TREND MICRO™

Network VirusWall™ Enforcer 1500i (R210 Series)

Administrator's Guide

Network Security for Enterprise and Medium Business

Document part no. NVEM05896/130315

Release date: April 2013

Product name: Trend Micro™ Network VirusWall™ Enforcer 1500i

Software version: 3.5

Protected by US patent no. 5,623,600

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

Detailed information about how to use specific features within the product are available in the online help file and the Knowledge Base at Trend Micro website.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome at the following site:

http://docs.trendmicro.com

Contents

Preface

Chapter 1: Understanding Network VirusWall Enforcer

Chapter 2: Setting Up the Device

Chapter 3: Preparing for Policy Enforcement

Chapter 4: Policy Creation and Deployment

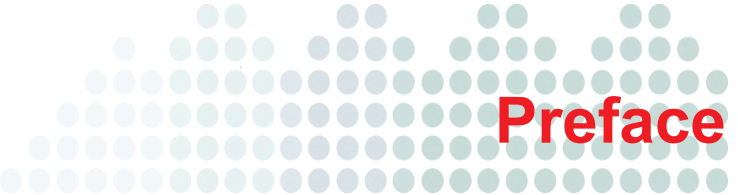
Chapter 5: Maintaining the Device

Chapter 6: Viewing Status, Logs, and Summaries

Chapter 7: Troubleshooting and FAQs

Chapter 8: Getting Support

Appendix A: Introducing Trend Micro Control Manager™



Preface

Welcome to the Administrator's Guide for Trend Micro™ Network VirusWall™ Enforcer. This book is intended for novice and experienced users of Network VirusWall Enforcer who want to quickly configure, deploy, and monitor the device.

This preface discusses the following topics:

About this Administrator's Guide

This document contains detailed information about how to configure and manage Network VirusWall Enforcer. It assumes that you have read and performed the tasks described in the *Installation and Deployment Guide*, particularly preconfiguring the device to enable access to the web console.

Content Overview

This *Administrator's Guide* provides the following information.

TABLE P-1. Document contents

CHAPTER	CONTENT SUMMARY
Understanding Network VirusWall Enforcer on page 1-1	Product overview and descriptions of features and capabilities
Setting Up the Device on page 2-1	Initial configuration procedures, including connecting to the network, securing the device, and updating components
Preparing for Policy Enforcement on page 3-1	Configuration procedures in preparation for policy enforcement
Policy Creation and Deployment on page 4-1	Policy creation procedures and examples
Maintaining the Device on page 5-1	Maintenance procedures, covering account management and configuration backup
Viewing Status, Logs, and Summaries on page 6-1	Procedures for viewing logs and managing quarantined endpoints
Troubleshooting and FAQs on page 7-1	Troubleshooting tips

TABLE P-1. Document contents

CHAPTER	CONTENT SUMMARY
Getting Support on page 8-1	How to contact technical support
Introducing Trend Micro Control Manager™ on page A-1	Overview of Control Manager, including how to use it to manage Network VirusWall Enforcer
Glossary on page GL-1	Definitions of relevant terms

Document Set

The following documents are provided with your product.

TABLE P-2. Product documentation

DOCUMENT	FORMAT	LOCATION	COVERAGE
Installation and Deployment Guide	PDF	• USB flash drive • Trend Micro Download Center	Guides you through device installation, deployment, and initial configuration
Administrator's Guide	PDF	• USB flash drive • Trend Micro Download Center	Explains features and guides your through managing policies, administrative tasks, and troubleshooting
Quick Start Guide	PDF and print	• USB flash drive • Trend Micro Download Center • Product package	Provides an overview of the device and initial tasks
Online Help	Web pages	• Web console	Explains options on the web console and relevant tasks
Readme	Text	• USB flash drive • Trend Micro Download Center	Provides late-breaking news and software build information

Documentation and Software Updates

For the latest documentation and software updates, visit the Trend Micro Download Center at:

http://downloadcenter.trendmicro.com/

Audience

This *Administrator's Guide* is targeted at the following audiences:

- Network administrators who will manage deployed devices
- Decision makers who will define policies and study how they can be enforced

Network VirusWall Enforcer documentation assumes that readers have networking knowledge and understand antivirus and content security concepts.

Device and Software Version

This *Administrator's Guide* is released for administrators that are using the following device and software version.

TABLE P-3. Target device and software

PRODUCT INFORMATION	TARGET
Device	Network VirusWall Enforcer 1500i
Hardware series	R210 Series
Software version	3.5

Document Conventions

Network VirusWall Enforcer documentation uses the following conventions.

TABLE P-4. Conventions used in the documentation

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	References to user interface items, including menus, buttons, tabs, and other labels
Italics	References to other documentation
`Monospace`	Actual text, typed commands, file names, and program output
Note:	Important information
Tip:	Recommendations
WARNING!	Critical information

Chapter 1

Understanding Network VirusWall Enforcer

This chapter introduces Trend Micro™ Network VirusWall™ Enforcer and provides an overview of its capabilities and design.

This chapter discusses the following topics:

Network VirusWall Enforcer Overview

Trend Micro™ Network VirusWall™ Enforcer is an outbreak prevention appliance that allows organizations to enforce security policies at the network layer. Network VirusWall Enforcer scans network traffic to help ensure that it is free of fast-spreading network viruses. It helps reduce the chance of severe security compromise by preventing ARP spoofing attacks.

Network VirusWall Enforcer can identify infected computers and deliver cleanup services to these endpoints. Because it works at the network layer, it can effectively quarantine and isolate actual and potential infection sources. It can address infected endpoints, endpoints with software vulnerabilities or those without adequate malware protection, and endpoints that violate network usage policies.

