2. This policy should always remain in last priority due to the first-match rule. Any policy that has a lower priority than this policy never applies to endpoints.

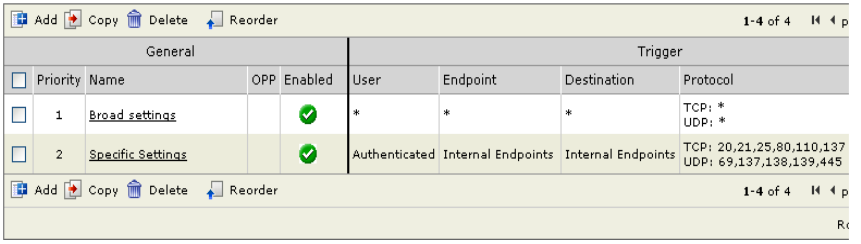


FIGURE 1-13. Example of incorrect prioritization resulting in a policy that never applies to endpoints

The second policy in this example never applies to endpoints since the higher priority policy's Trigger settings are any source, any destination, and all TCP/UDP ports. Network traffic that passes through Network VirusWall Enforcer 1200 always matches the higher priority policy. Since Network VirusWall Enforcer applies only one policy to each endpoint, once a match is made, no additional policies are applied.

Policy Scenario 2: Ensure that all endpoints have Windows XP Service Pack 2 installed.

This example requires a policy that ensures that endpoints with Windows XP operating systems have Service Pack 2 installed.

To create a policy that ensures that endpoints with Windows XP operating systems have Service Pack 2 installed:

1. Create a policy that specifies a persistent agent installation on endpoints.

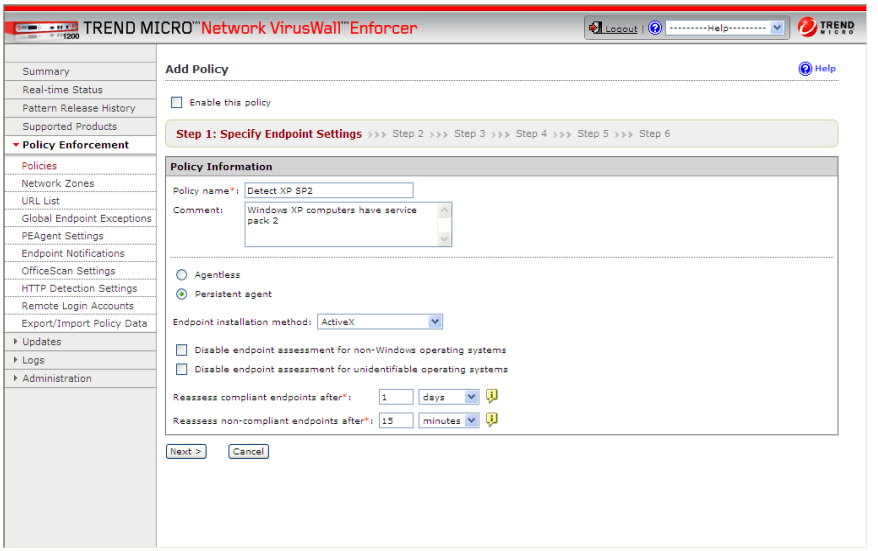


FIGURE 1-14. Policy Scenario 2: Step 1

2. For this policy, configure a network zone that includes all IP addresses of endpoints with Windows XP operating systems. You can click **Add** from **Step 2** of the **Add Policy** screens to configure a new **Network Zone**.

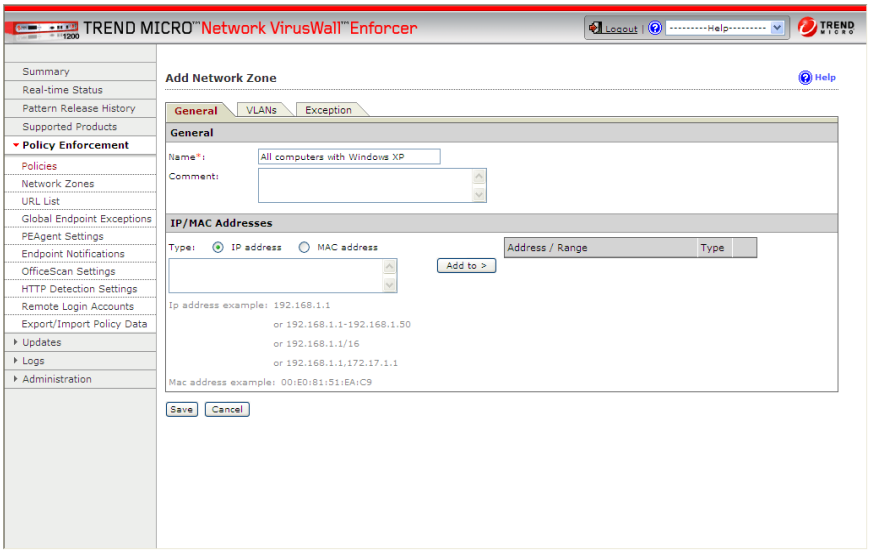


FIGURE 1-15. Policy Scenario 2: Add a Network Zone

3. Specify the Windows XP network zone as the **Source** and the **Destination** as any to apply this policy to the Windows XP endpoints.

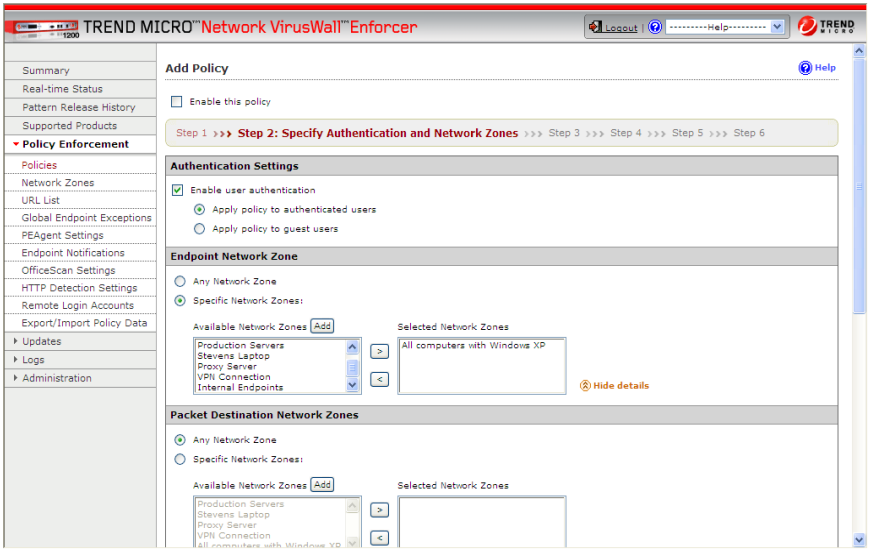


FIGURE 1-16. Policy Scenario 2: Step 2

4. Select the **Registry Key Scan** service.

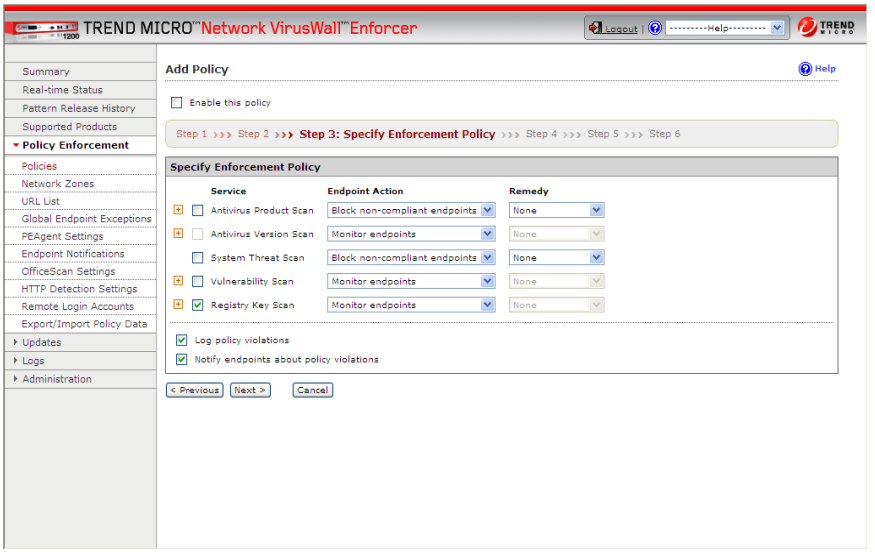


FIGURE 1-17. Policy Scenario 2: Step 3

5. Add the registry value for Service Pack 2 as a required registry key.

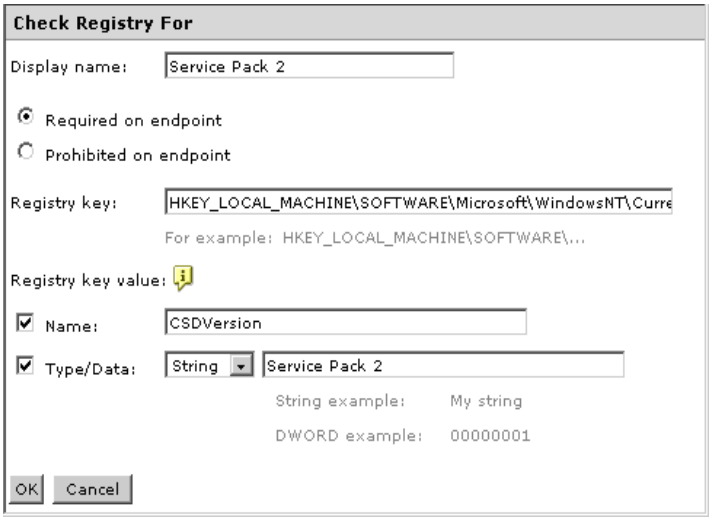


FIGURE 1-18. Policy Scenario 2: Add the required registry key

6. Confirm that the required registry key displays in the **Registry Key Scan** list.
7. Click **Save**.

Sample Deployment Scenario

Install Network VirusWall Enforcer 1200 on a network that contains Ethernet devices such as switches, routers, and hubs. Deploy the device between a switch that leads to the public network and an edge switch that protects a segment of the Local Area Network (LAN). You can also install the device between an edge switch and a hub. This section includes 3 sample deployment scenarios and 1 sample policy configuration based on the first deployment scenario.

Deployment Scenario: Standard Network

In this sample deployment scenario Network VirusWall Enforcer 1200:

- Protects the public server farm—The **Network Virus Policy** feature scans all traffic and **Policy Enforcement** applies to remote endpoints. Apply a remedy to endpoints that violate the policy.
- Protects an internal server farm—The **Network Virus Policy** feature scans all traffic.
- Is located between the switch and WAN module—The **Network Virus Policy** feature scans all traffic.
- Is located between the distribution switch and access switch—The **Network Virus Policy** feature scans all traffic and **Policy Enforcement** applies to all hosts.
- Protects a small branch office—The **Network Virus Policy** feature scans all traffic and **Policy Enforcement** applies to all hosts.

Note: In a three-level environment, it is best to not place Network VirusWall Enforcer 1200 between the core switch and distribution layer.

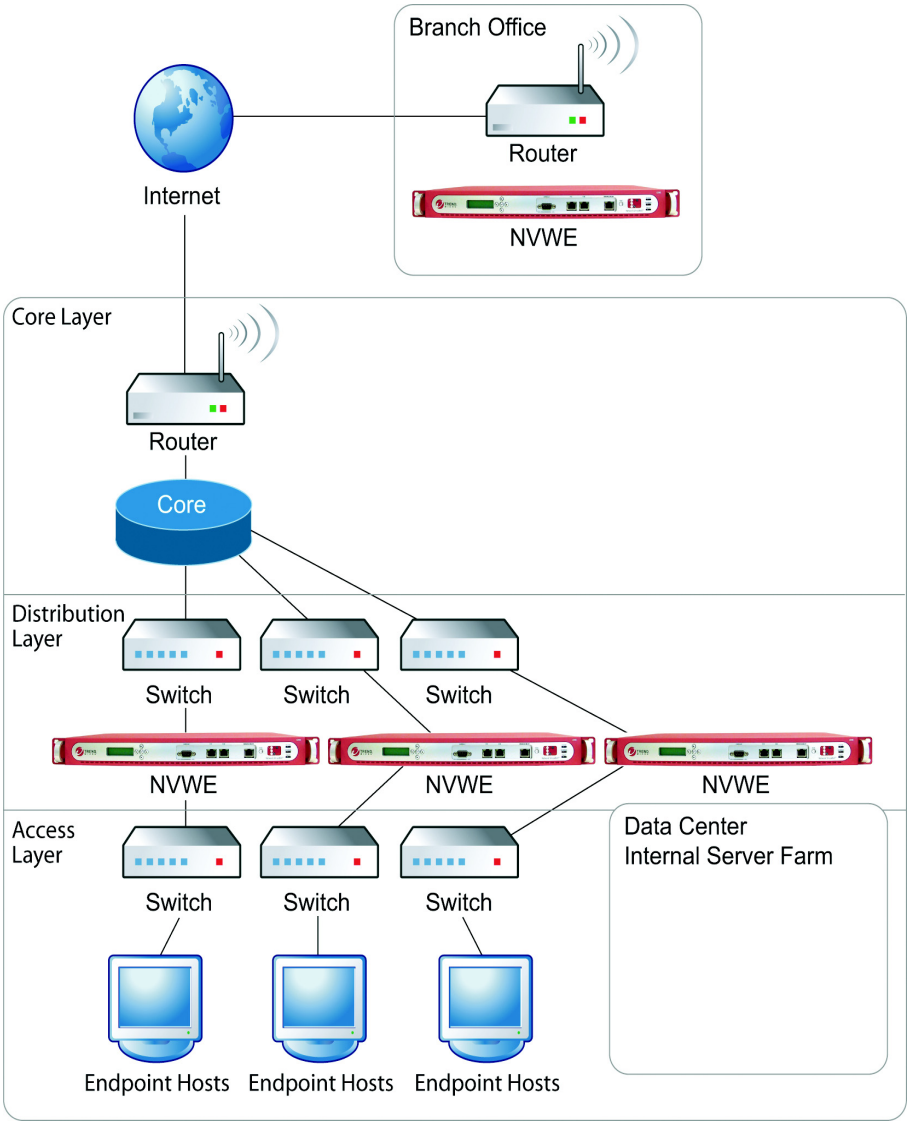


FIGURE 1-19. Standard Network Mode Scenario

Sample Policy Configuration

This section provides three sample policy configurations for *Deployment Scenario: Standard Network* on page 1-47. To protect each area of the network, create different policies based on area and type of access. For this example, we want to do the following:

- Configure policies to protect the public server farm
- Configure policies to scan packets going between the distribution switch and access switch

Server Farm Policies

This section includes a few sample policies that apply to the public server farm. Policies in the public server farm should address remote (VPN) endpoints and scan for network viruses.

The first policy, *Table 1-8*, specifically handles all traffic originating from payment processing since the public server farm can be used for billing purposes.

Settings	Details
Endpoint Settings	• **Policy name**: Priority Connection to Farm • **Policy Comment**: The priority of this should always be before "Server Farm" due to the first match rule in policies. • **Agent Type**: Agentless • **Agent deployment method**: ActiveX • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Default settings (check boxes are clear) • **Endpoint Network Zones**: Payment Processing • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **Specific ports**: 80,443,25,110,143,21 • **UDP Protocol Ports** **Specific ports**: 69,137,138,138,445 • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Drop packet **Remedy**: None • **Log policy violations**

TABLE 1-8. Priority 1: Sample Public Server Farm Policy Scenario

The second policy, *Table 1-9*, is necessary to handle all other traffic.

Settings	Details
Endpoint Settings	• **Policy name**: Server farm • **Policy comment**: The priority of this should always be after "Priority Connection to Farm" due to the first match rule in policies. • **Agent type**: Agentless • **Agent deployment method**: ActiveX • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Default settings (check boxes are clear) • **Endpoint Network Zones**: Any Network Zone • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **Specific ports**: 80,443,25,110,143,21 • **UDP Protocol Ports** **Specific ports**: 69,137,138,138,445 • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Start Damage Cleanup • **Log policy violations**

TABLE 1-9. Priority 2: Sample Public Server Farm Policy Scenario

The last policy, *Table 1-10*, handles all cases not covered by the other policies.

Tab	Details
Endpoint Settings	• **Policy name**: Catch All • **Policy comment**: The priority of this should always be last to address all other cases. • **Agent type**: Agentless • **Agent deployment method**: ActiveX • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Default settings (check boxes are clear) • **Endpoint Network Zones**: Any Network Zone • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **All ports** • **UDP Protocol Ports** **All ports** • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Start Damage Cleanup • **Log policy violations and notify endpoints about policy violations**

TABLE 1-10. Priority 3: Sample Public Server Farm Policy Scenario

WARNING! *Because of the first match rule, keep the first policy at a higher priority than the second policy and the third policy always last due to the first match rule. Once a host matches a trigger for a policy, the device does not apply any other policies to that host.*

Distribution Switch and Access Switch Policies

This section includes a few sample policies that apply to the distribution switch and access switch. Policies on this device should address endpoint hosts and scan for network viruses. You can configure these policies with the assumption that another Network VirusWall Enforcer 1200 device is between the core switch and WAN module.

The first policy, *Table 1-11*, specifically handles all traffic from Guest hosts.

Settings	Details
Endpoint Settings	• **Policy name**: Guest • **Policy comment**: This policy should be above authenticated users if using agentless detection. • **Agent type**: Agentless • **Agent deployment method**: ActiveX • **Endpoint operating system**: Disable endpoint detection for non-Windows operating systems • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Apply policy to authenticated users • **Endpoint Network Zones**: Any Network Zone • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **All ports** • **UDP Protocol Ports** **All ports** • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day

TABLE 1-11. Priority 1: Sample Distribution Switch and Access Switch Policy Scenario

Settings	Details
Enforcement Policy Settings	• **Antivirus Program Scan:** **Action**: Block non-compliant endpoints **Remedy: Redirect to URL** • **Details**: 56 Antivirus Products • **System Threat Scan** **Action**: Block non-compliant endpoints • **Vulnerability Scan** **Action**: Block non-compliant endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Log policy violations and notify endpoints about policy violations**
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Start Damage Cleanup • **Log policy violations and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, HTTP file transfer • **Log policy violations and notify endpoints about policy violations**

TABLE 1-11. Priority 1: Sample Distribution Switch and Access Switch Policy Scenario

The second policy, *Table 1-12*, specifically handles all traffic from Authenticated hosts. These are hosts that regularly access the network.

Settings	Details
Endpoint Settings	• **Policy name**: Authenticated users • **Policy comment:** This policy should be below guest and above policies that do not use the authentication feature. • **Agent type**: Persistent Agent • **Agent deployment method**: Remote login, ActiveX • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Apply policy to authenticated users • **Endpoint Network Zones**: Any Network Zone • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **Specific ports**: 80,443,25,110,143,21 • **UDP Protocol Ports** **Specific ports**: 80,443,25,110,143,21 • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day

TABLE 1-12. Priority 2: Sample Distribution Switch and Access Switch Policy Scenario

Settings	Details
Enforcement Policy Settings	• **Antivirus Program Scan** **Action**: Block non-compliant endpoints **Remedy**: Redirect to URL **Details**: 56 Antivirus Products • **Antivirus Version Scan** **Action, if detected**: Monitor **Details**: 2 versions old • **System Threat Scan** **Action**: Block non-compliant endpoints • **Vulnerability Scan** **Action**: Block non-compliant endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Registry Key Scan** **Action**: Block non-compliant endpoints **Remedy:** None **Details**: Windows Firewall, Prohibited • **Log policy violations and notify endpoints about policy violations**
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Start Damage Cleanup • **Log policy violations and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, FTP file transfer • **Log policy violations and notify endpoints about policy violations**

TABLE 1-12. Priority 2: Sample Distribution Switch and Access Switch Policy Scenario

The last policy, *Table 1-13*, handles all cases not covered by the other policies.