Network VirusWall Enforcer helps organizations take precise action on security policy violations to proactively detect, contain, and even eliminate malware outbreaks. With Network VirusWall Enforcer in the network, organizations can significantly reduce network downtime due to rapidly spreading malware and reduce the cost of dealing with the malware at individual endpoints.

Figure 1-1 depicts how Network VirusWall Enforcer can be deployed to protect a network.

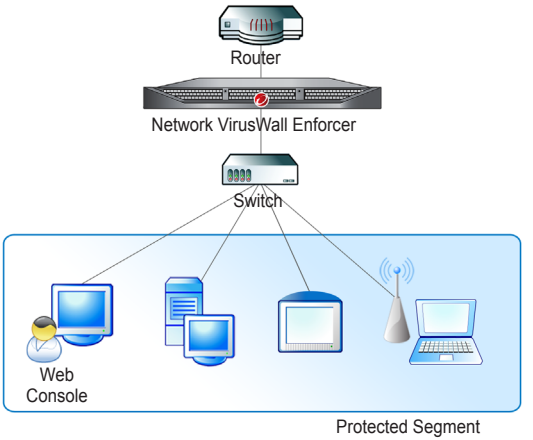


FIGURE 1-1. Basic deployment

What's New

In This Release

Software 3.5 adds the following new features and enhancements.

Block C&C Connections

Network VirusWall Enforcer can block C&C servers detected by Deep Discovery Inspector by monitoring the network and endpoint connections.

Other Enhancements

This version also includes the following features and enhancements:

- Network VirusWall Enforcer now supports TMAgent installation on Windows 8 computers.
- Network VirusWall Enforcer can now be managed using Control Manager 6.0.
- Network VirusWall Enforcer now supports the following for the Syslog:
  - Saving logs on the hard disk
  - Deleting logs on the hard disk
  - Adjusting the log level

Carried Over from Previous Versions

Software Version 3.2

64-bit Platform Support for TMAgent

Version 3.2 expands Windows 64-bit platform support, enabling the following policy enforcement capabilities:

- Antivirus software enforcement
- Pattern version enforcement
- System threat scans
- Vulnerability assessment
- Registry checks

Other Enhancements

This version also includes the following features and enhancements:

- Synchronization of global endpoint exception lists using Trend Micro Control Manager (TMCM).
- Central management of administrative accounts using the Microsoft Active Directory (AD) server.
- Adjusting the time interval for the Control Manager Log Schedule setting.

Software Version 3.1

Software version 3.1 adds the following enhancements.

Expanded IPv6 Support

Version 3.1 expands IPv6 support, enabling the following policy enforcement capabilities in IPv6 networks:

- Antivirus software enforcement
- Pattern version enforcement
- System threat scans
- Vulnerability assessment
- Registry checks

In addition to these policy enforcement capabilities, this version also supports the following in IPv6 networks:

- Web-based endpoint notifications, in addition to existing support for agent-based popup notifications
- Easy browser-based agent installation using ActiveX and remote login

Email Notifications for TDA-based Quarantine

To allow administrators to take immediate action after an endpoint is quarantined in response to a Threat Discovery Appliance (TDA) detection, Network VirusWall Enforcer can be configured to automatically send notification email. With the notification, administrators can immediately confirm and resolve any potential threats that have triggered the TDA detection. After resolving any threats, they can release the endpoint through the web console.

Software Version 3.0 Patch 3

Patch 3 for software version 3.0 includes the following enhancements:

- **Export filtered endpoint history data**—filter endpoint history data before exporting the data to a CSV file.
- **Easy shutdown**—power off the device through the web or the Preconfiguration console.
- **Easy patch installation**—apply hot fixes, patches, and service packs through the web console.

Software Version 3.0

The following features and enhancements were added with software version 3.0:

- **IPv6 support**—Network VirusWall Enforcer now supports pure IPv6 and dual-stack environments, with the following functionality available on IPv6 networks:
  - Management connections through the web console and SSH
  - Scanning for network viruses
  - Component updates and proxy settings
  - Product license setting and registration
  - SNMP trap notifications
  - System log collection
- **Agent-free policy enforcement**—with the "no agent" option, Network VirusWall Enforcer can now provide policy enforcement to endpoints running legacy and non-Windows platforms.
- **Hide agent icon**—administrators can select to prevent the agent icon from displaying on the system tray of endpoints.
- **Product license activation**—Network VirusWall Enforcer can now be activated by entering an Activation Code on the web console and then connecting to the online product registration system.

- **ARP spoofing prevention**—ARP spoofing attacks can leave networks and data severely compromised by giving attackers access to network packets. Attackers can manipulate redirected packets to extract data or compromise intended recipients. Network VirusWall Enforcer provides protection against ARP spoofing through preventive broadcast of legitimate Address Resolution Protocol (ARP) information for critical nodes. It also provides configuration options for detecting possible ARP spoofing activities and terminating applications responsible for these activities.
- **OfficeScan™ 10 and smart scan support**—Network VirusWall Enforcer can now detect OfficeScan 10 on endpoints and determine the component status of clients that are running smart scan cloud-based scanning.
- **Control Manager™ 5.0 support**—Network VirusWall Enforcer can now be managed using Control Manager™ 5.0.

Protection Features and Capabilities

Network VirusWall Enforcer protects against a wide variety of threats focusing on identifying and isolating actual and potential outbreak sources.

Endpoint Policy Enforcement

Network VirusWall Enforcer uses the agent to perform the following checks on endpoints:

- Antivirus Product Scan—checks if the endpoint is running supported antivirus software
- Antivirus Version Scan—checks if the installed antivirus software has the latest pattern
- System Threat Scan—runs a memory scan to check if malware is running on the endpoint and automatically performs cleanup upon detection
- Vulnerability Scan—checks if any installed Microsoft software is not patched for known vulnerabilities
- Registry Scan—checks the registry to identify unwanted and missing registry entries

Network Virus Scan

To prevent worms from spreading, Network VirusWall Enforcer inspects packets that pass through it for known malware code. Using packet scanning, Network VirusWall Enforcer is able to stop network viruses and other types of worms as they attempt to spread to other network segments. It can also clean up and quarantine the endpoints from where the worms spread.