Settings	Details
Endpoint Settings	• **Policy name**: Catch All • **Policy comment:** The priority of this should always be last to address all other cases. • **Agent type**: Agentless • **Agent deployment method**: ActiveX • **Compliant endpoint reassessment**: 1 day • **Non-compliant endpoint reassessment**: 15 minutes
Authentication and Network Zones Settings	• **Authentication**: Default settings (check boxes are clear) • **Endpoint Network Zones**: Any Network Zone • **Packet Destination Network Zones**: Any Network Zone • **TCP Protocol Ports** **All Ports** • **UDP Protocol Ports** **All Ports** • **Daily Schedule**: Everyday • **Hourly Schedule**: All Day
Enforcement Policy Settings	• **Antivirus Program Scan** **Action**: Block non-compliant endpoints **Remedy**: Redirect to URL **Details**: 56 Antivirus Products • **System Threat Scan** **Action**: Block non-compliant endpoints • **Vulnerability Scan** **Action**: Block non-compliant endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Registry Key Scan** **Action**: Block non-compliant endpoints **Remedy:** None **Details**: Windows Firewall, Prohibited • **Log policy violations and notify endpoints about policy violations**

TABLE 1-13. Priority 3: Sample Distribution Switch and Access Switch Policy Scenario

Settings	Details
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Start Damage Cleanup • **Log policy violations and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, FTP file transfer • **Log policy violations and notify endpoints about policy violations**

TABLE 1-13. Priority 3: Sample Distribution Switch and Access Switch Policy Scenario

It is important to keep the authentication policies at a higher priority than policies that do not use the authentication feature. Once a host matches a trigger for a policy, the device does not apply any other policies to that host. This means that if two identical policies are in the list, and the higher priority policy does not use the authentication feature whereas the lower priority policy does, no hosts will match the second policy.

Chapter 2

Configuring Policy Enforcement and Device Settings

This chapter describes the management tools that you can use to take advantage of Network VirusWall Enforcer 1200 virus-scanning capabilities, which include scan options, enforcement policies, settings, and device tasks.

Network VirusWall Enforcer 1200 provides three management tools that let you easily configure its settings. See *Table 1-1* to understand the configuration options allowable from the available management tools.

The topics discussed in this chapter include:

Getting Started with Network VirusWall Enforcer 1200

Trend Micro recommends performing the following tasks after preconfiguring a Network VirusWall Enforcer 1200 device and testing a successful deployment:

- Update components (see *page 3-1*)
- Modify the Preconfiguration console accounts
- Modify the Administrative Accounts from the Web console

Tip: Refer to the *Getting Started Guide* for details on how to preconfigure and test a successful Network VirusWall Enforcer 1200 deployment.

Configuring Policy Enforcement Settings

This section includes the following topics:

Configuring Policy Enforcement Settings

Create policies to assess the status of endpoint:

- antivirus product installations
- system folders, vulnerabilities
- registry keys
- application protocols
- instant messaging
- file transfers

Configure settings to pass, block, or redirect different types of endpoint traffic.

Perform the following steps to create and configure a policy:

Step 1: Specify Endpoint Settings

Step 2: Specify Authentication and Network Zones

Step 3: Specify Enforcement Policy

Step 4: Specify Network Virus Policy

Step 5: Specify Network Application Policy

Step 6: Policy URL Exceptions

Note: See *Policy Enforcement Considerations* on page 1-31 for important about policy rules and priorities before you create a policy.

Step 1: Specify Endpoint Settings

1. From the main menu, click **Policy Enforcement**. The drop down menu displays.
2. Click **Policies** from the drop down menu. The **Policies** screen displays.
3. Click **Add** from the Policies screen. The **Add Policy** screen displays.
4. Type a policy name in the **Policy name** text box.
5. Type a comment to describe this policy in the Comment text box. (This is optional.)

6. Specify the Policy Enforcement Agent setting by selecting one of the following:
   a. **Agentless—**a one time install/terminate.
   b. **Persistent agent**—an agent that remains on the endpoint computer.
7. Specify the Endpoint installation method by selecting one of the following:
   a. **Remote login, ActiveX**—installs the Policy Enforcement Agent (PEAgent) to the endpoint computer without confirmation from the endpoint. (Configure **Remote Login Accounts** if you select this option.) The device installs the Policy Enforcement Agent (PEAgent) using ActiveX if Remote Login does not complete successfully.

      Note: If you have configured your network with an account and password that has domain administrator privileges, you can use this account and password for remote deployment to endpoints belonging to that domain.

   b. **ActiveX**— Policy Enforcement Agent (PEAgent) installation requires confirmation from the endpoint.
8. Select **Disable endpoint detection for non-Windows operating systems** to not assess endpoints with non-Windows operating systems.
9. Select **Disable endpoint detection for unidentifiable operating systems** to not assess endpoints when the device is unable to identify the operating system.

   Note: If you select this option, Network VirusWall Enforcer 1200 will not scan endpoints that have enabled the firewall feature on their computers. For example, if endpoints with Windows XP Service Pack 2 have enabled the firewall feature, the device allows traffic from those endpoints to pass through and does not protect those endpoints.

10. Specify the **Reassess compliant endpoints after** time interval.
11. Specify the **Reassess non-compliant endpoints after** time interval.
12. Click **Next**.

Step 2 : Specify Authentication and Network Zones

1. Specify the **Authentication Settings** to apply this policy towards authenticated users or guest users. You do not have to enable this feature. However, if you do enable this feature, you must create another policy with the same Trigger (**Authentication** and **Network Zone**) settings to ensure that endpoints that do not pass authentication will match a policy. (See *Sample Policy Creation* on page 1-34 for an example.)
   a. Select the **Enable user authentication** checkbox.
   b. Select either **Apply policy to authenticated users** or **Apply policy to guest users**.

   Note: Configure LDAP settings if you select **Enable user authentication**. See *Configuring LDAP Settings* on page 2-25 for more information. If you create one policy for authenticated users, create a policy that applies to users that are not authenticated.

2. Specify the **Endpoint Network Zone** to apply this policy to traffic from a specified network segment.
3. Specify the **Packet Destination Network Zones** to apply this policy to traffic going to a specified network segment.
4. Specify the **TCP/UDP Protocol Ports** to apply this policy to.

   To apply this policy to specific ports, select **Specific ports** and type port number or port ranges in the text box.
5. Specify a **Schedule** for this policy. Use this feature to restrict policies to be effective on certain days or hours.

   For example, If you select a schedule of 8:00 A.M. to 7:00 A.M., the policy is disabled from 7:00 A.M. to 8:00 A.M.
6. Click **Next**.

Step 3: Specify Enforcement Policy

Specify the services by selecting the check box next to the scan to perform:

1. **Antivirus Program Scan**—Use this feature to scan for antivirus software installation on endpoints.
   a. Select the **Antivirus Program Scan** check box.
   b. Select the check box next to products to detect.

      To assess Trend Micro products only, select the **Assess Trend products only using networking protocols** checkbox. (Remote detection is used if you select this option or if you select only Trend Micro products from the list.)
   c. Specify the **Endpoint Action** by selecting one of the following:
      i. **Monitor**—allow traffic to continue to destination
      ii. **Block non-compliant endpoints—**you can select a **Remedy** from **None**, or **Redirect to URL** to a URL where the endpoint may rectify the violation.

      If you select **Redirect to URL**, you have the option of limiting the number of pages, by selecting **Allow off-page navigation** and **Link depth**, the endpoint can navigate from the specified URL.
2. **Antivirus Version Scan**—Use this feature to require endpoints to keep the antivirus pattern versions updated.
   a. Select the **Antivirus Version Scan** check box.
   b. Specify the acceptable pattern version by selecting one of the following:
      i. **Require the latest virus pattern file—**require the endpoint to keep the virus pattern updated.
      ii. **Allow virus pattern files that are**—you can specify up to four versions old.
   c. Specify the **Endpoint Action** by selecting one of the following:
      i. **Monitor**—allow traffic to continue to destination

ii. **Block non-compliant endpoints—**you can select a **Remedy** from **None** or **Redirect to URL** to a URL where the endpoint may rectify the violation.

If you select **Redirect to URL**, you have the option of limiting the number of pages, by selecting **Allow off-page navigation** and **Link depth**, the endpoint can navigate from the specified URL.

3. **System Threat Scan**—Use this feature to scan for system threats. This feature does not scan file-based viruses, instead the feature scans for security threats in memory.

Note: If you select persistent agent and System Threat Scan service in a policy, the device may not scan the endpoint more than once. However, if you select the agentless option, the device scans the endpoint at each reassessment time interval.

---

a. Select the **System Threat Scan** check box.

b. Specify the **Endpoint Action** by selecting one of the following:

i. **Monitor**—allow traffic to continue to destination

ii. **Block non-compliant endpoints—**you can select a **Remedy** from **None** or **Redirect to URL** to a URL where the endpoint may rectify the violation.

If you select **Redirect to URL**, you have the option of limiting the number of pages, by selecting **Allow off-page navigation** and **Link depth**, the endpoint can navigate from the specified URL.

4. **Vulnerability Scan**—Use this feature to scan for known vulnerabilities. You need to manually select new vulnerabilities in the vulnerability list when the vulnerability list updates.

a. Select the **Vulnerability Scan** check box

b. Select the type of vulnerabilities to scan. Click on the vulnerability risk rating to select individual vulnerabilities.

c. Specify the **Endpoint Action** by selecting one of the following:

i. **Monitor**—allow traffic to continue to destination

ii. **Block non-compliant endpoints—**you can select a **Remedy** from **None** or **Redirect to URL** to a URL where the endpoint may rectify the violation.

If you select **Redirect to URL**, you have the option of limiting the number of pages, by selecting **Allow off-page navigation** and **Link depth**, the endpoint can navigate from the specified URL.

5. **Registry Key Scan**—Use this feature to scan for required and prohibited software by using registry key information.
   a. Select the **Registry Key Scan** checkbox.
   b. Click **Add**. The **Check Registry For** screen displays.
   c. Type the **Display Name**.
   d. Specify if this is a **Required** registry key or a **Prohibited** registry key.

> **Note:** Required registry keys are those that you want endpoints to have on their computers. Prohibited registry keys are those that you do not want endpoints to have on their computers.

   e. Type the **Registry Key**.
   f. Select **Value name** to check the value.
   g. Select **Value** and select from **String** or **DWord**.
   h. Click **OK**. The window closes and the registry key displays in the list.
   i. Specify the **Endpoint Action** by selecting one of the following:
      i. **Monitor**—allow traffic to continue to destination
      ii. **Block non-compliant endpoints—**you can select a **Remedy** from **None** or **Redirect to URL** to a URL where the endpoint may rectify the violation.

      If you select **Redirect to URL**, you have the option of limiting the number of pages, by selecting **Allow off-page navigation** and **Link depth**, the endpoint can navigate from the specified URL.
6. Select **Log policy violations** to record log entries in the Endpoint History log.
7. Select **Notify endpoints about policy violations** to send messages to endpoints that violate the policy.

8. Click **Next**.

Step 4: Specify Network Virus Policy

1. Select the **Enable Network Virus scan** check box to detect network viruses in packets that pass through the device.
   a. Specify the Action, when detected by selecting one of the following:
      i. **Monitor endpoints—**allows traffic to continue to destination
      ii. **Drop packets—**drops the packet
      iii. **Quarantine endpoint—**drops the packet and blocks the endpoint from accessing the network.
   b. Specify the **Remedy, when detected** by selecting one of the following:
      i. **None**
      ii. **Start Damage Cleanup**
2. Select **Log policy violations** to record log entries in the Endpoint History log.
3. Select **Notify endpoints about policy violations** to infrom end users when Network VirusWall Enforcer blocks their computer for violating the policy.
4. Click **Next**.

Step 5: Specify Network Application Policy

Specify the service by selecting the check box next to the scan to perform:

1. **Application protocol detection**—Use this feature to scan specific TCP or UDP ports or port ranges.
   a. Select the **Application Protocol Detection** check box.
   b. In the **TCP port** text box, type the TCP ports or port ranges to scan.
   c. In the **UDP port** text box, type the UDP ports or port ranges to scan.
   d. Select the **ICMP** checkbox to assess ICMP.

   Note: To use ICMP, ensure you select **All ports** in the TCP and UDP Protocol Ports Settings.

   e. Specify an Endpoint Action by selecting one of the following:

i. **Monitor endpoints**—allow traffic to continue to destination.

ii. **Reject packets—**rejects the packet.

iii. **Drop packets—**drops the packet.

2. **Instant messaging detection**—Use this feature to assess instant messenger software activity.

   a. Select the **Instant messaging detection** check box.

   b. Select the instant messaging software to detect by selecting from the following:

      i. **MSN**—you can select to scan **File transfer** activity or **All activity**.

      ii. **Yahoo**—you can select to scan **File transfer** activity or **All activity**.

      iii. **ICQ/AIM**—you can select to scan **File transfer** activity or **All activity**.

      iv. **IRC**—the device can only scan all activity.

   c. Specify an Endpoint Action by selecting one of the following:

      i. **Monitor endpoints**—allow traffic to continue to destination.

      ii. **Reject packets—**rejects the packet.

      iii. **Drop packets—**drops the packet.

3. **File transfer detection**—Use this feature to assess file transfer activity. Ensure that combinations such as specifying *.* for **Files to assess** and selecting **HTTP file transfer** are not specified. This type of combination may prevent access to the Internet.

   a. Select the **File Transfer Detection** check box.

   b. Select from **Windows file transfer**, **HTTP file transfer**, **FTP file transfer** to assess.

   c. Type the files to quarantine next to **Files to assess** and the files to allow next to **Exception**.

   d. Specify an Endpoint Action by selecting one of the following:

      i. **Monitor endpoints—**rejects the packet.

      ii. **Reject packets—**drops the packet.

4. Select **Allow Control Manager to modify Network Application Policy settings when an outbreak occurs** if you use a Control Manager server to

manage your products. The policy temporarily changes to the Control Manager specified policy and reverts to the original policy on this page after an Outbreak.

5. Select **Log policy violations** to record log entries in the Endpoint History log.
6. Click **Next**.

Step 6: Policy URL Exceptions

Specify URL exceptions to allow endpoint endpoints to access URLs that help remedy policy violations.

You may use wildcards when you specify URLs. Network VirusWall Enforcer 1200 supports * wildcards to allow you to match multiple URLs with a single entry. To allow access to deeper links, include a wildcard at the end of the URL. For example, http://www.trendmicro.com/*.

Using * in an expression

To represent one or more unknown characters, follow these guidelines:

- *lock—matches: block, clock, glock, plock, and flock (but not lock)
- Trend*Micro—matches: Trend Micro, Trend-Micro, Trend_Micro (but not TrendMicro)
- block*—matches: blocking, blocked, blocker, blocks, blockhead, block-point (but not block)

To specify policy URL Exceptions:

1. Select URL's from the list or create new URLs.
2. To create new URLs:
   a. Click **Add**. The **ADD URL List** displays.
   b. Type the **Name**, optional **Comment**, and **URL**.
   c. Click **Add to.** The URL displays in the table.
   d. Click **Save**. The window closes.
3. Select the new URL from the list and add it to **Selected URL Lists**.
4. Click **Next**.
5. View the details of this policy from the **Review policy** screen and click **Save**.

Configuring Network Zones

Using Network Zones to group IP and MAC addresses with Network VirusWall Enforcer 1200 ports allows you to apply policies to traffic to or from specific segments of your network.

Performing the following tasks to create a network zone:

- Configure General settings
- Configure Interfaces / VLAN settings
- Configure Exceptions settings

Configuring General Settings

This is the first task to configuring a network zone to help manage network security.

Network Zone Considerations:

- If you do not specify any IP/MAC addresses, the network zone includes all IP/MAC addresses.
- If you do not select any interfaces, the network zone includes all the interfaces.
- If you do not specify any exceptions, the network zone does not include any exceptions.

To configure General network zone settings:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Network Zones** from the drop down menu. The **Network Zones** screen displays.
3. Click **Add**. The **Add Network Zones** screen displays.
4. Type the **Name** of the network zone and optional **Comment** under **General**.
5. Select **IP address** or **MAC address** under **IP/MAC Address**.
6. Type IP or MAC addresses in the text box.
7. Click **Add to**. The information displays in the table.
8. Click **Save**.

Configuring Interfaces / VLAN settings

This is the second task to configuring a network zone to help manage network security.

To configure Interfaces / VLAN settings:

1. Click the **Interfaces / VLAN** tab. The **Interfaces / VLAN** screen displays.
2. Select the ports for the network zone under **Customize Interface Settings**. You cannot select unavailable ports.

   Note: Selecting no ports is the same as selecting all ports.

3. Specify the **VLAN Settings** by selecting **All tagged and untagged VLAN IDs**, **All tagged VLAN IDs**, or **Specific VLAN IDs**.

   If you select **Specific VLAN IDs** you may type multiple **VLAN IDs** in the text box.
4. Click **Save**.

Configuring Exception Settings

This is the last task to configuring a network zone to help manage network security.

1. Click the **Exception** tab. The **Exception** screen displays.
2. Select **IP address** or **MAC address** under **Network Zone Exception**.
3. Type IP or MAC addresses in the text box.
4. Click **Add to**. The information displays in the table.
5. Click **Save**.

View the details of the network zone you created from the **Network Zones** screen.

Configuring the URL List

Specify URL exceptions to allow endpoints to access URLs that help remedy policy violations. This list can be used when you create policies to specify exceptions.

The URL exceptions list supports the * wildcard. Typing http://www.*.com allows access to the root directory. Specify access to deeper links by typing http://www.*.com/*.

To add to the URL List:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **URL List** from the drop down menu. The **URL List** screen displays.
3. Click **Add**. The **Add URL List** screen displays.
4. Type the **Name**, optional **Comment**, and **URL**.
5. Click **Add to**. The URL displays in the table.
6. Click **Save**. The **URL List** screen displays.

View the details of the new URL exception you've just created from the **URL List** screen. Use the **URL List** screen to manage all URL exceptions.

Specifying Global Endpoint Exceptions

Specify Global Endpoint exceptions to ensure that certain computers or network segments are not scanned. Policy Enforcement assessments will not scan any Global Endpoint exceptions.

To add to the Global Endpoint Exceptions:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Global Endpoint Exceptions** from the drop down menu. The **Global Endpoint Exceptions** screen displays.
3. Select **IP address** or **MAC address** under **Global Endpoint Exception List**.
4. Type IP or MAC addresses in the text box.
5. Click **Add to**. The information displays in the table.
6. Click **Save**.

WARNING! *Endpoints belonging to the Global Endpoint Exception list are not protected by Network VirusWall Enforcer 1200.*

Configuring PEAgent Settings

You can configure Network VirusWall Enforcer 1200 to use agentless or persistent agent mode. In persistent agent mode the PEAgent, which installs on the end-users' client computer, communicates with Network VirusWall Enforcer 1200. You can

configure the Network VirusWall Enforcer 1200 port which communicates with the PEAgents.

To configure the PEAgent communication port:

1. Click **Policy Enforcement > PEAgent Settings** in the side menu. The PEAgent Settings screen appears.
2. Type a valid port number for PEAgent-Network VirusWall Enforcer 1200 communication in the PEAgent port field.

   Valid port numbers are between 1024 to 65535.

WARNING! *Changing this setting will stop communication with all PEAgents until the PEAgents update their listening port to the same port number as Network VirusWall Enforcer 1200.*

---

3. Click **Save**.

Configuring Endpoint Notifications

Configure Endpoint Notifications to inform endpoints of policy violations. Specify PEAgent notifications to send as Windows messages or PEAgent pop up messages.

To configure Endpoint Notifications:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Endpoint Notifications** from the drop down menu. The **Endpoint Notifications** screen displays.

- Click the notification to configure under **Notification Type.** The Message screen displays.
- Type changes to the default message directly in the text box. Click **Preview**.
- Click **Save** when the message displays correctly.

To configure Endpoint Notification Settings:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Endpoint Notifications** from the drop down menu. The **Endpoint Notifications** screen displays.

3. Click the **Settings** tab.
4. Select to display the **Trend default look and feel** or **Custom** to specify the Page Title, Title Text color, and Banner color.
5. Select whether to enable or disable the detecting page. If you disable the detecting page, the endpoint may not be aware that the device is making an assessment.

Note: You may configure the appearance of **Endpoint Notifications** by selecting the **Settings** tab from the **Endpoint Notifications** screen.

---

6. Click **Save**.

To configure the Windows Messenger Service Settings:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Endpoint Notifications** from the drop down menu. The **Endpoint Notifications** screen displays.
3. Specify the encoding the method the messages should use. English is the default setting.
4. Specify the method in which the method appears from the Popup method drop down list.
5. Click **Save**.

Configuring OfficeScan Settings

The device can assess whether endpoints have antivirus software installed. If you use OfficeScan to protect your network, specify the port to use to communicate with OfficeScan.

To specify the OfficeScan detection port:

1. Click **Policy Enforcement** from the main menu. The Policy Enforcement menu displays.
2. Click **OfficeScan Settings** from the Policy Enforcement menu. The OfficeScan Detection screen displays.

3. Type the port number next to **Trend Micro OfficeScan port(s)**. Use a comma to separate ports.
4. Click **Save**.

HTTP Detection Settings

Specify the HTTP ports to allow the device to detect HTTP traffic.