Network Policy Enforcement

Network VirusWall Enforcer can regulate port, instant messenger, and file transfer activity with the following features:

- Application Protocol Detection—checks for activity on specified TCP or UDP ports or ICMP to reject or drop packets or monitor endpoints that use the ports
- Instant Messaging Detection—checks for instant messenger activity, either file transfer activity or all kinds of instant messenger activity
- File Transfer Detection—checks for file transfers using Windows shares, HTTP, or FTP

Network VirusWall Enforcer can be configured to closely monitor endpoints when found responsible for unwanted network activity. It can also drop and reject packets associated with the detected activity.

Threat Mitigation with TDA

Network VirusWall Enforcer works with Trend Micro Threat Discovery Appliance (TDA). TDA can identify endpoints with active threats by gathering and correlating network activity. To mitigate threats identified by TDA and prevent them from spreading, Network VirusWall Enforcer can actively monitor or quarantine endpoints.

ARP Spoofing Prevention

Network VirusWall Enforcer prevents ARP spoofing by broadcasting legitimate ARP information associated with critical nodes. To detect and terminate ARP spoofing malware on endpoints, it monitors applications for outgoing ARP traffic and terminates applications that are sending more than 100 ARP packets per second.

Technologies

Network VirusWall Enforcer is equipped with state-of-the-art antivirus technology. Designed to act as shield for a segment of your network, it can scan and drop infected network packets before they reach your endpoints. It can also prevent vulnerable or infected endpoints from accessing the rest of the network.

Packet Scanning

Using the Network Virus Engine and the Network Virus Pattern, Network VirusWall Enforcer scans every packet entering and leaving a network segment in real-time. Network VirusWall Enforcer is able to recognize network viruses, drop infected packets before they enter the network, and prevent further security compromise. See *Security Risks* on page 1-11 for more information on network viruses and other malware.

Threat Management Agent

In addition to its packet scanning capabilities, Network VirusWall Enforcer uses Threat Management Agent to perform endpoint assessments. The agent can scan for file-based threats, software vulnerabilities, antivirus software, and registry keys to help ensure that endpoints are secure.

Note: Network VirusWall Enforcer supports agent-free policy enforcement. During policy creation, select the "no agent" deployment option to enforce the policy without installing agents on endpoints. This option provides limited enforcement capabilities on endpoints running unsupported platforms.

The agent performs the following policy enforcement tasks:

- Checking for installed antivirus software
- Checking the version of the antivirus pattern
- Scanning for threats, including malware responsible for ARP spoofing
- Checking for unpatched vulnerabilities
- Checking for missing or prohibited registry entries
- Displaying popup notifications
- Checking for prohibited protocols, instant messenger activity, and file transfers

- Cleaning up of infected systems

Platforms Supported by the Agent

The agent version released with Network VirusWall Enforcer has been tested on the following platforms:

- Microsoft™ Windows™ 2000 (including Professional, Server, and Advanced Server editions) with Service Pack 4

  Note: Windows 2000 does not support IPv6 addressing.

- Windows Server™ 2003 (Standard and Enterprise editions) with Service Pack 1 or later
- Windows XP (Home and Professional editions) with Service Pack 2 or later

  Note: IPv6 support is not enabled on Windows XP by default.

- Windows Vista™ (Enterprise, Business, and Ultimate editions)
- Windows Server 2008 (all editions)
- Windows 7 (all editions)
- Windows 8 (all editions)

Note: The agent may be updated to support additional platforms. Refer to the readme provided with new agent releases for the latest information about each agent release.

Agent Deployment Options

When creating a policy, you can define how the agent is deployed. Your choice of deployment method affects the enforcement criteria you can specify on that policy. Network VirusWall Enforcer supports the following agent deployment options:

- **No agent**—this agent deployment method is recommended for organizations with unsupported platforms. With this deployment, only protocol-based antivirus detection, network virus scanning, network application policy assessment, and certain threat mitigation functions are supported.

- **Single-use agent**—installs an agent for assessment and stops the agent service after the assessment is completed. Unless the agent is outdated, Network VirusWall Enforcer will reuse the same agent to perform an assessment on the same endpoint.

Note: On earlier releases of Network VirusWall Enforcer, this deployment option was referred to as the "agentless" option.

- **Persistent agent**—installs an agent that periodically assesses the endpoint and handles threat mitigation requests. This is the default deployment option.

Security Risks

Tens of thousands of malware exist, with more and more coming into existence each day. These threats are known to infect endpoints by exploiting system vulnerabilities. They perform all kinds of malicious behavior, including information theft.

Network Viruses

The strictest definition of a "network virus" describes a type of self-contained malware that spreads from computer to computer without having to create file copies of itself. These viruses exist only as network packets, moving from one computer to another, and as code running in memory. Network VirusWall Enforcer provides protection against these sophisticated threats by scanning network traffic and then identifying the packets that contain code from known network viruses. It can also detect packets that contain generic exploit code used commonly by network viruses to propagate.

While allowing Network VirusWall Enforcer to detect network viruses at the network layer, its packet-scanning capability also allows it to block regular file-based malware as they propagate through the network. It supplements file-based scanning technologies and stops virulent threats before they can spread.

Vulnerabilities

Trend Micro assesses the risks posed by software vulnerabilities by considering the number and the significance of the threats that use them, their potential and actual impact, and the difficulty or ease by which they can be exploited. Vulnerabilities are considered low, moderate, important, critical, or highly critical as described below.