To add a port for HTTP detection:

1. Click **Policy Enforcement** from the main menu. The Policy Enforcement menu displays.
2. Click **HTTP Detection Settings** from the Policy Enforcement menu. The HTTP Detection Settings screen displays.
3. Type the port number next to **Port** and type an optional comment.
4. Click **Add to**. The port is added to the current list on the right.
5. Click **Save**.

Remote Login Accounts

To use the remote login feature for deploying the PEAgent to endpoints, you must configure remote login accounts. Windows 95, 98, ME, and XP Home operating systems do not support remote login. For operating systems that do not support remote login, agent installation will use ActiveX instead.

To add a remote login account:

1. Click **Policy Enforcement** from the main menu. The **Policy Enforcement** menu displays.
2. Click **Remote Login Accounts** from the **Policy Enforcement** menu. The Remote Login Accounts screen displays.
3. Click **Add**. The Add Remote Login Account screen displays.
4. Select the **Enable this account** checkbox.
5. Type the **User ID**, **Password**, **Confirm** (the password), and optional **Comment**.
6. Click **Save**.

Note: You can specify a User ID with [0-9], [a-z], [A-Z], [@], [-], [.], [_], [\ ], and [/]. You can specify a password with all alphanumeric characters and symbols, except ["], [‘], and [\ ]. The following format must be used if you want to specify a domain account as the **User ID**: domain\testuser, or domain/testuser, or testuser@zone.

No User ID can contain multiple copies of the following characters: [@], [\ ], or [/].

Exporting and Importing Policy Data

You can export policy data for backup purposes or for deploying policy data to another Network VirusWall Enforcer 1200 device. Import policies from another Network VirusWall Enforcer 1200 device to quickly replicate policy settings. When you import a policy file, the policy file overwrites all current policy settings.

To export Policies:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Export/Import Policy Data** from the drop down menu. The **Export/Import Policy Data** screen displays.
3. Click **Export** under **Export Policies**. A **File Download** screen displays.
4. Select **Save** and specify the location to save the policy data to.
5. Click **Save**.

To import Policies:

1. Click **Policy Enforcement** from the side menu. The drop down menu displays.
2. Click **Export/Import Policy Data** from the drop down menu. The **Export/Import Policy Data** screen displays.
3. Click **Browse** under **Import Policies**. The **Choose File** screen displays.
4. Select the file to import and click **Open**. Network VirusWall Enforcer 1200 resets after the import completes.

Configuring Device and System Settings

This section includes the following topics:

Configuring Access Control

Configure Access Control settings to help keep undesired users from accessing Network VirusWall Enforcer 1200.

Restricting SSH Console Access

Enable or disable SSH console access from the **Access Control** screen on the Web console.

From the Preconfiguration console, you must connect to Network VirusWall Enforcer 1200 using a direct console connection to change SSH console access.

IP Addresses Restriction

Enable IP address access from the **Access Control** screen on the Web console. Specify IP addresses to allow to access the Web console.

Configuring Administrative Accounts

Configure Administrative Accounts to manage Network VirusWall Enforcer 1200. There are three kinds of accounts in Network VirusWall Enforcer:

- **Operator accounts**—can view configuration information from the Web console, but cannot login to the Preconfiguration console.
- **Power User accounts**—can view configuration information from the Web and Preconfiguration consoles.
- **Administrator accounts**—has complete access to the Web and Preconfiguration consoles.

To add an administrative account:

1. Click **Administration** from the main menu. The **Administration** menu displays.
2. Click **Administrative Accounts** from **Administration** the menu. The **Administrative Accounts** screen displays.
3. Click **Add**. The **Add Administrative Account** screen displays.
4. Type the **User ID**, **Password**, and **Confirm** (the password).
5. Select the **Privileges**.
6. Click **Save**.

Using Backup Configuration

You can export configuration data for backup purposes or for deploying configuration data to another Network VirusWall Enforcer 1200 device. Import a configuration file from another Network VirusWall Enforcer 1200 device to quickly replicate configuration settings. When you import a configuration file, the configuration file overwrites all current policy and network settings.

To backup the configuration file:

1. Click **Administration** from the side menu. The drop down menu displays.
2. Click **Backup Configuration** from the drop down menu. The **Backup Configuration** screen displays.
3. Click **Backup** under **Backup Configuration File**. A **File Download** screen displays.
4. Select **Save** and specify the location to save the configuration file to.
5. Click **Save**.

To restore the configuration file:

1. Click **Administration** from the side menu. The drop down menu displays.
2. Click **Backup Configuration** from the drop down menu. The **Backup Configuration** screen displays.
3. Click **Browse** under **Restore Configuration File**. The **Choose File** screen displays.
4. Select the file to import and click **Open**. Network VirusWall Enforcer 1200 resets after the import completes.

Importing and Exporting the Configuration File from the Preconfiguration console

Use the Preconfiguration console to import and export the Network VirusWall Enforcer 1200 configuration. This allows easy replication of existing Network VirusWall Enforcer 1200 settings from one Network VirusWall Enforcer 1200 to other devices of the same model and locale settings.

Note: Importing or exporting the configuration is not possible when using Minicom or SSH.

To import the configuration file:

1. Access the Network VirusWall Enforcer 1200 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type 6 in the main menu. The System Tasks submenu appears.
3. Type `3` to import the configuration file. A confirmation screen appears.
4. Type `y` to continue.

Note: Refer to the Getting Started for detailed information on using the preconfiguration menu through the Preconfiguration console.

To export the configuration file:

1. Access the Network VirusWall Enforcer 1200 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Type `6` in the main menu. The System Tasks submenu appears.
3. Type `4` to export the configuration file. A confirmation screen appears.
4. Type `y` to continue.

Note: Refer to the *Getting Started Guide* for detailed information on using the preconfiguration menu through the Preconfiguration console.

Performing Device Tasks

If an emergency arises whereby you want to isolate your network, you can lock Network VirusWall Enforcer 1200 to block all traffic that would normally pass through the device. Likewise, if you are experiencing problems with Network VirusWall Enforcer 1200, you can perform a reset.

Locking Network VirusWall Enforcer 1200

The **Device Tasks** screen allows you to lock Network VirusWall Enforcer 1200, which performs the same function as physically disconnecting the device from the network. Unlock Network VirusWall Enforcer 1200 later to bring the device back online.

To set the network traffic lock:

1. Click **Administration**.
2. Click **Device Tasks**.
3. Click **Lock**.

Take note of the following scenarios:

- If the device is powered off, failopen is enabled, and network traffic lock is enabled, traffic passes through the ports
- If the device is powered on, failopen is enabled, and network traffic lock is enabled, traffic is not allowed to pass through the device

Resetting Network VirusWall Enforcer 1200

Reset Network VirusWall Enforcer 1200 if you experience any problems or if the Control Manager management console prompts you to perform a reset.

Reset Network VirusWall Enforcer 1200 through the:

- Preconfiguration console (see *page 2-23*)
- **RESET** button on the front panel of the device (see *page 2-24*)
- Web console (see *page 2-24*)

Any of the following actions invokes a device reset:

- Manually resetting the device by following one of the procedures listed in *page 2-23*
- Importing the configuration file through the Preconfiguration console or the Web console.
- Automatically or manually updating the Network VirusWall Enforcer 1200 program file (versions that require a reset) through the Web console.

If the device detects any of the above actions and failopen is in use, the device temporarily disconnects ports 1 and 2 for approximately thirty seconds (30s). See *Table 1-4* for details.

Note: The thirty-second (30s) delay only occurs when resetting the device. Powering on or off the device does not cause this delay.

To reset the device through the preconfiguration menu:

1. Access the Network VirusWall Enforcer 1200 Preconfiguration console (see *Getting Started Guide* > *Logging on to the Preconfiguration Console* for instructions).
2. Select item `6` in the main menu. The System Tasks submenu appears.
3. Select item `6` to reset the device. A confirmation screen appears.
4. Select `OK` to continue.

Note: Refer to the *Getting Started Guide* for detailed information on using the preconfiguration menu through the Preconfiguration console.

To reset the device with the Reset button:

Press the **Reset** button on the front panel of the device. Network VirusWall Enforcer 1200 resets.

To reset the device through the Web console:

1. Click **Administration**.
2. Click **Device Tasks**.
3. Click **Reset Now**.
4. Confirm the reset when prompted.

Replacing the HTTPS Certificate

Replace the HTTPS Certification from the Web console's **HTTPS Certificate** screen. Click **Replace Certificate** from **Administration > HTTPS Certificate**.

Use the following command to generate a certificate from a Linux operating system:

```
openssl req -new -x509 -days 365 -nodes -out FILE_NAME.pem -keyout
FILE_NAME.pem
```

Configuring IP Address Settings

Configure the **Management IP Address**, **Bridge IP Address**, and **Static Routes** to minimize transfer of data through an external router. Use this feature as a way to route the data directly between Network VirusWall Enforcer 1200 and network segments.

To configure the Management IP Address settings:

1. Click **Administration**. The drop down menu displays
2. Click **IP Address Settings** from the drop down menu. The **IP Address Settings** screen displays with the **Management IP Address** tab selected as default.
3. Select **Configure IP address using DHCP** or **Configure IP address manually**.
4. To bind the IP Address to a VLAN ID, select the **VLAN ID** checkbox and type a VLAN ID.
5. Click **Save**.

To configure the Bridge IP Address settings:

1. Click **Administration**. The drop down menu displays
2. Click **IP Address Settings** from the drop down menu. The **IP Address Settings** screen displays.
3. Select the **Bridge IP Address(es)** tab. The **Bridge IP Address Settings** screen displays.
4. Click **Add**. The **Add Bridge IP Address** screen displays.
5. Type the **IP address** and **Subnet mask** under **Bridge IP Settings**.
6. Select the **Port** and **VLAN ID** checkboxes under **Bound To**.
7. Click **Save**.

To configure the Static Routes settings:

1. Click **Administration**. The drop down menu displays
2. Click **IP Address Settings** from the drop down menu. The **IP Address Settings** screen displays.
3. Select the **Static Routes** tab. The **Static Routes** screen displays.
4. Click **Add**. The **Add Static Route** screen displays.
5. Type the **Network ID, Netmask,** and **Router** under **Static Route Settings**.
6. Select the **Interface** under **Bound To**.
7. Click **Save**. The **Static Routes** screen displays.

Configuring LDAP Settings

Configure LDAP settings from the Web console.

LDAP setting considerations:

- If you select Kerberos as the authentication method, ensure you fill out the KDC settings and that the device and LDAP server times match.
- If you select Simple as the authentication method, the password for Network VirusWall Enforcer 1200 and the LDAP server is not encrypted.

To configure LDAP server settings:

1. Click **Administration**. The drop down menu displays
2. Click **LDAP Settings** from the drop down menu. The **LDAP Server** screen displays.

3. Select **Use Microsoft ActiveDirectory** or **Use OpenLDAP**.
4. Select the **Authentication method**. For Microsoft ActiveDirectory, the device supports Simple and Kerberos. For OpenLDAP, the device supports Simple, Kerberos, and Digest MD5.
5. Type the **LDAP server location**. (Type an FQDN, such as www.trendmicro.com, or an IP address.)
6. Type the **LDAP server port**. (For example, 389.)
7. Type the **Base distinguished name**. (Type the DN setting, for example, dc=trend, dc=com.)
8. Type the **KDC server location**. (Type an FQDN, such as www.trendmicro.com, or an IP address.)
9. Type the **Default realm**. (For example, TREND.COM.)
10. Type the **Default domain.** (For example, trend.com.)
11. Type the **KDC server port.** (For example, 88.)
12. Click **Save**.

Configuring Proxy Settings

Configure proxy settings from the Web console for pattern and engine updates.

To configure proxy settings:

1. Click **Administration**. The drop down menu displays
2. Click **Proxy Settings** from the drop down menu. The **Proxy Settings** screen displays.
3. Select **Use a proxy server for pattern and engine updates**.
4. Select **HTTP**, **SOCKS4**, or **SOCKS5** for the **Proxy Protocol**.
5. Type the **Server name or IP address** and the **Port**.
6. Type the **User ID** and **Password** under **Proxy server authentication**.
7. Click **Save**.

Configuring SNMP Settings

Configure the SNMP settings from the Web console after downloading the MIB file and configuring your MIB browser. See *SNMP* on page 1-23 for more information about SNMP features in Network VirusWall Enforcer 1200.

To configure the SNMP settings:

1. Click **Administration**. The drop down menu displays
2. Click **SNMP Settings** from the drop down menu. The **SNMP Settings** screen displays.
3. Select the **Enable SNMP Trap** checkbox under **SNMP Trap**. If you enable the SNMP trap feature, Network VirusWall Enforcer 1200 sends an SNMP trap every 60 seconds.
4. Type the **Community name** and **Server IP address** under **SNMP Trap**.
5. Select the **Enable SNMP Agent** checkbox under **SNMP Agent**.
6. Type the **System location** and **System contact**.
7. Type a **Community name** to add under **Accepted Community Name(s)**.
8. Click **Add to**. The community name displays in the table.
9. Type the **IP Address** to add under **Trusted Network Management IP Address(es)**.
10. Click **Add to**. The IP address displays in the table.
11. Click **Save**.

To export the MIB file:

1. Click **Administration**. The drop down menu displays
2. Click **SNMP Settings** from the drop down menu. The **SNMP Settings** screen displays.
3. Click **Export MIB file**. The **Save As** screen displays.
4. Click **Save**. Specify the location and file name to the file as.
5. Click **Save**.

Using Tools

Use the **Case Diagnostic Information** from **Administration > Tools** for troubleshooting purposes. The Case Diagnostic Information feature will download all information required for use with the Case Diagnostic Tool that Trend Micro uses to debug the device.

Restoring Default Settings

If you experience any issues during configuration, you have the option of initializing Network VirusWall Enforcer 1200 through the Preconfiguration console, which restores settings to the factory defaults.

WARNING! *You will lose all changes to preconfiguration settings when you perform initialization.*

To initialize Network VirusWall Enforcer 1200:

1. In the **Main Menu**, select **System Tasks**.
2. On the System Tasks submenu, select restore default settings.

   WARNING! *Use care when restoring the default settings. Doing so erases the configurations you have set.*

3. Type y to continue.

The Network VirusWall Enforcer 1200 device will reset and restore factory defaults.

Table 2-1 lists the default settings:

SETTING	DEFAULT VALUE
Network VirusWall Enforcer 1200 host name	none
IP address type	Static
IP address	none

TABLE 2-1. Network VirusWall Enforcer 1200 default settings

SETTING	DEFAULT VALUE
Netmask	none
Default gateway	none
Primary DNS server	none
Secondary DNS server	none
Operation Mode	none
Interface speed and duplex mode	Auto

TABLE 2-1. Network VirusWall Enforcer 1200 default settings

System Recovery

You can perform pattern, engine, and system rollbacks using the Preconfiguration console.

Pattern and Engine Rollback

Perform pattern and engine rollbacks by connecting to the Preconfiguration console either using SSH or serial. From the **Main Menu** > **System Tasks** screen you have the option to perform a pattern rollback, engine rollback, reset device, or restore default settings.

System Rollback

Use a serial connection to perform a system rollback. When you reset Network VirusWall Enforcer 1200, after the "Booting the Network VirusWall Enforcer" message displays, type "ESC" for the main menu. You can select to boot the current system, previous system, or verbose mode with file checks.

Chapter 3

Updating Components

This chapter describes how to access Network VirusWall Enforcer 1200 devices from the Web console, view system information, deploy Network VirusWall Enforcer 1200 components, and modify device settings.

The topics discussed in this chapter include:

Understanding Updatable Components

Network VirusWall Enforcer 1200 uses the following components to detect, prevent or contain, and eliminate malware outbreaks:

- Network Scan Engine– scans all traffic passing through Network VirusWall Enforcer 1200 at the packet level.

  The network scan engine specifically searches for network viruses.

- Network Virus Pattern– contains a regularly updated database of packet-level network virus patterns.

  Trend Micro often updates the network virus pattern file to help ensure Network VirusWall Enforcer 1200 can identify any new network viruses.

Note: Visit http://www.trendmicro.com/download/ to view the latest Network Virus Pattern information.

- Vulnerability Engine—scans for vulnerabilities.
- Vulnerability Assessment Pattern—contains information about vulnerabilities and associated viruses.
- Damage Cleanup Engine—scans for and repairs damage caused by viruses and spyware/grayware.
- Damage Cleanup Pattern—contains information about the latest known viruses and spyware/grayware.
- Pattern Release History—contains information about antivirus product pattern version releases.
- Program file– the Network VirusWall Enforcer 1200 program, also referred to as the image, which includes the operating system, system programs, and all components necessary to get Network VirusWall Enforcer 1200 functioning properly. When you manually update the program file, Network VirusWall Enforcer 1200 prompts you to reboot the device if necessary. Otherwise, for scheduled program file updates and Control Manager program deployments, the device automatically reboots after the update.

Updating Components

Network VirusWall Enforcer 1200 components are software modules that comprise the Network VirusWall Enforcer 1200 operating system. To help ensure up-to-date protection, update the network scan engine, network virus pattern file, vulnerability and Damage Cleanup scan engine, vulnerability pattern file, Damage Cleanup pattern file, program file, and Pattern Release History after connecting to the network or during virus outbreaks.

Network VirusWall Enforcer 1200 provides the following methods to update and deploy the latest components to its managed products and devices:

- Manually

  Instruct Network VirusWall Enforcer 1200 to connect directly to the update source, download, and then apply the latest components. Use the **Manual Update** option from the Web console to set this type of update.

  Tip: Trend Micro recommends updating components manually after finishing with the Network VirusWall Enforcer 1200 preconfiguration.

- Automatically

  Instruct Network VirusWall Enforcer 1200 to automatically connect to the update source, download, and then apply the latest components. Use the **Scheduled Update** option from the Web console to set these types of update.

Note: Updating the Network VirusWall Enforcer program through Control Manager automatically causes the Network VirusWall Enforcer devices to reboot.

Updating Components Manually

After preconfiguring Network VirusWall Enforcer 1200, download the latest components (Network Virus Pattern, Cleanup templates, Network Virus Engine) to help maintain the highest security protection.

To perform a manual update:

1. Click **Updates** in the side bar. The drop down menu displays.
2. Click **Manual**. The Manual Update screen displays.
3. Select the **Component** checkbox to update all components or select checkboxes to update individual components.
4. Click **Update**.

Use the **Summary** screen from the Network VirusWall Enforcer 1200 Web console to verify whether Network VirusWall Enforcer 1200 updates the selected components during manual update.

Tip: Visit http://www.trendmicro.com/download/product.asp?productid=45 to view the latest Network Virus Pattern information.

Updating Components Automatically

Set a scheduled update to instruct Network VirusWall Enforcer 1200 to update and obtain the latest components directly from the update source. Use the **Scheduled Update** screen from the Web console to schedule update settings.

To update components automatically

1. Click **Updates** in the side bar. The drop down menu displays.
2. Click **Scheduled**. The **Scheduled Update** screen displays.
3. Select the components to automatically update.
4. Select the **Update Schedule**.

Setting the Update Source

Use the Update Settings screen to set the update source from which Network VirusWall Enforcer 1200 will obtain the latest components, including the proxy settings if your network has a proxy server to connect to the Internet.

To set the update source:

1. Click **Updates**. The drop down menu displays.
2. Click **Source**. The **Update Source** screen displays.
3. Select the **Trend Micro ActiveUpdate Server** or select **Other update source** and type the URL.
4. Click **Save**.

The Network VirusWall Enforcer 1200 Manual and Scheduled Update will obtain the latest components from the update source.

Chapter 4

Viewing Status, Logs, and Summaries

This chapter explains how to access antivirus information to evaluate your organization's virus protection policies and identify endpoints that are at a high risk of infection. Network VirusWall Enforcer 1200 logs a wide variety of information about events that occur on your network, such as endpoint infections and policy violations, virus outbreaks, and component updates.

The topics discussed in this chapter include:

Viewing Summary Information

The **Summary** screen provides an overview of network virus infections, policy violations, and existing Trend Micro antivirus component details. Click **Summary** from the main menu to view summary information. From this screen you can:

- View the **Policy Enforcement Status**.

  Click the number under **Violation** to display the **Endpoint History** log to remove endpoints from quarantine and view endpoint details.
- View the **Top 5 Policies with Violations**.
- View AV Product Detection Status

  Click **Export** to save the AV Product Detection Status to a file.
- View **Component Status**.

Viewing Real-time Status Information

The **Real-time Status** screen provides an overview of real-time device information. Click **Real-time Status** from the main menu to view real-time device information. From this screen you can:

- View the **LED Status**.

  For more information about the LEDs see *Chapter 2* in the *Getting Started Guide*.
- View the **Performance Status**.
- View the **Interface Configuration Status**.

Viewing the Pattern Release History

The Pattern Release History screen provides information on the virus pattern release history of antivirus products. Use the information on this screen to determine the pattern release version numbers for a variety of vendors. The screen displays the current version number and up to four older version numbers. This information will help you set a baseline for antivirus product version detection when creating policies.

Viewing Supported Products

The Supported Products screen provides information on the antivirus products Network VirusWall Enforcer 1200 can detect. Use the information on this screen to determine the products and versions supported by Antivirus Program Scan.

Understanding Logs

Logs provide information about the performance of managed Network VirusWall Enforcer 1200 devices. They allow you to monitor device activities and help you to troubleshoot issues.

This section provides the following information:

- Types of Network VirusWall Enforcer 1200 logs
- Configuring Log Settings

Types of Network VirusWall Enforcer 1200 Logs

Network VirusWall Enforcer 1200 generates the following log types:

- Event log
- Network Virus log
- Endpoint History

Viewing the Event Log

When the device detects an event, such as a virus outbreak, or performs an action, such as a reset or component update, it creates an event log entry. If you register the device to Control Manager, entries from this log send to the Control Manager server immediately. View the following information from the event log:

- **Module updates:** updates to the engine and virus pattern file
- **Network outbreaks:** any type of virus detection on the network
- **All events:** all events available from Web console

View the **Event Log** directly from the Web console. Click **Logs > Event Log** to view the log or export the log by clicking **Export** from the **Event Log** screen. The Event log displays the Date/Time, Severity, Event, and Description.

Viewing the Network Virus Log

When the device detects a virus or security violation, it creates a Network Virus Log entry. If you register the device to Control Manager, entries from this log send to the Control Manager server immediately.

View the Network Virus log from the Web console. Click **Logs** > **Network Virus Log** to view the log or export the log by clicking **Export** from the **Network Virus Log** screen. The Network Virus Log displays the Date/Time, IP Address, Endpoint, MAC Address Network Virus Name, Scan Action, Engine Version, and Pattern Version.

Endpoint History

When the device detects endpoints, detects violations, or quarantines a endpoint, it creates a Endpoint History entry. If you register the device to Control Manager, configure the time interval to send the Endpoint History to the Control Manager server from **Log Settings**.

View the Endpoint History from the Web console. Click **Logs** > **Endpoint History**. Select from three different lists: **Compliant**, **Violation**, and **Quarantine** or click **Export All** to save the information to a file.

Configuring Log Settings

Use log settings to send logs to a Control Manager server or syslog servers. Click **Logs > Log Settings** to configure log settings. From the log settings screen, you can:

- **Enable hostname resolution**.
- Select **Send logs to the Control Manager server** and specify the time interval in hours to send the Endpoint History log to Control Manager.
- Select **Send logs to the primary syslog server** to manage logs from a syslog application.
- Select **Send logs to the secondary syslog server** to manage logs on a backup or duplicate syslog application.

LCD Module Log Format and Interpretation

Logs displayed on the LCD console fall into the following categories:

- Asset tag error logs
- LCD module error logs

Asset Tag Logs

Asset tag logs refer to logs that record the device validity checking. When booting up or restarting (resetting) the device, Network VirusWall Enforcer 1200 checks whether the device hosting the Network VirusWall Enforcer 1200 software components are valid. An invalid casing or hardware component results to an asset tag log.

An asset tag log has the following format:

```
[Error #]
Invalid device
```

Where `#` indicates the error code and `Invalid device` indicates that a Network VirusWall software or hardware component is mounted on an invalid platform.

Table 4-1 enumerates all possible asset tag logs:

ERROR CODE	DESCRIPTION
0	Invalid asset tag.
-1	**Action**: Issue GET_FRU_INFO command GET_FRU_INFO is the function that obtains the Field Replaceable Unit. FRU is the component responsible for the actual device information. **Result**: The response data length does not match or the completion code is incorrect
-2	FRU size is equal to 0. The FRU size should not be equal to 0.
-3	**Action**: Issue GET_FRU_DATA command **Result**: The response data length does not match or the completion code is incorrect
-4	The FRU header version is not equal to 1. The FRU header version should be equal to 1.
-6	Missing product offset.

TABLE 4-1. Asset tag logs

Having any of the above error codes can only mean that someone has tampered with the device. Someone has altered or replaced the original components included with shipment of the product. The error codes help listed above help Trend Micro engineers to troubleshoot and pinpoint the exact device issue.

Using the Log Viewer

Network VirusWall Enforcer 1200 System Log Viewer (Network VirusWall Enforcer 1200 System Log Viewer) is a user-friendly, stand-alone application that displays system debug log information in real-time as Network VirusWall Enforcer 1200 creates log entries. Use the System Log Viewer to view system debug log entries and save them to a text file.

System logs contain information useful for troubleshooting. If you experience problems with Network VirusWall Enforcer 1200 and contact Trend Micro support, you may be asked to view the system log.

Chapter 5

Troubleshooting and FAQs

This chapter addresses troubleshooting issues that may arise and answers frequently asked questions.

The topics discussed in this chapter include:

Using Network VirusWall Enforcer 1200 Utilities

Network VirusWall Enforcer 1200 provides the Appliance Firmware Flash Utility to update the device BIOS, LCM, and program file (flash the DOM). The utility is a graphical user interface tool that provides a user-friendly method of uploading the latest program file and boot loader. The utility is included on the *Trend Micro Solutions CD for Network VirusWall Enforcer 1200*.

See the following sections for instructions on how to run the Network VirusWall Enforcer 1200 utilities:

- Uploading the latest program file (firmware) and boot loader, see *page 5-3*

Entering Rescue Mode

If you are experiencing problems that prohibit the normal functioning of Network VirusWall Enforcer 1200, enter rescue mode to upload the program file or boot file. While in rescue mode, Network VirusWall Enforcer 1200 has a default static IP address. See *Table 5-1* for a summary of rescue mode settings.

WARNING! *Use rescue mode for troubleshooting only.Under normal circumstances, you do not need to enter rescue mode.*

RESCUE MODE SETTING	VALUE
Network VirusWall Enforcer 1200 host name	Blank
IP address type	Reset
IP address	192.168.252.1
Netmask:	255.255.255.0
Default gateway	192.168.252.254
DNS server 1	Blank
DNS server 2	Blank

TABLE 5-1. Rescue mode settings

Note: Appliance Firmware Flash Utility will hang and will not function if any of these settings is not set. Use the Windows **Task Manager** to close the non-responsive utility.

Enter rescue mode through the:

- LCD module
- Preconfiguration console

To enter rescue mode with the LCD module panel:

1. Reset Network VirusWall Enforcer 1200 by pressing the **RESET** button. When the device resets, a message appears on the LCD display prompting you to enter rescue mode.
2. Press the **Enter** button. A message appears on the LCD display showing that the device is in rescue mode.

To enter rescue mode through the Preconfiguration console:

1. Select **Reset Device** from **System Tasks**.
2. When the device resets, a message appears prompting you to enter rescue mode.
3. Type `r` at the prompt. The Network VirusWall Enforcer 1200 rescue mode settings appear.

Note: To exit rescue mode at any time, reset Network VirusWall Enforcer 1200 by pressing the **RESET** button on the front panel. Ensure that the computer you use to perform the upgrade has an IP address in the 192.168.252.2 to 192.168.252.253 range and a netmask of 255.255.255.0.

Uploading the Program File and Boot Loader

The Network VirusWall Enforcer 1200 program file (firmware) contains all the components necessary to prepare Network VirusWall Enforcer 1200 devices for preconfiguration. This includes the operating system, network scan engine, network virus pattern file, and system programs.

Note: Uploading the program file will restore the Network VirusWall Enforcer 1200 default factory settings.

To preserve the existing settings, back up the Network VirusWall Enforcer 1200 configuration using the **System Tasks** > **Export Configuration File** option. After uploading the new or default program file, reconfigure the device settings through the Preconfiguration console > **Device Settings** menu or import the original configuration using the **System Tasks** > **Import Configuration File** option.

Note: After new firmware deploys to Network VirusWall Enforcer 1200, the device will automatically reboot.

The program file name is as follows:

`NVW_image.x.yy.zzzz.en_US.R`

Where:

- **`x`** is the major version
- **`yy`** is the minor version
- **`zzzz`** is the build number
- **`en_US`** is the program language version
- **`R`** denotes the nature of the file (that is, the Network VirusWall Enforcer 1200 program file)

The boot loader contains information necessary for the Network VirusWall Enforcer 1200 operating system to function. The boot loader file name is as follows:

`NVW_image.x.yy.zzzz.en_US.B`

Where:

- **`x`** is the major version
- **`yy`** is the minor version
- **`zzzz`** is the build number
- **`en_US`** is the program language version
- **`B`** denotes the nature of the file (that is, the Network VirusWall Enforcer 1200 boot loader file)

You can obtain these files from the following locations:

- **Trend Micro download Web site**—contains the most up-to-date versions (`http://www.trendmicro.com/download`)

- **Trend Micro Solutions CD for Network VirusWall Enforcer 1200**—the included CD contains the program file with factory defaults and the original boot loader. These files are located in the following path (replace D: with the path used by your CD-ROM drive):

  D:\Programs\NVW_Rescue

Troubleshooting

The section covers the following troubleshooting topics:

Hardware Issues

#	ISSUE	CORRECTIVE ACTION
1	LEDs do not illuminate	Verify secure power cable and network cable connections (see *Network VirusWall Enforcer 1200 Getting Started Guide* for more information). If the error persists, there may be a hardware problem. Contact your vendor.
2	Unable to access the Preconfiguration console	Verify secure console port connections and terminal communications software settings (refer to the *Getting Started Guide* > *Preconfiguring Network VirusWall Enforcer 1200 Using the Preconfiguration Console*).
3	Unable to change settings with the LCD module panel	To change settings with the LCD module panel, you must first press and hold down the <ENTER> button . If a problem with any LCD module buttons persist, there may be a hardware problem. Contact your vendor.

TABLE 5-2. Troubleshooting Network VirusWall Enforcer 1200 hardware issues

Configuration Issues

#	ISSUE	CORRECTIVE ACTION
Issues with Trend Micro Control Manager		
1	Network VirusWall Enforcer 1200 is unable to register with the Control Manager server	Check all network connections and ensure you have correctly performed preconfiguration (refer to the *Getting Started Guide* > *Preconfiguring Network VirusWall Enforcer 1200* section for more information). Network VirusWall Enforcer 1200 only registers to Control Manager 3.5 through port 443. If Control Manager is installed on Windows 2003, configure the firewall to allow port 443 to communicate with Network VirusWall Enforcer 1200. If the OS on which Control Manager 3.5 resides is Windows Server 2003, Network VirusWall Enforcer 1200 may not be able to use the Control Manager time service to synchronize with the server and will therefore be unable to register to the Control Manager service. **To remedy this problem, choose one of the following:** 1. Install Active Directory on the Windows Server 2003 server so Network VirusWall Enforcer 1200 can synchronize with the Windows Server 2003 time service. 2. Disable the Windows Server 2003 time service and enable **Trend Micro Network Time Protocol** so Network VirusWall Enforcer 1200 can synchronize with the Control Manager server time service. OR Check to ensure that ports 80 and 443 are enabled in Control Manager's IIS settings. OR If there are multiple IP addresses bound to the Control Manager server's network card, Network VirusWall Enforcer 1200 may not register to Control Manager successfully using FQDN. To resolve this issue, configure only one IP address per network card.
2	Network VirusWall Enforcer 1200 displays a **sync time** error and is unable to register to Control Manager server	A sync time error displays when Network VirusWall Enforcer 1200 is unable to synchronize with the Control Manager server. **To remedy this problem, do the following:** On the Web console **Administration** > **Time Settings** screen, select Use a NTP server to update the time.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
3	The Network VirusWall Enforcer 1200 icon on the Control Manager management console appears as active even when the device is offline	When Network VirusWall Enforcer 1200 is turned off, or is disconnected from the network, the Control Manager agent for Network VirusWall Enforcer 1200 is not given the opportunity to inform Control Manager that it is going offline. As a result, it relies on Control Manager's status verification mechanism to update its operating status. If the default heartbeat settings are used, Control Manager may require up to 180 minutes updating the status. The actual time would depend on when Network VirusWall Enforcer 1200 sent its last heartbeat. See the *Control Manager Getting Started Guide* and online help for information on changing Heartbeat settings.
4	The icon and user name for a Network VirusWall Enforcer 1200 device that was removed from the network still appears on Control Manager	Access the product directory on the Control Manager management console. Remove the Network VirusWall Enforcer 1200 device (see the *Control Manager Getting Started Guide* and online help for information on adding and removing products).
5	Network VirusWall Enforcer 1200 does not register to Control Manager even when Network VirusWall Enforcer 1200 and Control Manager belong to the same subnet and the Control Manager firewall is disabled.	Check the Control Manager's IIS server to ensure that it allows communication on port 443 (HTTPS).
6	Network VirusWall Enforcer is unable to register to Trend Micro Control Manager using FQDN.	Verify whether the FQDN is able to connect to the Control Manager server from a local computer. For example, instead of typing https://IPAddress/controlmanager, type https://fully.qualify.domain.name/controlmanager. If you are unable to connect to Control Manager, please change the Control Manager configuration to allow the connection. Network VirusWall Enforcer 1200 can only register to Control Manager if DNS is able to find the correct path to the Control Manager server.
Issues with quarantining and blocking endpoints		

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
7	Network VirusWall Enforcer 1200 is not quarantining endpoints whose packets are infected	Check the Policy Enforcement Service configuration from **Policy Enforcement > Policies**. Click on the Policy that includes settings that quarantines endpoints with infected packets. Network VirusWall Enforcer 1200 quarantines a maximum of 1024 endpoints and drops all network traffic from additional endpoints (over 1024) whose packets are infected. Reconsider your deployment plan to take into consideration the number of endpoints in your network.
8	An endpoint that was blocked because it does not have the latest Windows patch remains blocked even after running Windows Update	Connect to "Microsoft Security Bulletin Search" (http://www.microsoft.com/technet/security/current.aspx) and search for the vulnerability name (for example, MS01-059) shown in the blocking page. Download that specific patch and install it on the blocked endpoint.
9	No page (or a blank page) displays when endpoint tries to access Windows Update	Try to refresh the current page, or close it and reconnect to the Windows Update site. If doing so still does not solve the problem, use another computer and connect to http://support.microsoft.com and search for your problem.
Issues with policy enforcement		
10	A pending screen occasionally interrupts Windows or Office updates, forcing the update to begin again	On the **Policy Enforcement** > **Endpoint Notifications > Settings** screen, clear the **Enable the detecting page** checkbox**.**
11	Network VirusWall Enforcer 1200 Policy Enforcement does not correctly identify incompliant endpoints	An HTTP proxy server located between Network VirusWall Enforcer 1200 and endpoints on the network may prevent Network VirusWall Enforcer 1200 from correctly identify endpoint status. Reconsider your deployment plan to take into consideration proxy servers on the network. **Note:** If a SYN flood attack with fake source IP address occurs on your network, Network VirusWall Enforcer 1200 Policy Enforcement may not be able to detect the status of endpoints on the network.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
12	Network VirusWall Enforcer 1200 is unable to implement Outbreak Prevention Policies to block endpoint ports	If an endpoint routes its traffic through a proxy server, the machine actually sends packets to the proxy using a proxy port; the proxy is responsible for actual packet delivery. Unless the proxy itself is within the network, Network VirusWall Enforcer 1200 does not block the endpoint traffic.
13	When Kerberos Authentication is used, the User Authentication does not function as expected	Check the clock sync between the authentication server and Network VirusWall Enforcer 1200. The authentication server and Network VirusWall Enforcer 1200 should have the same time setting. For Kerberos and MD5 authentication, users only need to input account information (without the domain) and password.
14	Why doesn't the endpoint detection page update	When there is a PEAgent update that downloads with a program file update, Network VirusWall Enforcer 1200 stops all services before installing the new PEAgent. However, Network VirusWall Enforcer 1200 cannot stop Real-time scan which causes the detection page to freeze. Restart the endpoint computer to solve this problem.
15	An endpoint in a different subnet than Network VirusWall Enforcer does not pass user authentication	Add a bridge IP address that is in the same subnet as the endpoint and bind it to a port.
16	Network VirusWall Enforcer cannot update the endpoint status using the PEAgent	Add a bridge IP address that is in the same subnet as the endpoint and bind it to a port.
17	Windows 98 users cannot pass user authentication	Older versions of Internet Explorer do not support secure connections. Upgrade the endpoint's Internet Explorer to allow a secure connection.
18	An error displays about not being able to run ActiveX when the endpoint tries to access the Internet	Please locate the %windir%\PEAgent folder and remove the PEAgentSFX.exe file on the endpoint computer.
19	The detecting page displays while OfficeScan or PC-cillin scans the endpoint and does not continue to the next page	If the real-time scan feature is enabled for OfficeScan or PC-cillin, Network VirusWall Enforcer waits for the scan to complete before continuing.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
Other issues		
20	Endpoints are unable to access the update source for component updates	If there is a proxy server on your network, ensure that your proxy settings are correct. If you want quarantined or blocked endpoints to access the update source, add the IP address of the update source to the URL Exception List.
21	Network VirusWall Enforcer 1200 is either unable to obtain, or gets incorrect, DNS server information	This occurs if the DHCP server that assigns the Network VirusWall Enforcer 1200 IP address does not specify a DNS server. Confirm your network DHCP and DNS server settings are correct (see *Configuring Device and System Settings* on page 2-19).
22	Third-party vulnerability scanners are not detecting certain vulnerabilities	Network VirusWall Enforcer is not compatible with some vulnerability scanners and may render them unable to detect NIMDA-related vulnerabilities. Tentatively disable Real-time network virus scan or set the scan option to pass while other vulnerability scanners on your network are performing vulnerability scans.
23	Exporting the configuration file displays garbage characters	This is a known issue. The garbage characters do not cause any adverse effects on the exported configuration file.
24	When a NAT device resides between Control Manager server and BRI port of the device, if the device uses dynamic IP address to register to Control Manager, the network administrator may need to change port forwarding settings each time	Set Network VirusWall Enforcer 1200 by static IP address.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
25	User cannot see popup messages on a Windows XP SP2 endpoint	There are two possible causes: 1. By default in Windows XP SP2 the "Messenger" service is disabled. To resolve the problem, enable the "Messenger" service. 2. The necessary ports in the Windows Firewall Exceptions list may be disabled. Network VirusWall Enforcer 1200 uses ports TPC 139 and UDP 137 to deliver popup messages through Windows Messenger. In Windows XP SP2 by default the firewall is enabled. However, if at any point a user clicks **Restore Defaults**, the necessary Exceptions ports become disabled. **To re-enable the necessary ports:** a. Go to **Windows Security Center** > **Windows Firewall** > **Exceptions** > **File and Printer Sharing**. b. Check to see if "TCP 139 Port" and "UDP 137 Port " are selected in the Windows Firewall Exceptions. If these ports are not selected, select them now. c. Click **Save** to save your change.
26	The root domain controller cannot be deployed unless two registry keys are modified in Windows	The root domain controller (Active Directory Server) cannot deploy unless two registry keys are modified in Windows. Modify the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\lanmanserver\parameters value enablesecuritysignature to 0 requiresecuritysignature to 0
27	HyperTerminal is not working with the device	Configure the terminal console emulation to VT100 and the terminal ID to VT102.
28	The authentication feature not working as expected	If the LDAP host name cannot be resolved, then authentication will fail. Set the DNS from the Web console to allow the host name of the LDAP server to be resolved.
29	Unable to ping Network VirusWall Enforcer 1200	If you make changes such as disabling a port, installing a new fiber card, or specifying a new port type, you will need to clear the ARP table first. Use the "arp -d" command to clear the table and try again.
30	The device is not functioning as expected after changing the port speed to 100 Mbps Full	When the speed is changed from Auto to 100 Mbps, auto MDI-X is disabled. If your switch does not support Auto MDI-X, a crossover cable is required to connect to the device.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

#	ISSUE	CORRECTIVE ACTION
31	Why can't I access the Web console after changing the Management IP address	The Management IP address and Bridge IP addresses cannot be the same. If you have recently changed the Management IP address, change the Management IP address from the Preconfiguration console using HyperTerminal.
32	Unable to perform schedule update correctly	Ensure that the scheduled update configurations for updating pattern release history and other pattern/engines are not set to update at the same time.
33	Unable to see blocking page when the endpoint and Network VirusWall Enforcer 1200 are in different subnets	Do one of the following: 1. Configure a Bridge IP address with the same subnet as the endpoint IP address. This is for endpoints that cannot connect to it's default gateway. 2. If the endpoint can reach it's default gateway without going through Network VirusWall Enforcer, configure a Static Route to allow Network VirusWall Enforcer to establish a correct network path to connect to the endpoint.
34	Automatically logged off the preconfiguration console	If you change the current window size, Network VirusWall Enforcer 1200 automatically logs off.
35	Unable to download Pattern File History using DNS	Try to use a different DNS server.
36	Unable to upgrade from Network VirusWall 1200 to Network VirusWall Enforcer 1200	This version of Network VirusWall Enforcer 1200 does not support a direct upgrade. The release build cannot be used for upgrading the device from previous versions to 2.0.
37	Why does the endpoint browser display "Page not found" after Network VirusWall Enforcer 1200 performs an assessment of the endpoint?	If you use a proxy script in your network, Network VirusWall Enforcer 1200 may prevent the proxy script from downloading to the endpoint during endpoint assessment. Close the endpoint browser and open the endpoint browser again to access the Internet after the assessment. To prevent this issue, add the proxy script to the Network Zone Exceptions list. **Note:** If you add a proxy server to the Global Endpoint Exceptions list, Network VirusWall Enforcer 1200 does not assess endpoints that use that proxy server.