- Highly Critical—vulnerabilities considered highly critical are vulnerabilities associated with at least ten Internet threats, regardless of the impact of these Internet threats. Systems and networks not patched against these vulnerabilities will likely become infected due to the prevalence or sheer variety of associated Internet threats.
- Critical—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—vulnerabilities that compromise vital information and allow unauthorized access to passwords and other valuable data are automatically considered important. Vulnerabilities that compromise the integrity or availability of system resources are also in the same category.
- Moderate—vulnerabilities that are hard to exploit because of default platform or applications settings, auditing, or sheer technical complexity, are considered moderate risk.
- Low-risk—these vulnerabilities either have minimal impact on affected systems or are very difficult to exploit.

ARP Spoofing

Address Resolution Protocol (ARP) spoofing involves sending a fake or "spoofed" ARP message to a network host to trick the host into associating an IP address to the sender's MAC address. This technique can cause the recipient to send traffic intended for another node or host to the sender, which is typically a host controlled by an attacker. As a result, the attacker has access to the misdirected network traffic and can manipulate this traffic for his or her own purposes. For example, attackers can extract confidential data from the misdirected traffic or modify the traffic before forwarding them to their intended recipients.

File-Based Malware

Most malware programs can be classified as file-based—they exist as files in physical drives. Such malware programs include what are commonly known as viruses, Trojans, and worms.

- Viruses—although the term "virus" has been commonly used to refer to malware that can propagate, many security professionals prefer to use this term to refer only to malware that can infect files and thus propagate from file to file. Viruses generally affect executable files and macros in Microsoft™ Office documents.
- Worms—malware programs that can propagate from system to system are generally referred to as "worms". Worms are known to propagate by taking advantage of social engineering through attractively packaged email messages, instant messages, or shared files. They are also known to copy themselves to accessible network shares and spread to other computers by exploiting vulnerabilities. When worms are memory-only or packet-only programs (that is, they are not file based), they are generally referred to as "network viruses".
- Trojans—malware programs that do not have inherent abilities to spread are generally referred to as "Trojan horse programs" or "Trojans". Although unable to spread, Trojans are often found in infected computers after being installed by a worm or by a human attacker. Trojans are known to perform all kinds of malicious activities, including stealing information, opening ports for attackers, and damaging system integrity.

Network VirusWall Enforcer leverages conventional antivirus scanning technology in the TMAgent to check for active file-based malware.

Unprotected Endpoints

Endpoints without antivirus software or those with outdated patterns pose severe risks to overall network security. When allowed to access the Internet or other external resources, these endpoints can serve as infection vectors (the means by which malware programs penetrate the network). Network VirusWall Enforcer can identify these endpoints and isolate them from the network.

Prohibited Network Use

Unregulated user activities on the network can severely compromise security. Depending on the needs of your network, Network VirusWall Enforcer allows you to regulate the following network use:

- Port activity—by regulating port activity, you can control the use of certain applications or protocols.
- Instant messaging—Network VirusWall Enforcer can regulate the use of certain instant messaging applications. You can choose to regulate all activities associated with these applications or only file transfers.

  The following table lists supported instant messaging applications.

TABLE 1-1. Instant messenger support

APPLICATION	VERSION SUPPORT
Windows Live (MSN) Messenger	Supports versions 8.1 and 9. Note that Windows Live Messenger refuses logon attempts when the client is older than version 8.1.
Yahoo! Messenger	Supports 8.1.0.421 or lower; 9.0.0.2018 or higher are not supported
AOL Instant Messenger (AIM)	Supports version 6.5.5.2 or lower; 6.8.8.2 or higher not supported
ICQ	Supports version 6.5.1042 or lower
IRC (mIRC)	Supports mIRC version 6.35 or lower
Pidgin (Gaim)	Supports version 2.5.6 or lower
Gaim	Supports version 2.0.0 Beta 2 and or lower

- File transfers—in addition to regulating file transfers though instant messaging applications, you can regulate file transfers made though the CIFS and Samba protocols, HTTP file transfers, and FTP file transfers.

Enforcement Coverage

The following features let you control when a policy applies to an endpoint or a connection:

- User authentication—during policy creation, you can define whether the policy applies to all users, authenticated users only, or guest users only. Network VirusWall Enforcer assesses an endpoint against the policy only when the specified type of user is logged on to the endpoint.
- Network zones—you can define endpoint groupings or network zones using IP or MAC addresses and VLAN IDs. During policy creation, you can indicate whether the policy applies only to specific network zones. Network zones can also be used to specify IP or MAC addresses that are exempted from policy enforcement.
- URL exception lists—when a policy is matched against an endpoint, Network VirusWall Enforcer can be configured to block network traffic to and from the endpoint. During policy creation, you can specify URL exception lists to ensure that URLs on these lists remain accessible even to noncompliant endpoints. Typically, you will want to exempt URLs to web pages containing antivirus software downloads and vulnerability patches.
- Global endpoint exceptions—you can specify a list of IP or MAC addresses that are exempted from all policy enforcement. All policies will not apply to the endpoints with these IP or MAC addresses. For more information, see *Specifying Globally Exempted Endpoints* on page 3-6.

Visibility

Network VirusWall Enforcer provides status screens, endpoint notifications, and logs to allow end users and administrators to easily access enforcement results.

Endpoint Notifications

When Network VirusWall Enforcer finds that an endpoint is noncompliant, it can send the following notifications to the endpoint:

- Web notifications—this message is displayed on the web browser and is visible only when end users attempt to access a web page while being blocked due to noncompliance.

- Popup notifications—these notifications use either the Windows Messenger service to display messages on a standard Windows message box or the agent to display a balloon message from the agent system tray icon.

  Note: If you have selected to hide the agent system tray icon, any balloon messages from the icon will not display.