TABLE 5-3. Troubleshooting Network VirusWall Enforcer 1200 configuration issues

Control Manager and Network VirusWall Enforcer 1200 Communication Issues

Tip: Refer to the *Getting Started Guide* > *Control Manager and Network VirusWall Enforcer 1200 Integration* for additional information.

When troubleshooting the Control Manager and Network VirusWall Enforcer 1200 integration and communication:

- Check the Network Time Protocol (NTP) used (see *page 5-15*)

Check if Network Time Protocol (NTP) is in Use

Windows Network Time Protocol (NTP) and Control Manager NTP are both time servers. Windows NTP may provide some other features for Active Directory Server (ADS) endpoints. In addition, Windows NTP does not work unless you have installed ADS.

To enable NTP:

From the Web console, on the **Administration** > **Time Settings** screen, select **Use a NTP server to update the time**.

Frequently Asked Questions (FAQs)

This section answers the following common questions about Network VirusWall Enforcer 1200:

Where does Network VirusWall Enforcer 1200 store its logs, and how can I access them?

Network VirusWall Enforcer 1200 only uses a 128 MB IDE Disk On Module (DOM) flash disk for storage. Consequently, it does not have memory space available to store log files; Event and Network Virus Logs. Network VirusWall Enforcer 1200 sends its logs to the Control Manager server. Alternatively, Network VirusWall Enforcer 1200 can send system logs (which also include debug information) to any computer on the network with a Syslog Server. See *Configuring Device and System Settings* on page 2-19 and *Understanding Logs* on page 4-3 for more information.

Can the length of the network cable affect the failopen functionality of Network VirusWall Enforcer 1200?

Yes, the network cable connecting Network VirusWall Enforcer 1200 and other devices must not be longer than 100 meters (328 feet). Otherwise, Network VirusWall Enforcer 1200 failopen will not work.

Can I configure the time interval for Logs?

For this version of Network VirusWall Enforcer 1200, you cannot configure the time interval for both Event logs and Network Virus logs.

Can I register a Network VirusWall Enforcer 1200 device to more than one Control Manager server?

No, you cannot register a device to more than one Control Manager server. To register a device to a Control Manager server through the Network VirusWall Enforcer 1200 Preconfiguration **Device Settings** option.

Does Network VirusWall Enforcer 1200 support spanning tree protocol (STP)?

No, Network VirusWall Enforcer 1200 does not support STP. However, Network VirusWall Enforcer 1200 does not affect STP that switches use.

Will modifying the duplex settings from half-duplex to full-duplex have any adverse effect on Network VirusWall Enforcer 1200?

Modifying the interface speed and duplex mode setting from the Preconfiguration console causes Network VirusWall Enforcer 1200 to refresh its settings and perform a network refresh. During this time, the network connection is disconnected for a short time.

Will changing the Network VirusWall Enforcer 1200 IP address prevent it from communicating with the Control Manager server?

Yes, changing the Network VirusWall Enforcer 1200 IP address through the Preconfiguration console Device Settings menu will temporary disconnect (30 seconds) the Network VirusWall Enforcer 1200. During the time the MCP agent is disconnected from Control Manager, the MCP agent logs off from Control Manager and then logs in and provides Control Manager with the updated information.

Can I perform extensive Network VirusWall Enforcer 1200 configuration settings locally through the Network VirusWall Enforcer 1200 front panel?

No, you cannot perform extensive configuration settings using the device itself.

The Network VirusWall Enforcer 1200 front panel interface only allows you to configure the **Device Settings**, view System Information and hardware logs, and reset the device. In addition, the front panel interface has a serial port that allows you to complete the preconfiguration tasks.

To perform extensive configuration changes, use the Web console.

See *Table 1-1* for a comparison of the available Network VirusWall Enforcer 1200 management tools.

How can I back up the Network VirusWall Enforcer 1200 configuration before modifying the firmware?

Use the Preconfiguration console **System Tasks** > **Export Configuration File** option to back up the Network VirusWall Enforcer 1200 configuration. In addition, the Preconfiguration console **System Tasks** > **Import Configuration File** option allows you to import settings from an identical Network VirusWall Enforcer 1200 devices.

You can also perform this procedure from the Network VirusWall Enforcer 1200 Web console from **Administration > Backup Configuration**.

Why is it that I cannot find any preconfiguration information in the Administrator's Guide?

This Administrator's Guide includes instructions and details that you will need when configuring and administering a device from the available management tools. For preconfiguration instructions, please refer to the printed or PDF *Getting Started Guide*.

Does Network VirusWall Enforcer 1200 bridge all non-IP address traffic?

Yes, Network VirusWall Enforcer 1200 bridges all non-IP address traffic.

Can I import and export the Network VirusWall Enforcer 1200 configuration?

Yes, the Network VirusWall Enforcer 1200 Preconfiguration console > **System Tasks** option allows you to import and export the Network VirusWall Enforcer 1200 configuration when accessed through a HyperTerminal session. However, importing or exporting the Network VirusWall Enforcer 1200 configuration is not possible when using Minicom (available in Linux servers).

Note: Export configuration files only for backup purposes. This feature is not intended for copying the configuration of one Network VirusWall Enforcer 1200 device to another.

Does the Remote login, ActiveX feature support use with Windows 95, 98, and ME?

The device only supports ActiveX, but not remote login, for Windows 98 and ME. For Windows 95, the device does not support remote login or ActiveX.

Does the Remote login, ActiveX feature support use with endpoints who are behind NAT?

Network VirusWall Enforcer 1200 does not support Remote login, ActiveX for endpoints behind NAT.

How can I pass Windows Active Directory Simple authentication?

Configure the User ID as a full UPN (user principle name) such as account@realm or domain\account. When logging in provide the correct UPN and password.

Why does the agent not install to an endpoint successfully?

Network VirusWall does not support installation of agents to Windows 95 and NT4.

Can blocked files be transferred?

FTP and HTTP blocked files can be transferred again when Network VirusWall Enforcer 1200 drops the connection after time-out. (10 minutes.)

Why does HTTPS traffic not redirect to the block page?

This version of the device does not support decryption of encrypted HTTPS traffic.

Will the installed agent that has been removed from Task Manager in Windows 2003 be reinstalled?

If the endpoint matches a policy, then the agent will reinstall. Otherwise, the endpoint will not have an agent installed.

Will Network VirusWall Enforcer 1200 block activities with SOCKS4 and SOCKS5?

This version of the device does not block IM activities with socks4 and socks5.

Can I type a DBCS URL link as the Redirect URL or Exception URL?

This version of the device does not support DBCS URL links.

Why doesn't the Remote Login, ActiveX for endpoint installation feature not work?

Check for the following:

- If the endpoint has a Windows 98, ME, or XP Home, remote login is not supported.
- In Windows XP Professional, endpoint users need to disable simple files sharing by deselecting "Simple files sharing" in Option > View.
- Endpoint firewall settings must be disabled for remote login installation.
- Ensure the endpoint user account has administrator privileges and that ActiveX controls can be downloaded.

How many sessions can there be for HTTP, HTTPS, and SSH management consoles?

HTTP and HTTPS each can have 10 concurrent sessions and SSH can have an unlimited number of concurrent sessions.

Does the device block uploading to HTTP?

This version of the device does not support this feature.

Why was I logged out of the remote terminal console?

If you change the current window size, the device automatically logs you out.

Why is MSN blocked?

If the HTTP file blocking settings matches gateway.dll, MSN will be blocked also. Avoid using *.dll when specifying files to block.

Why is there a login screen when I am completing the Registry Key scan configuration?

This means you have timed out of the session and will need to login.

Where are non-Windows and Unknown OS endpoints displayed?

They are included in the violation count.

Does IM management support LCS?

This version of the device does not support LCS.

Can I create a new account to access the Preconfiguration console?

The `admin` and `poweruser` accounts are the predefined Preconfiguration console accounts. Administrator accounts allows full access of the Preconfiguration console. Alternatively, Power User accounts allows you to read the current settings in the Preconfiguration console menus.

Manage accounts from the Network VirusWall Enforcer 1200 Web console. New accounts can only be added using the Web console. You can create Administrator, Power User, and Operator Accounts.

How many domains does Network VirusWall Enforcer 1200 support for user authentication?

In this release, Network VirusWall Enforcer 1200 supports one domain for user authentication.

Why doesn't simple authentication for an OpenLDAP work?

Ensure that the DNS server can map the OpenLDAP server IP address and host name. For a DN, please type the full path in the Base Distinguished Name field. (For example, ou = sales, dc = trend, dc = com.)

Why does the ICQ status change to offline on endpoint computers?

If you select IM Management and select to assess ICQ file transfer activity with a drop or reject action, the ICQ status on endpoints changes to offline if the endpoint sends a file through ICQ.

Does Network VirusWall Enforcer support file blocking for the shared folder MSN 8.0?

No, Network VirusWall Enforcer does not support file blocking for the shared folder in MSN 8.0.

What happens if there is more than one antivirus application on the endpoint?

Network VirusWall detects the first antivirus application in a list of supported products that are sorted in ascending alphabetical order by product name.

Why can't I upgrade the device?

If you are upgrading from version 1.x to 2.0, please ensure that you upgrade the boot loader (.B file) first. For detailed information, please refer to Network VirusWall Enforcer 1200 Upgrade Guide.

Does the Antivirus Program Scan feature support non-English applications for endpoint computers with Windows 9x operating systems?

The **Antivirus Program Scan** feature only supports English applications for endpoint computers with Windows 9x operating systems.

Does Network VirusWall Enforcer 1200 support Antivirus Program Scan for Kaspersky Chinese version 5.0.388?

Please refer to the Supported Products list on the Web console for the latest information.

Does Network VirusWall Enforcer 1200 support Antivirus Program Scan for Trend Micro ServerProtect™ 5.58?

This version of Network VirusWall Enforcer 1200 supports Antivirus Program Scan for Trend Micro ServerProtect 5.58 English version. **Enable Assess Trend Micro products only by using networking protocols** to detect multiple language versions of ServerProtect.

Does Network VirusWall Enforcer support Windows endpoint notification for endpoints with host names in Chinese?

This version of Network VirusWall Enforcer 1200 does not support Windows endpoint notification for endpoints with host names in Chinese.

Why does the pop-up window display the Network VirusWall Enforcer logon screen?

After 10 minutes of inactivity, Network VirusWall Enforcer 1200 logs out the inactive session.

I have just installed Network VirusWall Enforcer 1200, why can't I access the Web console?

If you are using Windows 2003 Internet Explorer, default settings on the browser require you to add the Network VirusWall Enforcer 1200 IP address to the trusted sites list for access.

For system other than 2003, please make sure the network is connected between Network VirusWall Enforcer 1200 and the endpoint, and also verify that under Preconfiguration Console -> Advance Settings, Web console is enabled.

Why do log entry times from Network VirusWall Enforcer 1200 differ from log entry times from the kernel?

You can change the time setting for Network VirusWall Enforcer 1200, but you cannot change the kernel time setting.

Why do I receive the "Same IP and Port pairs" message when I configure Log Settings?

You cannot specify the same IP address and port pair for both primary and secondary Syslog server settings.

Does Network VirusWall Enforcer 1200 FTP file assessment support double byte characters?

The FTP file assessment feature in Network VirusWall Enforcer does not support double byte characters.

How does Network VirusWall Enforcer 1200 handle FTP transfers when I configure specific ports to assess?

When you assess and block specific ports, the FTP connection and download may not be successful. Initial communication goes through port 21 to the FTP server. However, since the download goes through port 20, the connection may match two different policies and never complete.

What are the configuration file names?

The configuration file from the Web console exports to "CONF-2_00_XXXX.EXPORT" and the configuration file from the Preconfiguration console exports to "conf-2[1].00.XXXX". Where XXXX is the version number.

Is the Current connections item on the Real-time Status screen updated after disabling Network Virus Scan from the Web console?

No, the sessions count is not cleared after you disable Network Virus Scan.

What happens to exception hosts when I import a Network VirusWall 1200 1.3 configuration file to Network VirusWall Enforcer 1200 2.0?

All groups are converted to **Network Zones** in Network VirusWall Enforcer 1200 for greater flexibility.

Why does an Internal Error message display instead of the Summary screen?

When Network VirusWall Enforcer blocks over 1000 endpoints simultaneously, the **Summary** screen does not display.

Does Network VirusWall Enforcer 1200 support Windows™ Vista™?

No, this version of Network VirusWall Enforcer 1200 does not support Windows Vista.

Why can't I deploy the PEAgent to Windows Server 2003 R2 endpoints?

The default Internet Explorer security settings prevent deployment. Please change the security settings on the endpoint's Internet Explorer to enable Java Script, Signed ActiveX download/execute.

Why are there multiple copies of the same policy in the policy list?

If you select a policy and click **Copy** multiple times, multiple copies of that policy are added to the list.

What may prevent successful deployment of PEAgent?

The following will prevent successful deployment of PEAgent:

- If Network VirusWall Enforcer 1200 and the endpoint do not belong to the same network segment.
- The traffic from the endpoint goes to directly to a router after passing through the device.

Why did my session terminate while downloading the Case Diagnostic Information?

When multiple requests to download the Case Diagnostic Information, the first session terminates when the second session begins the download. No error message displays.

Why does the screen only display the login screen in the lower right section of the page?

If you click the lower right section of the screen after some idle time, the login screen only displays in the lower right section of the page. Click the left panel to refresh the screen.

Can I redirect traffic to another port?

Yes, if you use the Redirect to URL feature. For example, "http://x.x.x.x:1234" as the URL to redirect HTTP traffic to port 1234.

Can Network VirusWall Enforcer 1200 devices be connected or stacked together to improve throughput?

Network VirusWall Enforcer devices are designed for parallel connections, not serial connections. Thus, they cannot be connected together to improve throughput.

Can Network VirusWall Enforcer 1200 be considered a repeater in the network?

No, Network VirusWall Enforcer 1200 does not amplify signals or packets.

How many types of agents are running on my workstation when authentication policy applies?

Currently there will be two types of agents running on your workstation, and the agent deployed depends on the authentication policy combination you configured in a policy.

- Persistent Agent = Persistent agent + authentication
- Temp Agent = Agentless agent (one time agent) + authentication (valid until log out/reboot)
- Temp Agent = No agent + authentication (valid until log out/reboot)

I typed the wrong the username or password three times when logging in to the Preconfiguration console. Then I could not log on to the console. What should I do?

If the wrong username or password are used three times in a row, the system will lock for 30 seconds before the user can try to log on again. Wait 30 seconds and try to log on again if this happens.

Why are some files not being blocked?

If a the first or last character in a file's name is a space the file cannot be properly assessed. For example, " test.exe".

Why is the status of port 3 not consistent with the configuration?

This will occur when configuring port 3 to DIS, while the port 3 is still up and running. Because Port 3 was configured as the Management port before changing the configuration to DIS and the Management port was not set to bridge after configuring port 3 to DIS.

Chapter 6

Getting Support

Trend Micro is committed to providing service and support that exceeds our user's expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try to find a solution to your problem:

- **Check your documentation**– the Administrator's Guide, Getting Started Guide, and Online Help provide comprehensive information about Network VirusWall Enforcer 1200. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site**– our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit

  `http://esupport.trendmicro.com`

Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- Email support

  `support@trendmicro.com`

- Help database- configuring the product and parameter-specific tips
- Readme- late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base- technical information procedures provided by the Support team:

  `http://esupport.trendmicro.com`

- Product updates and patches

  `http://www.trendmicro.com/download/`

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- Network VirusWall Enforcer 1200 model and image (firmware) version (if possible)
- Interface speed and duplex mode setting
- Exact text of the error message, if any
- Steps to reproduce the problem

Sending Infected Files to Trend Micro

You can send viruses, infected files, Trojan horse programs, and other malware to Trend Micro. More specifically, if you have a file that you think is some kind of malware but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following Web address:
`subwiz.trendmicro.com`

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any viruses it may contain and return the cleaned file to you within 48 hours.

Introducing TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of hundreds of engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Lake Forest, CA, ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 — one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

```
http://www.trendmicro.com/en/security/trendlabs/overview.htm
```

Other Useful Resources

Trend Micro offers a endpoint of services via its Web site, www.trendmicro.com.

Internet-based tools and services include:

- Virus Map—monitors virus incidents around the world
- HouseCall™ — Trend Micro online virus scanner
- Virus risk assessment—the Trend Micro online virus protection assessment program for corporate networks

Appendix A

Device Specifications

This appendix provides general system and hardware specifications for Network VirusWall Enforcer 1200.

Physical	
Height	1.75" (44.4mm)
Depth	12.6" (320.5mm)
Width	16.8" (426mm)
Weight	9.9 lbs. (4.5Kg)
Processor system	
CPU	Intel Celeron 1.2 GHz, 256KB L2 cache
Chipset	Intel 815E
BIOS	Award 4 Mb Flash
Bus	
PCI	32-bit/33MHz
Memory	
Technology	PC-133 SDRAM

TABLE 1-1. Network VirusWall Enforcer 1200 device specifications

Max. Capacity	256 MB	
Socket	144-pin SO-DIMM	
Ethernet		
Interface	10/100 Base-TX (3 ports)	
Controller	Intel 82562ETx1 i82559ERx2	
Connector	RJ-45 x3	
Fail-Over	Ethernet bypass support	
Cooling		
Blower	1 (3CFM), 1 (4 CFM)	
Management		
Serial connection	RS-232 x1	
Power Adaptor	**Input**	**Output**
	AT PS, AC voltage: 90 ~ 264V @ 47 ~ 63 Hz, full range	180 W
Environmental	**Operating condition**	**Non-operating**
Temperature	32 ~ 104°F (0° ~ 40°C)	-4 ~ 167°F (-20° ~ 75°C)
Humidity	5 ~ 85% @ 104°F (40°C)	5 ~ 95%
Performance		
Maximum throughput	180 Mbps	
Maximum concurrent connections	68,000 connections	

TABLE 1-1. Network VirusWall Enforcer 1200 device specifications

Appendix B

Introducing Trend Micro Control Manager™

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter discusses the following topics:

Control Manager Basic Features

Control Manager is designed to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

FEATURE	DESCRIPTION
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console This helps ensure consistent enforcement of your organization's virus and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure management console access and component download
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage via user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control Network VirusWall Enforcer 2500 devices in real-time. Control Manager immediately sends configuration modifications made on the management console to the Network VirusWall Enforcer 2500 devices. System administrators can run manual scans from the management console. This command system is indispensable during a virus outbreak.

TABLE B-1. Control Manager Features

FEATURE	DESCRIPTION
Centralized update control	Update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

TABLE B-1. Control Manager Features

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with Network VirusWall Enforcer 1200 devices. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

XML parsing requires more system resources compared to the other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).

The agent footprint required to transfer information is much larger in XML compared with other data formats.

Data processing performance is slower due to the larger data footprint.

Packet transmissions take longer and the transmission rate is less than other data formats.

With the issues mentioned above, MCP's data format is devised to resolve these issues. The MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility is also been considered since each item is composed of name ID, type, length and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with/or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IPs on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when agent sits behinds a NAT device (or TMCM server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the TMCM server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

The MCP deals with this issue by introducing a one-way communication model. With one-way communication, only the agent initiates the network connection to the server. The server cannot initiate connection to the agent. This one-way communication works well for log data transfers. However, the server dispatching of commands occurs under a passive mode. That is, the command deployment relies on the agent to poll the server for available commands.

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

- A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues
- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used.

Using MCP, Control Manager has three security levels:

- **Normal security:** Control Manager uses HTTP for communication
- **Medium security:** Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security:** Control Manager uses HTTPS for communication

One-Way and Two-Way Communication Support

MCP supports one-way and two-way communication.

One-Way Communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. In order to address this issue, MCP uses one-way communication. One-way communication has the Control Manager agent initiating the connection to and polling of commands from the server. Each request is a CGI-like command query or log transmission. In order to reduce the network impact, the connection is kept alive and open as much as possible. A subsequent request uses an existing open connection. Even if the connection is dropped, all connections involving SSL to the same host benefit from session ID cache that drastically reduces re-connection time.

Two-Way Communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on HTTP protocol. Two-way communication can improve real time dispatching and processing of commands from the server by the Control Manager agent. The Control Manager agent side needs a Web server or CGI compatible program that can process CGI-like requests to receive notifications from Control Manager server.

Single Sign-on (SSO) Support

Through MCP, Control Manager 3.5 now supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

The following products support SSO with Control Manager 3.5:

- SeverProtect for Linux version 2.5
- Network VirusWall™ Enforcer 2500
- Network VirusWall Enforcer 1200

Cluster Node Support

Under varying cases administrators may like to group certain product instances as a logical unit, or cluster (for example products installed under a cluster environment present all installed product instances under one cluster group). However, from the Control Manager server's perspective, each product instance that goes through the formal registration process is regarded as an independent managed unit and each managed unit is no different from another.

Through MCP, Control Manager supports cluster nodes.

Control Manager Agent Heartbeat

To monitor the status of Network VirusWall Enforcer 1200 devices, Control Manager agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the Network VirusWall Enforcer 1200 device and to check for commands to the Network VirusWall Enforcer 1200 device from Control Manager. The Control Manager Web console then presents the product status. This means that the Network VirusWall Enforcer 1200 device's status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each Network VirusWall Enforcer 1200 device in a sequential manner in the background. Control Manager changes the status of Network VirusWall Enforcer 1200 devices to offline, when a fixed period of time elapses without a heartbeat from the Network VirusWall Enforcer 1200 device.

Active heartbeats are not the only means Control Manager has for determining the status of Network VirusWall Enforcer 1200 devices. The following also provide Control Manager with the Network VirusWall Enforcer 1200 device's status:

- Control Manager receives logs from the Network VirusWall Enforcer 1200 device. Once Control Manager receives any type of log from the Network VirusWall Enforcer 1200 device successfully, this implies that the Network VirusWall Enforcer 1200 device is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the Network VirusWall Enforcer 1200 device to retrieve the pending command. If server connects to the Network VirusWall Enforcer 1200 device successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.

- In one-way communication mode, the Control Manager agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The Control Manager agent heartbeats implement with the following ways:

- **UDP:** If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also the transmitting client cannot make sure that the server does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the Network VirusWall Enforcer 1200 device applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains Network VirusWall Enforcer 1200 device activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 PM, and from 6:00 P.M. to 12:00 P.M.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

TABLE B-2. Heartbeat Recommendations

Registering Network VirusWall Enforcer 1200 to Control Manager

Network VirusWall Enforcer 1200 is a standalone product and you do not need to register the device to Control Manager. However, by registering to Control Manager you gain the benefits explained earlier in this appendix. All features are managed using the Network VirusWall Enforcer 1200 Preconfiguration console and Web console. Before registering Network VirusWall Enforcer 1200 to a Control Manager 3.5 server, you must ensure that both the device and the Control Manager server belong to the same network segment.

To register Network VirusWall Enforcer 1200 to Control Manager:

1. Log on to the Preconfiguration console.
2. On the **Main Menu** of the Preconfiguration console, type 2 to select **Device Settings** and press **Enter**. The Device Settings Screen displays.

Note: Control Manager uses the name specified in the Host name field to identify Network VirusWall Enforcer 1200 devices. The Host name appears in the Product Directory of Control Manager.

3. Use the down arrow to bring the cursor down to **Register to Control Manager**, then use the spacebar to change the option to **[yes]**.
4. Type the Control Manager server IP address in the **FQDN or IP address** field.
5. Type the port number and IP address of your router or NAT device server in the **Port forwarding IP address** and **Port forwarding port number** fields.

Note: The Network VirusWall Enforcer 1200 device uses the **Port forwarding IP address** and **Port forwarding port number** for two-way communication with Control Manager.

6. Use the down arrow to bring the cursor down to **Return to main menu** and press **Enter**.
7. On the Main Menu, type `A` to select **Save and log off** and press **Enter**. A confirmation screen displays.
8. Ensure the cursor is on **OK** and press **Enter**.
9. From the Control Manager management console **Main Menu**, click **Products**.
10. On the left most menu, select **Managed Products** from the list and then click **Go**.
11. Check to see that Network VirusWall Enforcer 1200 displays.

Managing Network VirusWall Enforcer 1200 From Control Manager

A managed product refers to a Network VirusWall Enforcer 1200 device, an antivirus, a content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons. These icons represent Network VirusWall Enforcer 1200 devices, other Trend Micro antivirus and content security products, as well as third party products.

Indirectly administer the managed products either individually or by groups through the Product Directory. Use the Directory Manager to customize the Product Directory organization.

Understanding Product Directory

Take care when planning the structure of the Product Directory, a logical grouping of managed products, because it affects the following:

- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For example, granting access to the root segment grants access to the entire Directory. On the other hand, granting access to a specific Network VirusWall Enforcer 2500 device only grants access to that specific product.
- **Deployment planning:** Control Manager deploys virus pattern, scan engine, spam rule, and program updates to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory will therefore simplify the designation of recipients.
- **Outbreak Prevention Policy and Damage Control Template deployments:** OPP and DCS deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

Product Directory icons:

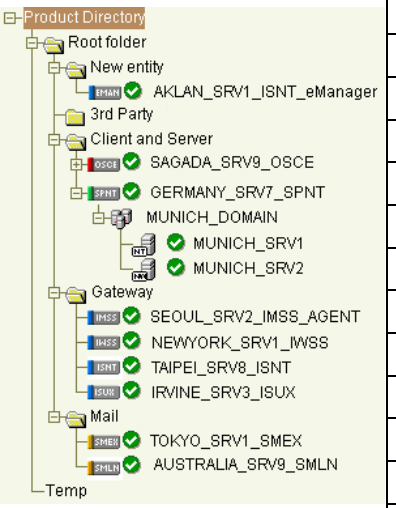
PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
		New entity or user-defined folder name
		InterScan eManager
		OfficeScan Corporate Edition
		ServerProtect Information Server
		ServerProtect Domain
		ServerProtect for Windows (Normal Server)
		ServerProtect for NetWare (Normal Server)
		InterScan Messaging Security Suite
		InterScan Web Security Suite
		InterScan VirusWall for Windows
		InterScan VirusWall for UNIX
		ScanMail for Microsoft Exchange
		ScanMail for Lotus Notes
		Network VirusWall
		
		
		NetScreen Global PRO Firewall
		Managed Product connection status icon

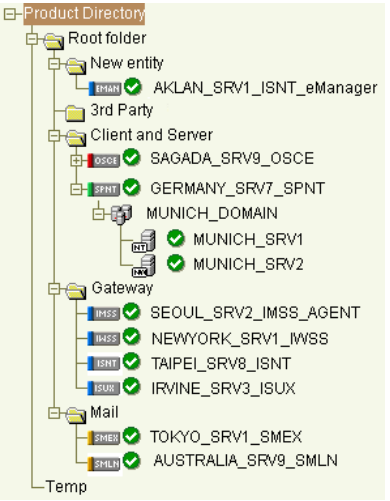
TABLE B-3. Managed Product Icons

Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your Network VirusWall Enforcer 1200 devices according to their protection type and the Control Manager network administration model. For example, grant access rights to mail administrators to configure the Mail folder.

Accessing a Network VirusWall Enforcer 1200 Device's Default Folder

Newly registered Network VirusWall Enforcer 1200 devices usually appear in the New entity folder depending on the user account specified during the agent installation. Control Manager determines the default folder for the Network VirusWall Enforcer 1200 device by the privileges of the user account specified during the product agent installation. However, Control Manager segregates managed products handled by Trend VCS agents under the Trend VCS agents folder.

The following presents different scenarios for the accessible folders given to the account and the resulting default managed product location:



Accessible Folder Given to the Account	Default Managed Product Location
Root folder	New entity
Mail	Mail
SAGADA_SRV9_OSCE	New entity

User accounts set to access a specific managed product cannot access any newly registered managed products.

TABLE B-4. Managed Products vs. User Access

Access Product Directory

Use the Product Directory to administer Network VirusWall Enforcer 1200 devices registered with the Control Manager server.

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.

Manually Deploy New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your Network VirusWall Enforcer 1200 devices and other managed products on demand. This is useful especially during virus outbreaks.

Download new components before deploying updates to specific or groups of Network VirusWall Enforcer 1200 devices or managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired folder or Network VirusWall Enforcer 1200 device.
4. On the working area, click the **Tasks** tab.
5. Select **Deploy <component>** from the Select task list.
6. Click **Next>>**.
7. Click **Deploy Now** to start the manual deployment of new components.
8. Monitor the progress via Command Tracking.
9. Click the **Command Details** link to view details for the Deploy Now task.

View Network VirusWall Enforcer 1200 Devices Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all Network VirusWall Enforcer 1200 devices and other managed products present in the Product Directory tree.

There are two ways to view the Network VirusWall Enforcer 1200 devices status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or Network VirusWall Enforcer 1200 device.
   - If you click a Network VirusWall Enforcer 1200 device or managed product, the Product Status tab displays the Network VirusWall Enforcer 1200 device or managed product's summary
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries

---

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configure Network VirusWall Enforcer 1200 Devices and Managed Products

Depending on the product and agent version:

- You can configure devices or products either individually or in groups according to folder division

  Perform group configuration using the folder Configuration tab.

Note: When performing a group configuration, verify that you want all Network VirusWall Enforcer 1200 device in a group to have the same configuration. Otherwise, add devices or managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows either the product's Web console or a Control Manager-generated console

To configure a product:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired Network VirusWall Enforcer 1200 device, managed product or folder.
4. On the working area, click the **Configuration** tab.
5. Select the product to configure from the Select product list.

Note: Step 4 is necessary when you use the folder Configuration tab.

---

6. At the Select configuration list, select the product feature to access or configure.
7. Click **Next**. The Network VirusWall Enforcer 1200 or managed product Web-based console or Control Manager-generated console appears.

Issue Tasks to Network VirusWall Enforcer 1200 Devices and Managed Products

Use the Tasks tab to invoke available actions to a group or specific Network VirusWall Enforcer 1200 device or managed product. You can perform the following tasks on Network VirusWall Enforcer 1200 devices:

- Configuration Replication
- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Replicate configuration to entire folder

Deploy the latest pattern file, or scan engine to Network VirusWall Enforcer 1200 devices with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to Network VirusWall Enforcer 1200 devices:

1. Access the Product Directory.
2. On the left-hand menu, select the desired Network VirusWall Enforcer 1200 device or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the Select task list.
5. Click **Next**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View Network VirusWall Enforcer 1200 Device and Managed Product Logs

Use the Logs tab to query and view logs for a group or specific Network VirusWall Enforcer 1200 device.

To query and view Network VirusWall Enforcer 1200 device logs:

1. Access the Product Directory.

2. On the left-hand menu, select the desired Network VirusWall Enforcer 1200 device or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

   Event Logs:

   a. Provide the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE B-5. Search Parameters for Event Logs

   b. Click **Display Logs** to begin the query and display the query results.

   Security Logs:

   a. Select All virus log incidents or a specific security logs type and then click **Query**.

b. Provide the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE B-6. Search Parameters for Security Logs

c. Click **Display Logs** to begin the query.

Note: eManager managed products records content security violations in the Security Logs, not in the Virus Logs.

5. The Query Result screen displays the results in a table format.
6. The Generated at entity column of the result table indicates the Control Manager server time.

Recover Network VirusWall Enforcer 1200 Devices Removed From the Product Directory

The following scenarios can cause Control Manager to delete Network VirusWall Enforcer 1200 devices from the Product Directory:

- Reinstalling the Control Manager server and selecting Delete existing records and create a new database option

  This option creates a new database using the name of the existing one.
- Replacing the corrupted Control Manager database with another database of the same name
- Accidentally deleting theNetwork VirusWall Enforcer 1200 device using the Directory Manager

If a Control Manager server's Network VirusWall Enforcer 1200 devices records are lost, the agents on the products still "know" where they are registered to. The product agent will automatically re-register itself after 8 hours or when the service is restarts.

To recover Network VirusWall Enforcer 1200 devices removed from the Product Directory:

- Restart the Network VirusWall Enforcer 1200 device.
- **Wait for the Agent to re-register itself:** By default, the Control Manager agent verifies its connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

  Refer to Change agent connection re-verification frequency to modify the agent verification time.

Search for Network VirusWall Enforcer 1200 Devices, Product Directory Folders or Computers

Use the Search button to quickly:

- Add a specific or a group of Network VirusWall Enforcer 1200 devices to Temp
- Find and locate a specific Network VirusWall Enforcer 1200 device in the Product Directory

To search for a folder or Network VirusWall Enforcer 1200 device:

1. Access Product Directory.
2. On the left menu, click **Search**.
3. On the working area, provide the following search parameters:

PARAMETER	DESCRIPTION
Search for	Select the object of the search from the drop down list Search for managed products or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name Select **Case sensitive** to narrow down the search results.

TABLE B-7. Search Parameters

PARAMETER	DESCRIPTION
Managed product status / Communicator status	Select the appropriate connection status, for the Communicator or managed product The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose All to search for objects regardless of the connection status.
Product	Select the appropriate product from the list. Choose **All** to search for all products.

TABLE B-7. Search Parameters

4. Click **Begin Search** to start searching.
5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Refresh the Product Directory

To refresh the Product Directory:

- In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Understanding Directory Manager

After the registering to Control Manager, the Network VirusWall Enforcer 1200 device first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs. For example, you can group products by location or product-type messaging security, web security, file storage protection, and so on.

The Directory allows you to create, modify, or delete folders, and move Network VirusWall Enforcer 1200 devices between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the Network VirusWall Enforcer 1200 devices belonging to each folder. Consider the following factors when planning and implementing your folder and Network VirusWall Enforcer 1200 device structure:

- Product Directory

- User Accounts
- Deployment Plans

Group Network VirusWall Enforcer 1200 devices according to geographical, administrative, or product specific reasons. In combination with different access rights used to access Network VirusWall Enforcer 1200 devices or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages:

Grouping Type	Pro's	Con's
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

TABLE B-8. Product Grouping Comparison

Using the Directory Manager Options

Directory Manager provides seven options: New Folder, Delete, Rename, Undo, Redo, Cut, and Paste.

Use these options to manipulate and organize Network VirusWall Enforcer 1200 devices in your Control Manager network.

To use and apply changes in the Directory Manager:

- Right-click a folder or Network VirusWall Enforcer 1200 device to open a pop-up menu that presents a list of actions you can perform
- Click + or the folder to display the Network VirusWall Enforcer 1200 devices belonging to a folder
- Press **Enter** or click anywhere when you rename a folder
- Click **Save** to apply your changes and update the Directory Manager organization
- Click **Reset** to discard changes that are not yet saved

Access Directory Manager

Use Directory Manager to group Network VirusWall Enforcer 1200 devices together.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

Create Folders

Group Network VirusWall Enforcer 1200 devices into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If you are building the tree for the first time, right-click the Root folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming Folders or Network VirusWall Enforcer 1200 Devices

To rename a folder or Network VirusWall Enforcer 1200 device:

1. Access Directory Manager.
2. On the working area, right-click the folder or Network VirusWall Enforcer 1200 device you want to rename and then select **Rename** from the pop-up menu. The folder/Network VirusWall Enforcer 1200 device name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

Note: Renaming a Network VirusWall Enforcer 1200 device only changes the name stored in the Control Manager database there are no effects to the product.

Move Folders or Network VirusWall Enforcer 1200 Devices

To transfer or move a folder or Network VirusWall Enforcer 1200 device to another location:

1. Access Directory Manager.
2. On the working area, select the folder or Network VirusWall Enforcer 1200 device you want to move.
3. Do one of the following:
   - Drag-and-drop the folder or Network VirusWall Enforcer 1200 device to the target new location
   - Cut and paste the folder or Network VirusWall Enforcer 1200 device to the target new location
4. Click **Save**.

Delete User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a Network VirusWall Enforcer 1200 device which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder

Take caution when deleting user-defined folders, you may accidentally delete a Network VirusWall Enforcer 1200 device

Understanding Temp

Temp, a collection of Network VirusWall Enforcer 1200 device shortcuts, allows you to focus your attention on specific products without changing the Product Directory organization. Use Temp for deploying updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all Network VirusWall Enforcer 1200 device shortcuts when you log off the management console.
- You can only add the Network VirusWall Enforcer 1200 devices to Temp if you can see them in the Product Directory, you cannot make shortcuts to products that you cannot access.

Using Temp

You can manipulate Network VirusWall Enforcer 1200 devices in Temp the same way you would with Network VirusWall Enforcer 1200 devices in the Product Directory. The folders and Network VirusWall Enforcer 1200 devices belonging to Temp have the same folder and Network VirusWall Enforcer 1200 device-level controls. However, Control Manager determines what actions you can perform on the Network VirusWall Enforcer 1200 devices according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of Network VirusWall Enforcer 1200 devices using folder-level access rights.
- Select a specific Network VirusWall Enforcer 1200 device, and then use the available Product Directory tabs to perform an action.

Access Temp

Use Temp to collect Network VirusWall Enforcer 1200 device shortcuts.

To access Temp:

1. Access Product Directory.
2. On the left most menu, click **Temp**.

Adding Network VirusWall Enforcer 1200 Devices to Temp

There are three methods to add Network VirusWall Enforcer 1200 devices to Temp:

- From the Search results
- From the Product Directory
- Add Network VirusWall Enforcer 1200 devices with outdated components based on the Status Summary page

Trend Micro recommends that you add several Network VirusWall Enforcer 1200 devices at once to Temp using the last method. The Status Summary screen provides information as to which Network VirusWall Enforcer 1200 devices use outdated components. It simplifies virus pattern and scan engine updates on groups of Network VirusWall Enforcer 1200 devices belonging to different folder groups.

Note: Adding Network VirusWall Enforcer 1200 devices to Temp only allows you to collect Network VirusWall Enforcer 1200 devices with outdated components doing so does not trigger automatic deployment.

To add from the Search results

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for Network VirusWall Enforcer 1200 devices or folders.

4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the Network VirusWall Enforcer 1200 device shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field. For example, if you specify \pattern\mail, the following Temp structure appears:

---

5. Click **Add**. Control Manager adds Network VirusWall Enforcer 1200 devices from the search results to Temp.

To add from the Product Directory

1. Access the Product Directory.
2. On the left-hand menu, select the Network VirusWall Enforcer 1200 device you want to add to Temp.
3. Press "+" on the numeric keypad.

To add Network VirusWall Enforcer 1200 devices with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of Network VirusWall Enforcer 1200 devices that are outdated. Depending on the link you clicked, the Virus Pattern Status (Outdated), Scan Engine Status (Outdated), Spam Rule Status (Outdated) screen opens displaying

the computer name, product name, product version, and outdated component version.

5. Click **Add to Temp** in the status page. Control Manager organizes theNetwork VirusWall Enforcer 1200 devices to Temp using folders named after the page from which they were added. For example, Control Manager places Network VirusWall Enforcer 1200 devices added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

Note: Clicking **Add to Temp** only adds the Network VirusWall Enforcer 1200 devices shown on the status page. If the list of Network VirusWall Enforcer 1200 devices spans more than one screen, click **Add to Temp** on all screens to add all products with outdated component.

---

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated Network VirusWall Enforcer 1200 devices to Temp.

Removing Network VirusWall Enforcer 1200 Devices From Temp

To remove a Network VirusWall Enforcer 1200 device from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.
3. From the available Network VirusWall Enforcer 1200 devices on the Temp list, select the folder or Network VirusWall Enforcer 1200 shortcut that you want to remove.
4. Press "-" in the numeric keypad.

Note: Control Manager removes Network VirusWall Enforcer 1200 device shortcuts in Temp when you log off from the management console.

Removing Network VirusWall Enforcer 1200 devices from Temp will neither disconnect the antivirus or content security product nor uninstall the Control Manager agent from the Control Manager server.

Download and Deploy New Components From Control Manager

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

- **Pattern files/Cleanup templates** - refer to virus pattern files, Damage Cleanup templates, Vulnerability Assessment patterns, network outbreak rules, Pattern Release History, and network virus pattern files
- **Anti-spam rules** - refer to import and rule files used for anti-spam and content filtering
- **Engines** - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux
- **Product program** - these are product specific components (for example, Service Pack releases)

Note: Only registered users are eligible for components update. For more information, see the Control Manager online help Registering and Activating your Software > Understanding product activation topic.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

Understanding Update Manager

Update Manager provides functions that help you update the antivirus and content security components of your Control Manager network.