- Email notifications—Network VirusWall Enforcer can be configured to send an email to certain addresses whenever it quarantines an endpoint in response to a Threat Discovery Appliance detection.

Status Screens

Use the Summary and Real-time status screens to get a quick overview of the status of policy enforcement and the device.

The Summary screen displays the following information:

- Policy Enforcement Status—provides statistics on policy compliance and violations. Click the number under Violations for more information.
- Threat Mitigation Events—provides statistics on the results of mitigation efforts. Click the number to view additional information.
- Top 5 Policies with Violations—use this information to determine the most common policy violations. Click the number under Violations to view additional information.
- Endpoint Summary—provides statistics on the number of endpoints that are compliant, noncompliant, or quarantined.
- AV Product Detection Status—provides statistics on the number of endpoints with antivirus products. Click **Export** to save the information to a file.
- Component Status—lists the Network VirusWall Enforcer components, the last time they were updated, and their current versions. Use this information to determine whether you have the latest components and if updates are successful.

The Real-time Status screen displays the following information:

- Performance Status—displays CPU usage, memory usage, and concurrent connections
- Interface Configuration Status—displays a graphical view of the current port settings that correspond to the physical port layout

Tip: For detailed information on any web console screen, click the help button while on the screen.

Logs

Logs provide information to help you monitor policy enforcement on your network. During policy creation, you can specify whether log entries are generated for policy violations. You can view these entries later through the web console screens and export them to CSV files.

If Network VirusWall Enforcer is registered to Control Manager, the device automatically sends log entries to Control Manager. The device can also be configured to send logs to up to two syslog servers or save logs on the hard disk.

Network VirusWall Enforcer supports the following logs:

- Event Log—Network VirusWall Enforcer generates an entry on the event log every time it detects an event, such as a virus outbreak, or performs an action, such as a reset or a component update. If you register the device to Control Manager, it automatically sends event log entries to the Control Manager server.
- Network Virus Log—whenever Network VirusWall Enforcer detects a network virus, it creates a network virus log entry. If you register the device to Control Manager, it automatically sends network virus log entries to the Control Manager server.
- ARP Spoofing Log—whenever Network VirusWall Enforcer detects a malware associated with ARP spoofing, it generates an entry on the ARP spoofing log. Consult this log regularly to address any occurrences of this serious security breach.
- Threat Mitigation Log—whenever Network VirusWall Enforcer attempts to respond to a detection by Threat Discovery Appliance (TDA), it generates an entry in the threat mitigation log. If you register the device to Control Manager, it automatically sends threat mitigation log entries to the Control Manager server.

- Endpoint History—whenever Network VirusWall Enforcer matches a policy to an endpoint, it creates an endpoint history entry. If you register the device to Control Manager, you can configure the time interval for sending endpoint history entries to the Control Manager server.

Understanding Endpoints

Network VirusWall Enforcer considers each network host that functions as a packet source and is identified by its own IP address to be an individual endpoint. A network device with more than one network interface card (NIC) and subsequently multiple IP and MAC addresses may be treated by Network VirusWall Enforcer as multiple endpoints, resulting in separate policy matching events.

Based on assessment results, endpoints can be generally categorized as one of the three following types:

- Compliant—endpoints that have not violated any policies.
- Noncompliant—endpoints that have violated at least one policy; the most common tasks associated with noncompliant endpoints are blocking or monitoring them. Monitored endpoints have unhampered access to the network, but may be reassessed against policies sooner than compliant endpoints.

Note: When creating a policy, you can define different reassessment schedules for compliant and noncompliant endpoints.

- Blocked—endpoints that have violated a policy and are restricted from accessing network resources. If an endpoint is blocked, the device drops all packets directed towards or coming from the endpoint. The only types of traffic a blocked endpoint can receive are notifications and remedy-related traffic.
- Quarantined—blocked endpoints that can only be released and allowed access to the network through the web console. Unless released, quarantined endpoints remain blocked regardless of subsequent assessment results.

Endpoints may also be classified into the following categories depending on current assessment status:

- Assessing—endpoints that are currently being checked for policy compliance

- Unsupported OS—endpoints that cannot be assessed because they are running on unsupported platforms

Assessment Intervals

Noncompliant endpoints, by default, are assessed more frequently to help increase compliance across the network. The following table shows the different reassessment schedules and the factors that may trigger them.

TABLE 1-2. Endpoint assessment intervals

ASSESSMENT TYPE	DEPLOYMENT METHOD	COMPLIANT	NONCOMPLIANT
Default interval		1 day	15 minutes
Agent-based assessments	Persistent agent	1/2 of configured interval	1/2 of configured interval
	Single-use agent	As configured, triggered by traffic	As configured, triggered by traffic
	No agent	N/A	N/A
Device-based assessments	All types	Real-time, triggered by traffic	Real-time, triggered by traffic

SNMP Support

Simple Network Management Protocol (SNMP) is set of communication 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.

For instructions on how to configure SNMP settings, see *Configuring SNMP Settings* on page 5-7.

MIB 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 NMSs 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 1-3 enumerates the SNMP specifications supported by Network VirusWall Enforcer.

TABLE 1-3. Supported SNMP agent 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

TABLE 1-3. Supported SNMP agent specifications (Continued)

TRUSTED NETWORK MANAGEMENT STATIONS (NMS)	Allows up to 255 specific network management station IP addresses to access the agent

Table 1-4 enumerates the supported SNMP trap specifications.

TABLE 1-4. Supported SNMP trap specifications

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

SNMP Trap Limitations

The following SNMP traps limitations exist:

- Version supported: 2c
- Community names—one community name allowed; 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 trap messages, Network VirusWall Enforcer sends the following traps:

- Cold start—SNMP agent enabled
- Link down—port connection down
- Link up—connection to port established

- Authentication failure—three consecutive attempts to log on to the Preconfiguration console during the same local or remote SSH session were unsuccessful
- Shutdown—SNMP agent disabled

Note: This trap is also sent if Network VirusWall Enforcer shuts down while the SNMP agent is enabled. No trap is sent if the device shuts down while the agent is disabled.