Updating the Control Manager network involves two steps:

- Downloading components: You can do this manually or by schedule
- Deploying components: You do this manually or by schedule

Understanding Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Manually Download Components

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

Tip: Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

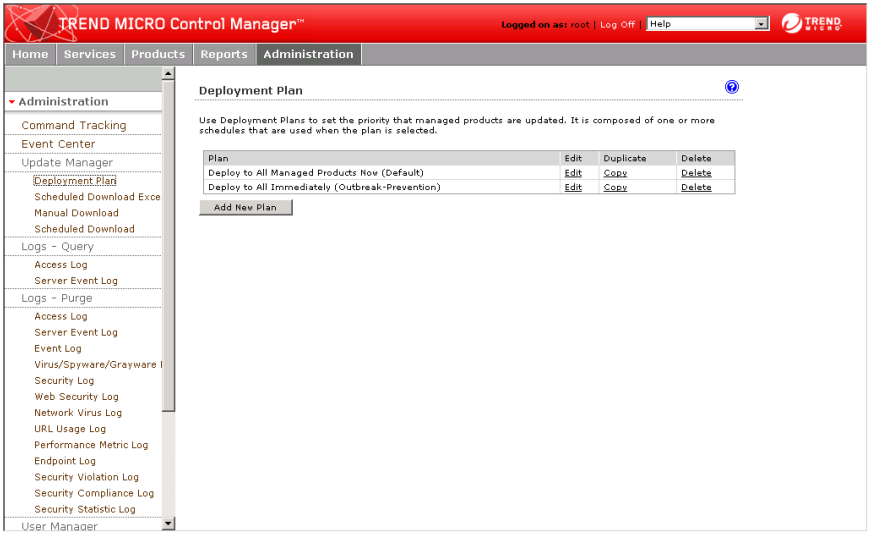
Step 6: Complete the manual download

To manually download components:

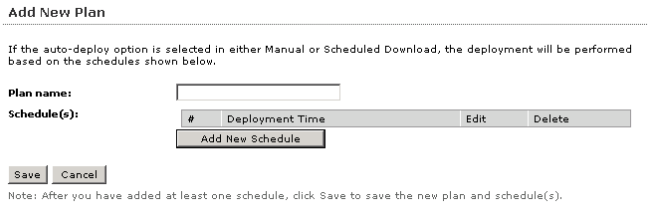
Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.

2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

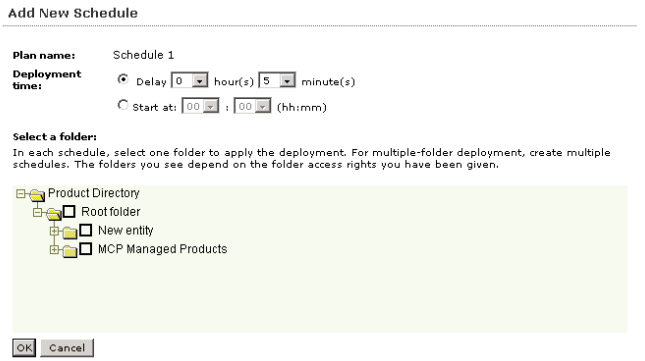


3. On the working area, click **Add New Plan**.



4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.



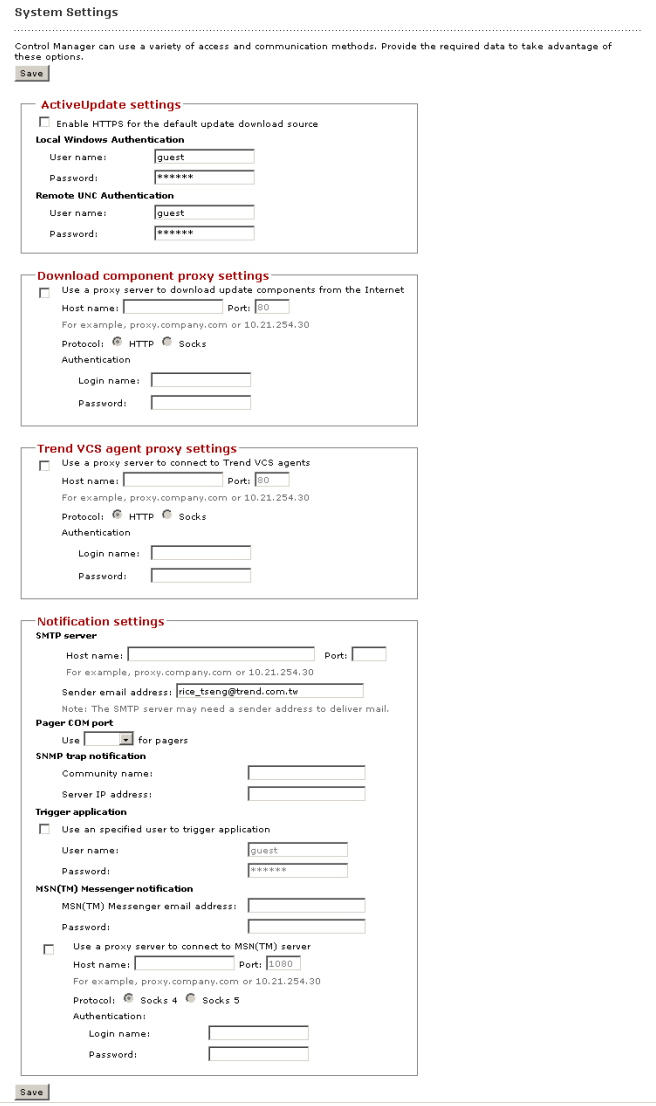
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

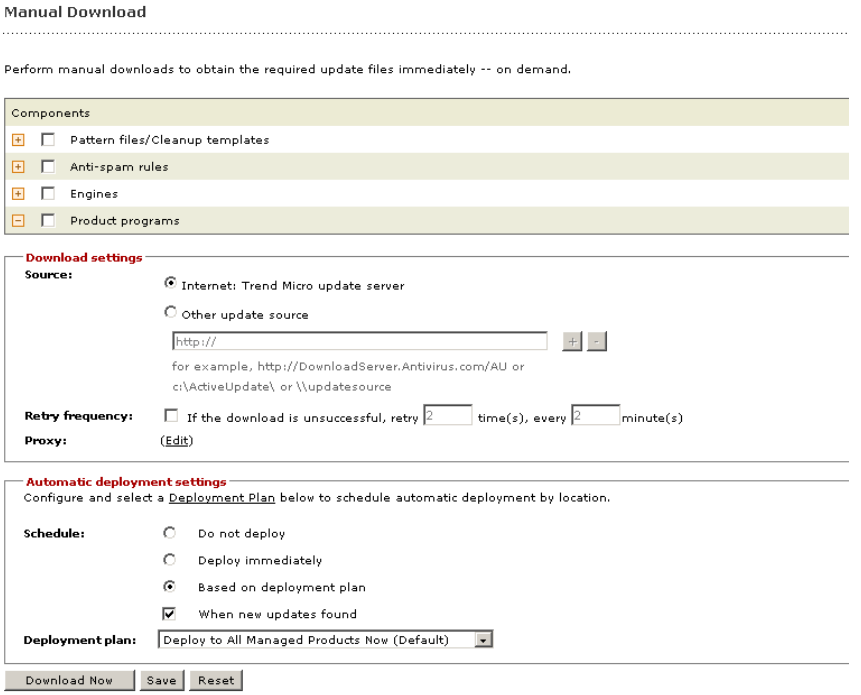
1. Click **Administration > System Settings**. The System Settings screen appears.



2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
   - **HTTP**
   - **SOCKS**
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Manual Download**. The Manual Download screen appears.



2. From the Components area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the following components to download:

      From Pattern files/Cleanup templates:

      - Virus pattern file
      - Damage cleanup template
      - Network virus pattern file for NVW

- Vulnerability assessment pattern file
- Pattern Release History

From Engines:

- Damage cleanup engine
- Network VirusWall Enforcer engine
- 32 bit DLL (95/98/ME)
- VxD
- 32 bit DLL (NT/2000)
- NTKD

Step 4: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select Retry frequency and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 5: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:

- Deploying to the managed products individually
- Testing the updated components before deployment

- **Deploy immediately:** Components download to Control Manager, then deploy to managed products
- **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
- **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
3. Click **Save**.

Step 6: Complete the manual download

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
2. Click the **Command Details** to view details from the Command Details screen.
3. Click **OK** to return to the Manual Download screen.

Configure Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.

3. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, all downloads for the selected hours are blocked.
4. Click **Save**.

Understanding Scheduled Downloads

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group, downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component is updated
- **Enabled:** Indicates if the schedule for the component is either enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

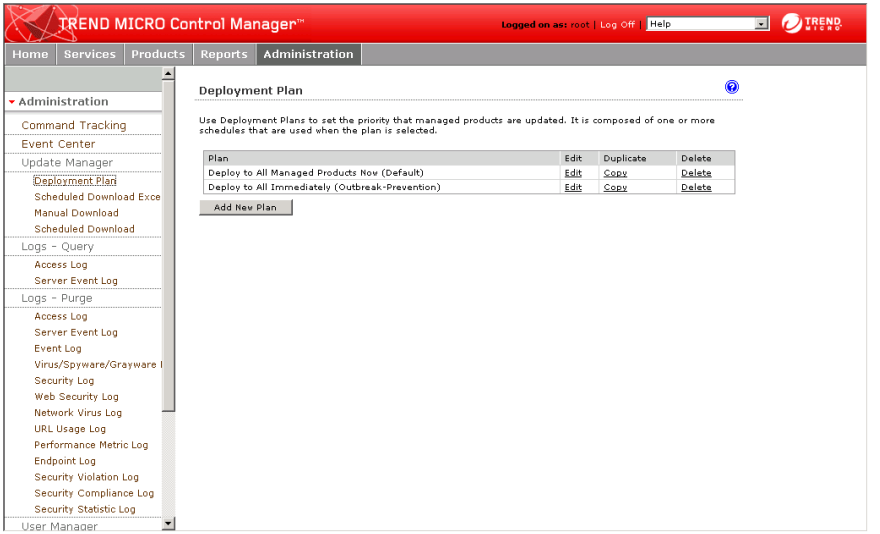
Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

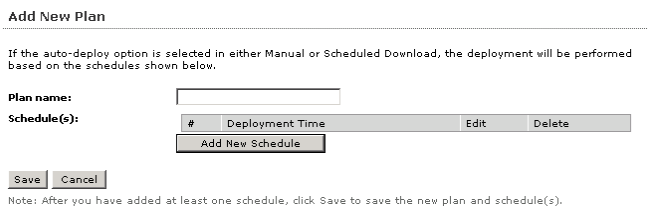
Configure Scheduled Downloads and Enable Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.



3. On the working area, click **Add New Plan**.



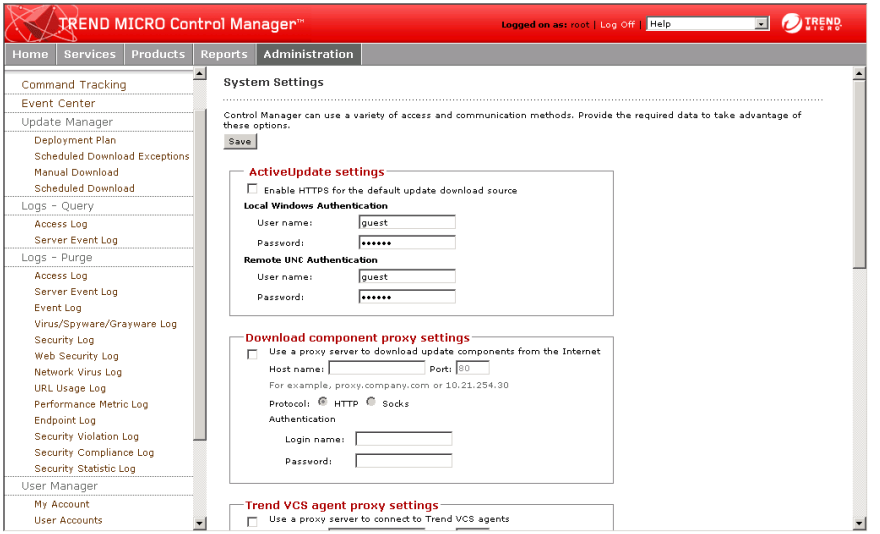
4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

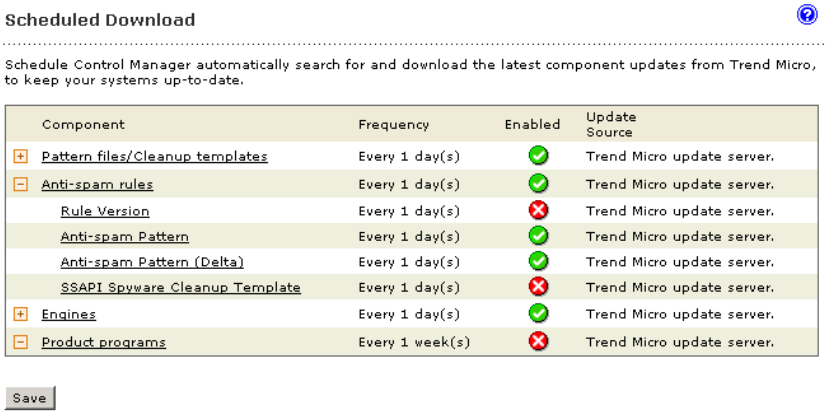
1. Click **Administration > System Settings**. The System Settings screen appears.



2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
   - HTTP
   - SOCKS
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Scheduled Download**. The Scheduled Download screen appears.



2. From the Components area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the following components to download:

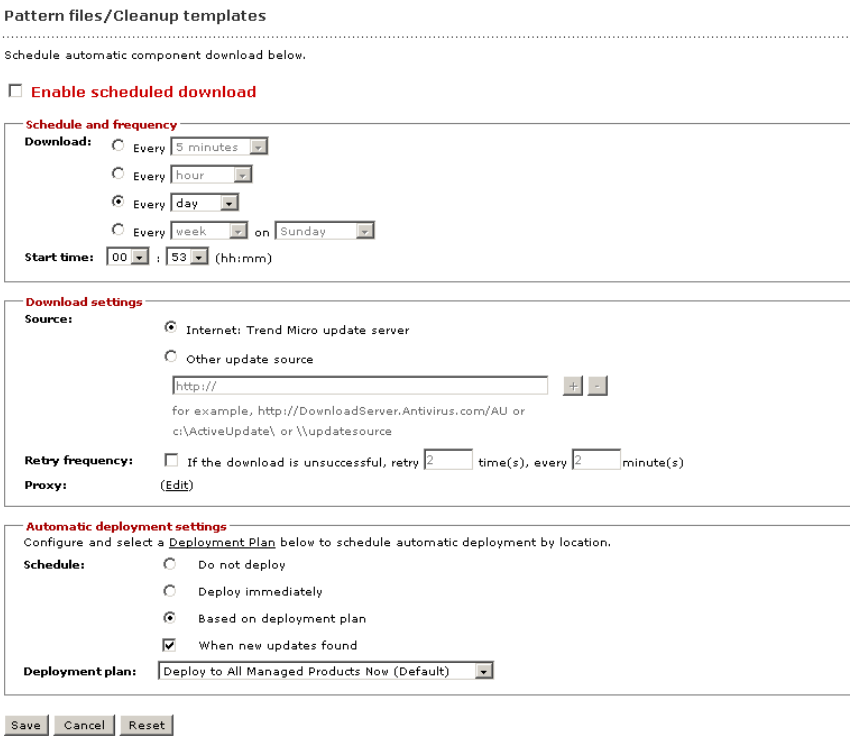
      From Pattern files/Cleanup templates:

      - Virus pattern file
      - Damage cleanup template
      - Network virus pattern file for NVW
      - Vulnerability assessment pattern file

      From Engines:

      - Damage cleanup engine
      - Network VirusWall Enforcer engine
      - 32 bit DLL (95/98/ME)
      - VxD
      - 32 bit DLL (NT/2000)
      - NTKD

The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.



Step 4: Configure the download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
   - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the **Deployment plan** list.
3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click the status button in the Enabled column.
2. Click **Save**.

Use Reports

A Control Manager **report** is an online collection of figures about virus, spyware/grayware, and content security events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- *Local reports*
- *Global reports*

Note: You can only configure the **Global Report Profile** option through the *parent server management console*.

Local Reports

Local reports are reports about managed products administered by the parent server. Local reports do not include reports generated by child servers. Use the Global Report options to view reports about managed products administered by child servers registered to the parent server.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Local Report Profile**.

Note: When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about managed products administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Global Report Profile**.
3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Understanding Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Trend Micro Control Manager 3.5 adds 3 new report templates to the 77 previously available since Service Pack 3. The reports added in Service Pack 3 fall into five categories: Desktop, Fileserver, Gateway, MailServer and Executive Summary. The new reports in Control Manager 3.5 fall into a new 6th category: Network Products. This category offers reports related to Network VirusWall.

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses. This change effects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can enter a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the six categories of reports listed below. Clicking a mark into a check box includes the associated report in the final exported report file.

Control Manager 3.5 also provides 18 templates stored in `<root>\Program Files\Trend Micro\Control Manager\Reports` as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports..

Understanding Report Profiles

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF:** Rich text format; use a word processor (for example, Microsoft Word™) to view *.RTF reports
- **PDF:** Portable document format; use Adobe Reader to view *.PDF reports
- **ActiveX™:** ActiveX documents; use a Web browser to view reports in ActiveX format

---

Note: Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT:** Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

Create Report Profiles

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

Step 4: Configure the Frequency tab settings

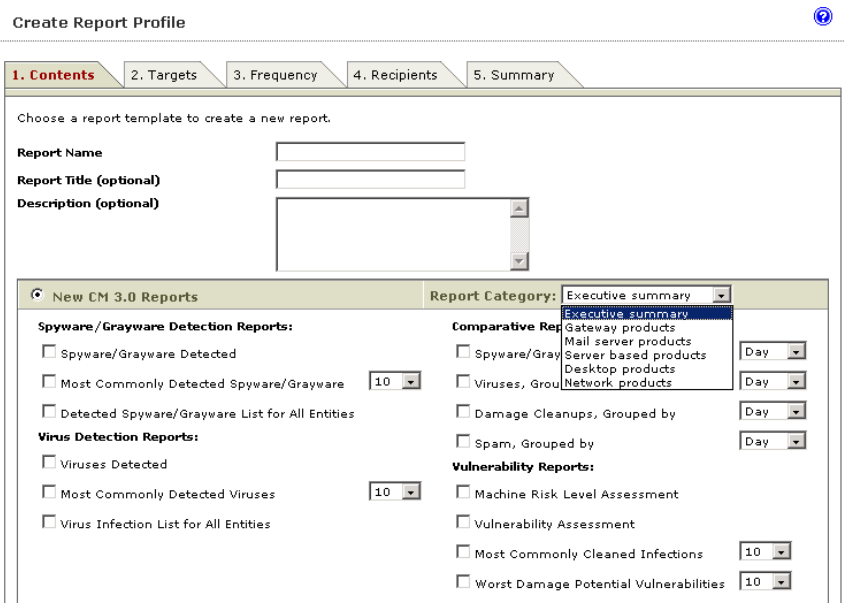
Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

1. Click **Reports** on the main menu.

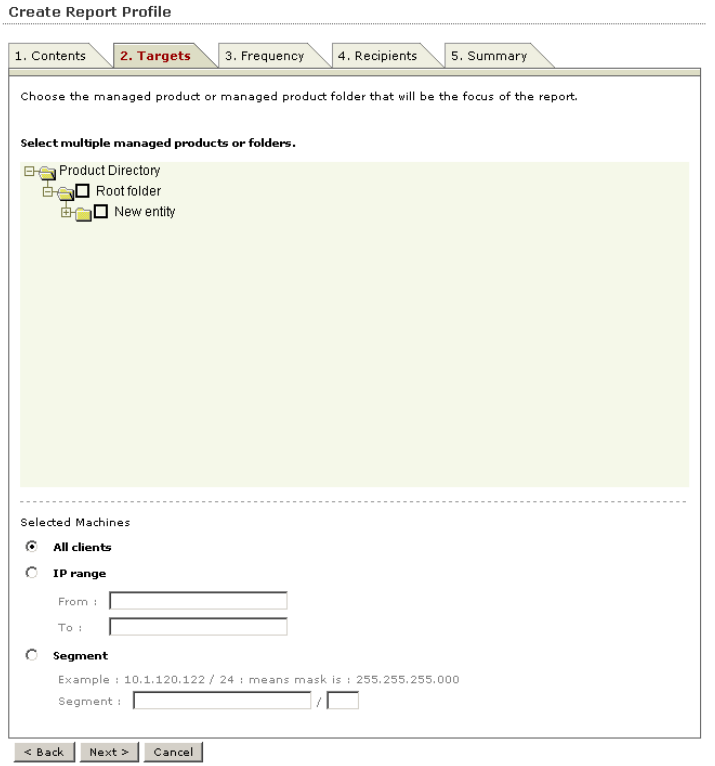
2. Take one of the following actions:
   - To create a local report profile, click **Local Report Profile** under Reports.
   - To create a global report profile, click **Global Report Profile** under Reports.
3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.