- Boot to factory default—boot to default rescue partition. This sends an SNMP trap every minute.
- Boot to previous partition—started device using previous partition in response to keyboard commands. This SNMP trap message is sent after the device has started.
- Turn on/off OPP—whenever Control Manager sends an OPP command to Network VirusWall Enforcer, an SNMP trap indicates whether or not OPP support is enabled.

SNMP Agent Messages

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

- nvwScanCurrConn—concurrent scan connections.
- nvwScanCurrMem—current memory use for scans.
- nvwPolicyCurrConn—concurrent number of endpoints with the Threat Management Agent (TMAgent).

VLAN Support

A virtual local area network (VLAN) is a network consisting of endpoints that are not on the same physical 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. 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 which VLAN the packet belongs. When other switches receive the packet, they determine VLAN membership implicitly using MAC address information or explicitly using a tag that the first switch adds to the MAC address header.

Network VirusWall Enforcer 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 to the same VLAN (tagged or non-tagged). This will help ensure effective communication between the Control Manager server and Network VirusWall Enforcer.

Chapter 2

Setting Up the Device

After installing Network VirusWall Enforcer and performing all preconfiguration tasks described in the *Installation and Deployment Guide*, there are a number of tasks you need to perform to ensure that everything is properly set up.

This chapter describes how to ensure that Network VirusWall Enforcer is connected to the network and that it is activated and fully updated. It discusses the following topics:

Management Options

Network VirusWall Enforcer provides a Preconfiguration console and a web console for configuring or managing the device.

Preconfiguration Console

The Preconfiguration console lets you configure the device before deploying it to your network. Access the console to set the most basic device settings, including port functions and IP address configuration.

You can view the Preconfiguration console directly by connecting a keyboard and a VGA monitor to the device or remotely using an SSH client.

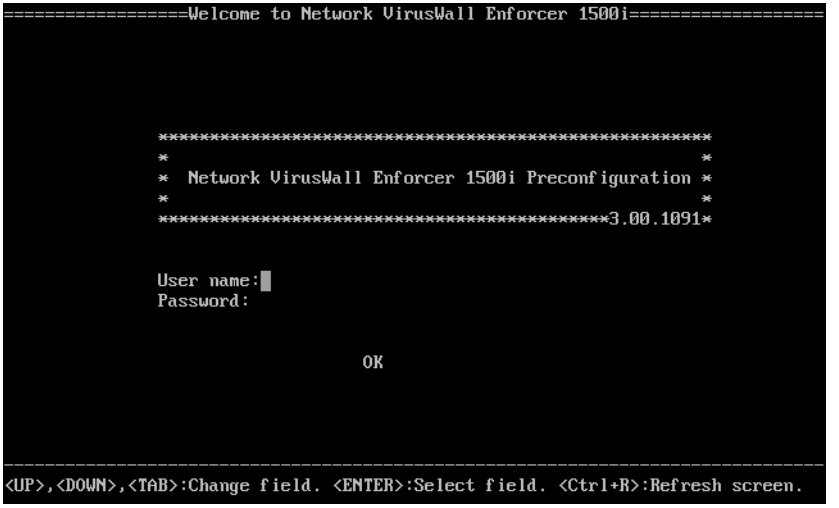


FIGURE 2-1. The Preconfiguration console logon screen

Accessing the Preconfiguration Console Remotely

To access the preconfiguration console remotely, you need an SSH client like PuTTY, which you can download here:

http://www.putty.org/

Consider the following when accessing the console remotely:

- SSH console access must be enabled from the web console. See *Configuring Access Control* on page 2-12.
- Connect to the device management IP address using SSH.
- When prompted to log on to the Linux root console, use the user name "root" and a blank password.
- Certain options are not available when accessing the Preconfiguration console remotely. For example, you cannot disable SSH connections. Also, you will not be able to import or export configuration information or export an HTTPS certificate when.

Web Console

The Network VirusWall Enforcer web console provides a browser-based interface for managing policies and other aspects of the device. The console lets you react quickly to network virus emergencies from nearly anywhere.

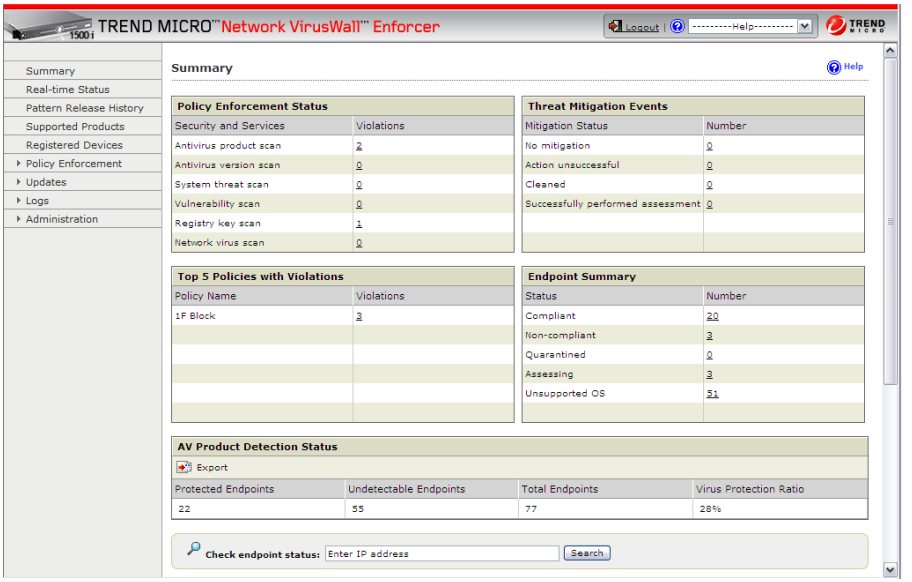


FIGURE 2-2. Network VirusWall Enforcer web console

After preconfiguration, the web console lets you perform the following administrative tasks:

- Analyze your network's protection against viruses
- View the Pattern Release History
- View the list of supported antivirus products
- Update Network VirusWall Enforcer components and settings
- Enforce security policies
- View and manage logs
- Configure certain device settings

Comparing the Consoles

The following table lists the differences between the consoles:

TABLE 2-1. Comparison of the Network VirusWall Enforcer consoles

TASK	PRECONFIGURATION CONSOLE	WEB CONSOLE
Configure port functions	✓	✗
Configure interface speed and duplex mode	✓	✗
Configure IP address settings	✓	✓
Manage policies	✗	✓
Configure proxy settings and updates	✗	✓
Manage access control	✓	✓
Manage administrative accounts	✗	✓
Monitor device events, status, and summaries	✗	✓
Configure notifications	✗	✓
Perform system rollback/restore	✓	✗
Register the device to Control Manager	✓	✗

TABLE 2-1. Comparison of the Network VirusWall Enforcer consoles (Continued)

TASK	PRECONFIGURATION CONSOLE	WEB CONSOLE
Restart and shut down device	✓	✓
View device information (CPU and memory usage)	✓	✓
View interface configuration	✓	✓

Logging on to the Web Console

If you have preconfigured the device as described in the *Installation and Deployment Guide*, you can log on to the web console using the management IP address or host name you have specified for the device.

To access the Network VirusWall Enforcer web console, use Microsoft™ Internet Explorer™ 6.0 or later. The console address is:

- **IPv4:** `http://<device IP address or host name>`
- **IPv6:** `http://<[device IP address] or host name>`

Connecting to the Network

When the management IP address, bridge IP address, and static route settings are correct, Network VirusWall Enforcer is able to connect to the network and packets to and from the device are efficiently routed.

Note: You can configure these settings on both the web console and the Preconfiguration console.

Management IP Address

The management IP address lets you access the web console and manage the device. For instructions, see *Configuring IP Address Settings* on page 2-10.

Note: If you have a dual-stack environment, ensure that you specify both IPv4 and IPv6 address settings.

Bridge IP Addresses

To effectively deploy the agent, provide remediation measures, and perform other policy enforcement tasks, Network VirusWall Enforcer requires direct and unrouted communication between itself and protected network segments. Network VirusWall Enforcer may use the management IP address to communicate with all endpoints. However, direct and unrouted communication is possible only if:

- The management IP address is *not* bound to a management port (ports 1-2); and
- All the protected endpoints are in the same segment as the management IP address.

Specify a bridge IP address for each protected segment with which device cannot directly communicate. The bridge IP addresses must be in the same segment to avoid routing and ensure effective policy enforcement.

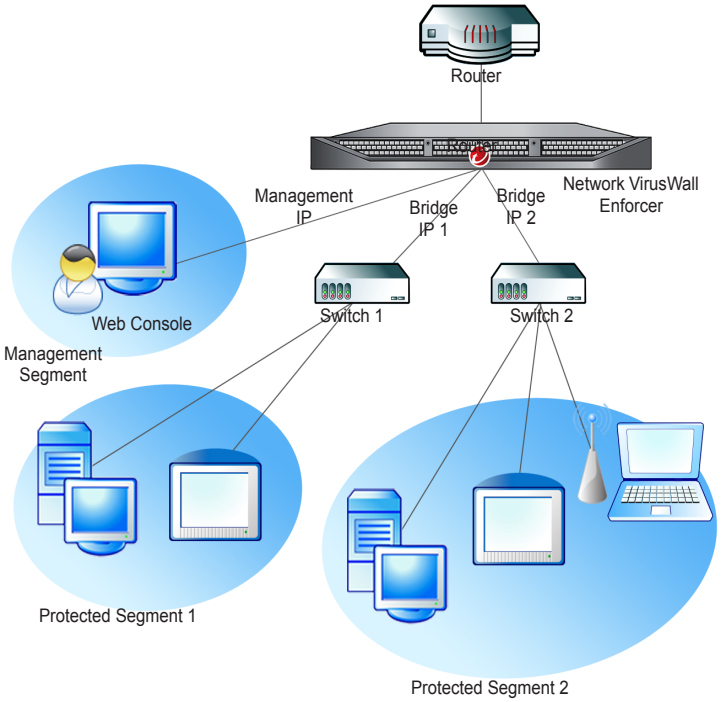


FIGURE 2-3. Bridge IP addresses and protected segments

Static Routes

A static route defines a specific router IP address that Network VirusWall Enforcer should use to reach endpoints in a particular segment. A static route is required for each router between Network VirusWall Enforcer and a protected segment or segments. You can define up to 50 static routes.

Note: To add a static route, add a bridge IP address for each segment first. Ensure that you do not delete bridge IP addresses that are being used by your static routes.

To allow Network VirusWall Enforcer to protect endpoints in segment 1 in the following diagram, the following settings must be defined:

- A bridge IP address (bridge IP 1) for segment 1. This IP address should be in the same segment as the upper interface of router 2.
- A static route pointing to segment 1 and router 2, specifically the IP address of the upper interface of router 2 facing switch 1.

Note: You can bind a bridge IP address to a bridge with a specific VLAN ID. You can add up to 128 bridge IP addresses.