Step 2: Configure the Contents tab settings

1. In the working area under the Contents tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.
2. Type a title for the report in the **Report Title** field (optional).
3. Type a description of the report profile in the **Description** field (optional).
4. Select **Network Products** from the **Select report template** list.
5. Select the report format.

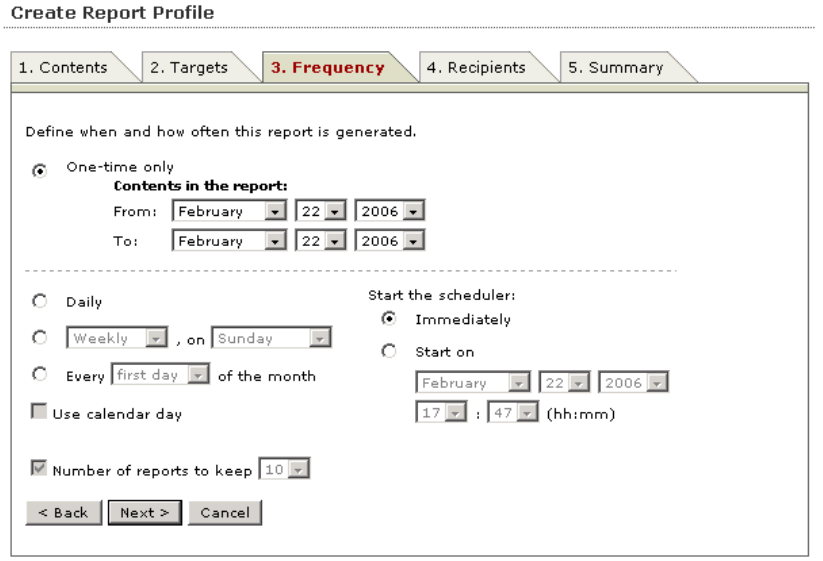
6. Click **Next >** to proceed to the Targets tab.



Step 2: Configure the Contents tab settings

1. On the working area under the Targets tab, select the target of the local or global report profile:
   - Select the Network VirusWall Enforcer 1200 devices or folders. The profile only contains information about the Network VirusWall Enforcer 1200 devices or folders selected.
   - Select the child servers. The profile only contains information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.

2. Select the machines that will the report will include:
   - **All clients:** All clients the selected Network VirusWall Enforcer 1200 device protects
   - **IP range:** Select the IP range of the clients you want to include in the report
   - **Segment:** Select the IP range and segment of the clients you want to include in the report
3. Click **Next >** to proceed to the Frequency tab.



Step 4: Configure the Frequency tab settings

1. On the working area under the Frequency tab, specify how often Control Manager generates this report. You have the following options:
   - **One-time only:** Provides information you specified in the From and To dates
   - **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time

- **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
- **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
- **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation

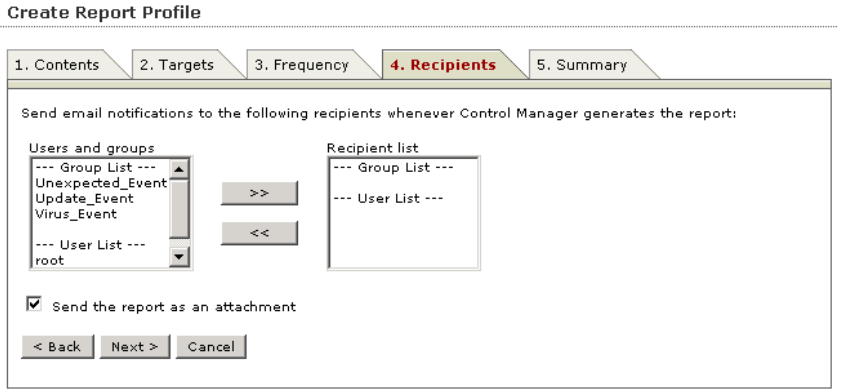
  If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs

2. Under Start the scheduler, specify when the Report Server starts collecting information for this report. Select one of the following:
   - **Immediately:** The report server collects information as soon as you save the report profile
   - **Start at:** The report server collects information at the specified date and time
3. For scheduled reports, click **Number of reports to keep** and then specify the instance Control Manager will maintain on the server.

Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

---

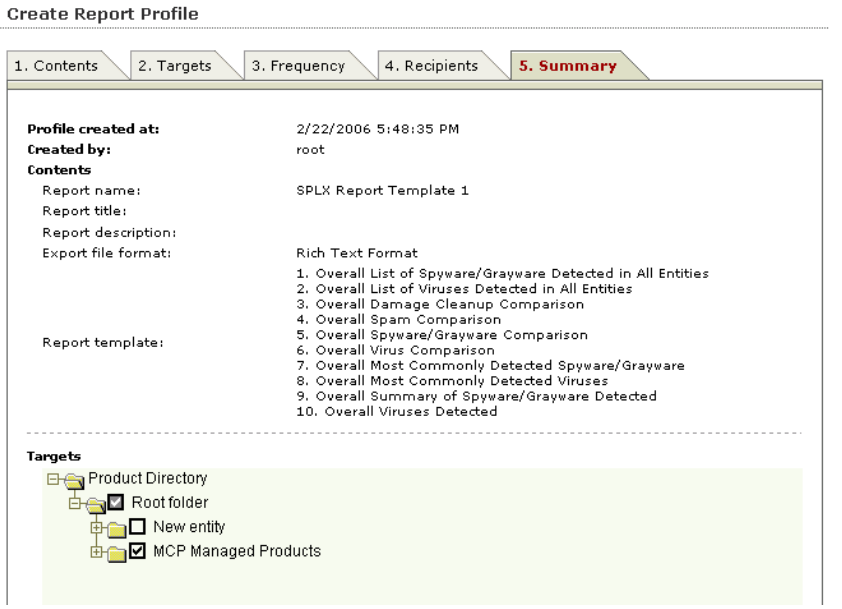
4. Click **Next >** to proceed to the Recipient tab.



Step 5: Configure the Recipient tab settings

1. On the working area under the Recipients tab, select recipients from the existing Control Manager users and groups.
   - Use >> to add recipients from the **Users and groups** list to the Recipient list
   - Use << to remove recipients from the **Recipient** list
2. Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report being generated.

3. Click **Next >** to proceed to the Summary tab.



4. On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

Review Report Profile Settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports

  On the working area under the Profile Summary column, click **View Profile**.
- Access Local or Global Scheduled Reports

  On the working area under the Profile Summary column, click **View Profile**.

Enable Scheduled Report Profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it via the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, click the profile check box.

   Click the check box adjacent to Report Profiles to select or deselect all profiles.
3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available because Control Manager generates these reports only once.

Generate On-demand Scheduled Reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.
4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.
5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

View Generated Reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

   On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time.**
4. Under the Status column, click **View Report**. The default program used to open the file format opens.

Appendix C

Supported Antivirus Products

This appendix provides a list of supported antivirus products for endpoints with Microsoft™ Windows™ 98, ME™ operating systems.

The tables in this chapter include:

Supported Products for Endpoints with Windows 98 or ME Operating Systems

Vendor	Product	Product Version
Computer Associates International, Inc.	CA eTrust Antivirus	7.x
Computer Associates International, Inc.	eTrust EZ Armor	6.1.x
Computer Associates International, Inc.	eTrust EZ Antivirus	6.1.x
Computer Associates International, Inc.	eTrust EZ Antivirus	6.2.x
Computer Associates International, Inc.	eTrust EZ Antivirus	6.4.x
Computer Associates International, Inc.	eTrust EZ Antivirus	7.x
McAfee, Inc.	McAfee VirusScan	4.5.1.x
McAfee, Inc.	McAfee VirusScan	8.x
McAfee, Inc.	McAfee VirusScan	9.x
McAfee, Inc.	McAfee VirusScan	10.x
McAfee, Inc.	McAfee VirusScan Professional Edition	7.x
McAfee, Inc.	McAfee VirusScan Professional	8.x
McAfee, Inc.	McAfee VirusScan Professional	9.x
McAfee, Inc.	McAfee Managed VirusScan	3.x
McAfee, Inc.	McAfee VirusScan	8xxx
SOFTWIN	BitDefender Free Edition	7.x
SOFTWIN	BitDefender Standard Edition	7.x

TABLE C-1. Supported Products for Endpoints with Windows 98 and ME Operating Systems

Vendor	Product	Product Version
SOFTWIN	BitDefender Professional Edition	7.x
SOFTWIN	BitDefender 8 Free Edition	8.x
SOFTWIN	BitDefender 8 Standard	8.x
SOFTWIN	BitDefender 8 Professional Plus	8.x
SOFTWIN	BitDefender 9 Standard	9.x
SOFTWIN	BitDefender 9 Professional Plus	9.x
Symantec Corp.	Symantec AntiVirus	9.x
Symantec Corp.	Symantec AntiVirus Client	8.x
Symantec Corp.	Norton AntiVirus 2002	8.00.58.x
Symantec Corp.	Norton AntiVirus 2003	9.x
Symantec Corp.	Norton AntiVirus 2003 Professional Edition	9.x
Symantec Corp.	Norton AntiVirus 2004	10.x
Symantec Corp.	Norton AntiVirus 2004 (Symantec Corporation)	10.x
Symantec Corp.	Norton AntiVirus	10.x
Symantec Corp.	Norton AntiVirus 2005	11.0.x
Symantec Corp.	Norton Internet Security	8.0.x
Trend Micro, Inc.	Trend Micro Internet Security	11.x
Trend Micro, Inc.	Trend Micro PC-cillin Internet Security 2005	12.x
Trend Micro, Inc.	PC-cillin 2003	10.x
Trend Micro, Inc.	Trend Micro PC-cillin Internet 2004	11.x
Trend Micro, Inc.	Trend Micro Internet Security	12.x

TABLE C-1. Supported Products for Endpoints with Windows 98 and ME Operating Systems

Supported Products for Endpoints with Windows XP, 2000, or 2003 Operating Systems

Refer to the Supported Products screen in the Web console for the latest list for endpoints with Windows XP, 200, or 2003 operating systems.

Glossary

Tip: For a faster glossary search when viewing this appendix online, use the Acrobat Reader's **Find** option to search for a term.

A **B** **C** **D** **E** **F** G H **I**

J K **L** **M** **N** **O** **P** Q **R**

S **T** **U** **V** **W** X Y Z

A

Top

Active
In a failover solution, it refers to the device that is currently in use.

ActiveUpdate
ActiveUpdate server. The Trend Micro server hosting the Network VirusWall Enforcer 2500 components. The ActiveUpdate server can be set as the update source.

B

Top

Baseboard management controller
Short for BMC. It is a microcontroller responsible for the Intelligent Platform Management Interface (IPMI).

BMC logs
Short for Board Management Control logs. These type of logs report critical hardware status and error.

BPDU
Short for **b**ridge **p**rotocol **d**ata **u**nit. BPDUs are data messages that travel across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where the sender intended it to go. BPDU messages go back and forth across bridges to detect loops in a network topology. The protocol then removes the loops by shutting down selected bridge interfaces and places redundant switch ports in a backup, or blocked, state.

C

Top

Client
Refers to an IP address, which Network VirusWall Enforcer 1200 scans for unwanted packets.

D

Top

Device role
A device identifies its role after assigning the original attribute setting (Primary or Secondary).

DHCP
Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DIMM
Short for dual in-line memory module, a small circuit board that holds memory chips. A single in-line memory module (SIMM) has a 32-bit path

to the memory chips whereas a DIMM has 64-bit path. Because the Pentium processor requires a 64-bit path to memory, you need to install SIMMs two at a time. With DIMMs, you can install memory one DIMM at a time.

Directory Manager
Allows you to customize the Product Directory organization to suit your administration model needs.

E

Top

Ethernet
One of the most widely implemented local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10Mbps, 100Mbps (100Base-T or Fast Ethernet), or 1,000Mbps or 1Gbps.

F

Top

Failopen
A fault-tolerance solution allows the Network VirusWall Enforcer 1200 device to continue to pass traffic in an event when a software or hardware failure occurs within the device.

Fault tolerance
The ability of a system to respond gracefully to an unexpected hardware or software failure.

I

Top

IETF
Short for Internet Engineering Task Force, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

IGMP
Short for Internet Group Management Protocol. It is the standard protocol for IP multicasting in the Internet.

The purpose of IGMP is to establish host memberships in particular multicast groups on a single network. Its mechanism allows a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group.

Image
Refers to the Network VirusWall Enforcer 1200 firmware or program file.

Intelligent Platform Management Interface
Short for IPMI. IPMI is an interface or gateway between the host system (that is, server management software) and the periphery devices.
Internal port

Also referred to as INT. The Network VirusWall Enforcer 1200 port/interface that connects to the network.

Internet Control Message Protocol
Short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

IP multicasting
Sending out data to distributed servers on the MBone. For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic, which requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source, transmitting just one set of packets for all the destinations.

IPsec
Short for IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec is a widely used method of implementing Virtual Private Net-

works (VPNs).

L

Top

L2 devices
Short for layer 2 devices. These devices refer to hardware devices connected to the Data Link layer of the OSI model. Switches are examples of L2 devices.

L3 devices
Short for layer 3 devices. These devices refer to hardware devices connected to the Network layer of the OSI model. Routers are examples of L3 devices.

L2TP
Short for Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).

LAN
Short for local area network. A computer network that spans a relatively small area. Most LANs reside in a single building or a group of buildings.

LCD module
See LCM console.

LCD
Short for Liquid Crystal Display. A 5x7 dot display LCD on the Network VirusWall Enforcer 1200 front panel that is capable if displaying 2x16 character messages.

LCM console
Also referred to as the LCD module. It is composed of the LCD and Control Panel, which is located on the Network VirusWall Enforcer 2500 front panel. This allows basic Network VirusWall Enforcer 2500 device settings configuration. See *Table 1-1, "Comparison of the Network VirusWall Enforcer 1200 management tools," on page 9*.

M

Top

Managed product
Refers to any software or hardware application managed by a Control Manager server.

Management console
Short for Control Manager management console. A Web-based console published via IIS from the Control Manager server, which administrators use to administer managed products and devices registered to Control Manager.

MBone
Short for Multicast Backbone. MBone is an extension to the Internet to support IP multicasting -- two-way transmission of data between multiple sites.

Mesh network
A mesh network is a network that employs one of two connection arrangements: full mesh topology or partial mesh topology. In the full mesh topology, each node connects directly to each of the others. In the partial mesh topology, nodes e connect to only some, not all, of the other nodes.

MIB
Management Information Base (MIB). Groups the SNMP information organized in the form of objects. Each object is an essential data about a particular aspect of the managed Network VirusWall Enforcer 1200 device, such as the number of packets received or memory utilization statistics.

N

Top

NAT
See Network Address Translation.

Network Address Translation
Also known as NAT. The term refers to an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT device located where the LAN meets the Internet makes all necessary IP address translations.

Network Interface Card
Also known as NIC. The term refers to an expansion board inserted into a computer so the computer can connect to a network. Most NICs

work only with a particular type of network, protocol, and media, although some can serve multiple networks.

Network segment
A section of a network that falls within the bounds of bridges, routers, or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN. If segmented correctly, most network traffic remains within a single segment, enjoying the full 10 Mbps bandwidth. Hubs and switches connect each segment to the rest of the LAN.

Network Time Protocol
Also known as NTP. The term refers to an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

Network virus
The type of threat that Network VirusWall Enforcer 1200 devices can detect, eliminate, and contain.

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the known malware programs, such as worms, are actually network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

NIC
See network interface card.

NMS
In the SNMP management architecture, one or more computers on the network act as a network management station (NMS) and poll the managed devices to gather information about their performance and status.

NTKD
Refers to scan engine used by products running on Windows NT, 2000, or XP machines.Operation Mode

The Network VirusWall Enforcer 1200 Preconfiguration menu (menu number 3) that provides the options to configure the failopen, failover, and port redundancy settings.

NTP
See Network Time Protocol.

O Top

OSI model
Short for Open System Interconnection model. This model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. Network VirusWall Enforcer 1200 works with L2 and L3 devices.

P Top

Port-based VLAN
A type of virtual LAN setup wherein each physical switch port has an access list specifying membership in a set of VLANs.
Network VirusWall Enforcer 1200 supports port-based VLAN through Port Grouping Operation Mode.

PPPoE
Short for Point-to-Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device, or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

PPTP

Short for Point-to-Point Tunneling Protocol, a new technology for creating Virtual Private Networks (VPNs), developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum.

Preconfiguration console
The console used to preconfigure a Network VirusWall Enforcer 1200 device.

Preconfiguring a Network VirusWall Enforcer 2500 device allows you to modify the basic Network VirusWall Enforcer 1200 default settings, perform network configuration, and set the Operation Mode. See *Table 1-1, "Comparison of the Network VirusWall Enforcer 1200 management tools," on page 9*.

Primary
Primary device. Identifies the original attribute of a device to support the failover mode. The Primary Network VirusWall Enforcer 1200 device is automatically assigned the Management role.

Product Directory
The Product Directory is a logical grouping of managed products accessible from the Control Manager management console.

R

Top

Redundant device pair
Describes Network VirusWall Enforcer 1200 devices configured to filter traffic through the same routes where if one device fails the other continues to filter and assumes all traffic filtering.

Redundant ports
Describes Network VirusWall Enforcer 1200 ports used when the other port fails.

S

Top

Scan engine
Trend Micro Network Virus Scan Engine. The antivirus component that filters network packets for threats and other viruses.

Secondary
Identifies the original attribute of a device to support the failover switchback mode. The Secondary Network VirusWall Enforcer 1200 device automatically takes on the Standby role.

Segment
A section of a network that is bounded by bridges, routers, or switches.

SNMP agent
A software module in a managed device, which communicates with the NMS.

SNMP
Simple Network Management Protocol (SNMP) is set of communications specifications for managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

Spanning Port
Spanning Port indicates the ability to copy traffic from all the ports to a single port but also typically disallows bi-directional traffic on the port. In the case of Cisco, SPAN stands for Switch Port ANalyzer.

Spanning tree protocol
Also known as STP. This terms refers to a link management protocol that is part of the IEEE 802.1 standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing undesirable loops in a network. Multiple active paths between stations create such loops, which occur when there are alternate routes between hosts. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

Secondary Device
In a failover solution, it refers to the device that filters traffic, but is not the default Management device. This device receives configuration settings from the default Management device. This device becomes the Management device if the Management device fails. Depending on the switch-back setting, this device may or may not return the Management role to the default Management (Primary) device.

STP
See spanning tree protocol.

Switch
A device that filters and forwards packets between LAN segments.

Automatic Switch-back
A mode that allows the Management device to automatically switch-back to the default Primary device once it becomes online.

Switched Ethernet LANs
Ethernet networks that use switches to join segments.

Switched LANs
LANs that use switches to join segments.

T

Top

Tagged VLAN
A type of VLAN that uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag can indicate VLAN and QoS (Quality of Service) priority identification.

TCP
Short for Transmission Control Protocol, and pronounced as separate letters. TCP is one of

the main protocols in TCP/IP networks.

Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and guarantees packet delivery in the same order in which the originating machine sends them.

Traps
Notifications sent by managed devices to the NMS when certain events occur, such as a shutdown or authentication error.

U

Top

UDP
Short for User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. Its primary use is for broadcasting messages over a network.

V

Top

Virus pattern file
Trend Micro Network Virus Pattern (NVP). The antivirus component that provides rules and signatures to detect network threats and other vulnerabilities. Network VirusWall Enforcer 1200 uses both the Network Virus Scan Engine and Network Virus Pattern to detect known threats.

VLAN
Short for virtual LAN. A network consisting of clients that are not on the same segment of a Local Area Network (LAN) but behave as if they are.

VPN
Short for virtual private network, a network that makes use of public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanism to ensure only authorized users can access the network and unauthorized users cannot intercept information.

VxD
Refers to scan engine used by Trend Micro products running on Windows 95, 98, or ME machines.

W

Top

Worms
A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email.

Index