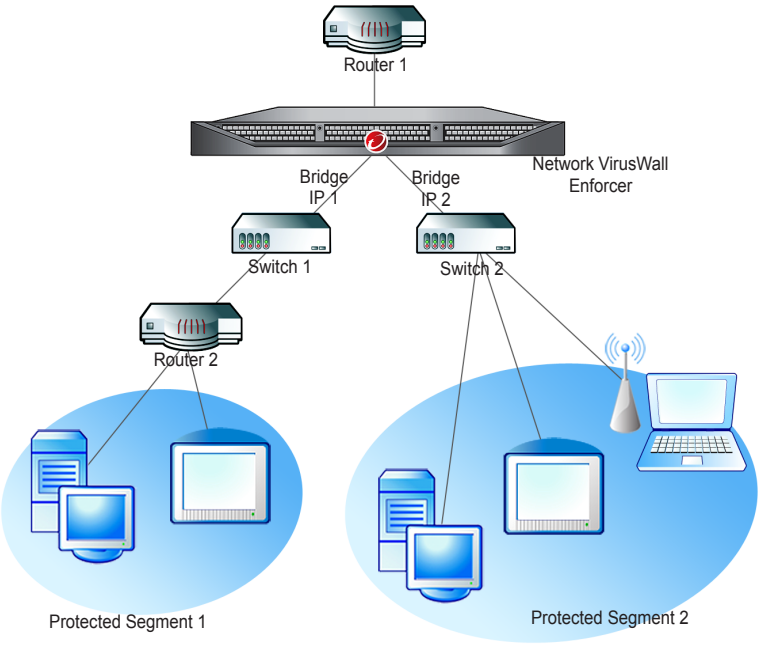


FIGURE 2-4. Deployment requiring a static route

Configuring IP Address Settings

Configure the management IP address, bridge IP address, and static routes to ensure that Network VirusWall Enforcer and efficient routing is established.

Note: Specify IPv4 settings if you have deployed Network VirusWall Enforcer to an IPv4 or a dual-stack environment. Specify IPv6 settings if you have deployed Network VirusWall Enforcer to an IPv6 or a dual-stack environment.

To configure IP address settings:

1. Click **IP Address Settings** in the **Administration** menu.
2. Select to allow Network VirusWall Enforcer to obtain IP address settings from a DHCP server or configure the settings manually.
3. Click the **Bridge IP Address** tab to add or delete bridge IP addresses. Bridge IP addresses allow the device to access endpoints in another segment.
4. Select the **Static Routes** tab to add or delete static routes. You can add up to 50 static routes.

Note: For more information on bridge IP addresses and static routes, see *Bridge IP Addresses* on page 2-7 and *Static Routes* on page 2-9.

Securing the Device

To secure the device, perform the following tasks:

- Change the password of default accounts to secure the console. See *Changing Account Passwords* on page 2-11.
- Control access to the device. See *Configuring Access Control* on page 2-12.

Changing Account Passwords

Secure the console by immediately changing the passwords to the default accounts, "admin" and "poweruser".

To change the password for an account:

1. Click **Administration > Account Management**. The Account Management screen appears.
2. Click the name of the account to edit the account.

3. Type the new password and retype it for confirmation.

Note: Trend Micro strongly recommends changing all default passwords as soon as you are able to access the web console. A strong password is at least 8 characters long and a combination of upper and lower case letters, numbers, punctuation marks, and other special characters. Avoid dictionary words, names, and dates.

4. Click **Save**.

Configuring Access Control

Reduce the risk of unauthorized web console access by granting access only to certain IP addresses. You can also enable or disabled remote SSH access to the Preconfiguration console. You can have up to 10 concurrent HTTP web console sessions and up to 10 concurrent HTTPS sessions.

To configure Access Control:

1. Click **Access Control** in the **Administration** menu.
2. To allow SSH console access, select **Enable SSH console access**.

Tip: With SSH access enabled, you can access the Preconfiguration console using any SSH client.

3. To restrict IP addresses, select **Enable IP address restriction**. You can add up to 20 IP addresses to this list.
   a. Type an IP address in the **IP address** text box.
   b. Type a comment (optional). Use this field to provide more information about the IP address.
   c. Click **Add to** add the IP address.
   d. Add more IP addresses as needed.

e. Click **Save**.

Note: When you enable IP address access restriction, you will be logged off from the web console and will need to log on again. If you did not add your current IP address to the access control list, you will be prevented from accessing the web console and from logging on.

Activating and Updating the Device

Ensure that the device can connect to the Internet and then activate your license. After activation, you will be able to perform updates. Perform the following procedures to activate and update your device:

- If necessary, configure proxy server settings so the device can connect to the Internet. See *Configuring Proxy Settings* on page 2-14.
- Activate the device license. See *Activating the Device License* on page 2-15.
- If you are using a Control Manager server as a local update server, specify the URL of the server so the device can download updates from this server. See *Specifying the Update Source* on page 2-14.
- Perform an update of Network VirusWall Enforcer pattern and program files. You may need to reset the device after the update. See *Updating Components* on page 2-17.
- Schedule automatic pattern and engine updates. See *Scheduling Component Updates* on page 2-18.

Update Options

Network VirusWall Enforcer components are software modules that comprise the Network VirusWall Enforcer operating system. To help ensure up-to-date protection, update all the components regularly.

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

- Manually—instruct Network VirusWall Enforcer to connect directly to the update source, download, and then apply the latest components. Use the **Manual Update** option on the web console to perform this type of update.

- Automatically—configure Network VirusWall Enforcer to automatically connect to the update source, download, and then apply the latest components. Use the **Scheduled Update** option on the web console to set this type of update.

Configuring Proxy Settings

Specify the necessary proxy server settings to ensure that Network VirusWall Enforcer can connect to the Internet. Network VirusWall Enforcer connects to the Internet during license registration and when downloading updates.

To configure proxy settings:

1. Click **Proxy Settings** from the **Administration** menu.
2. Select **Use a proxy server to connect to the Internet**.
3. Select **HTTP**, **SOCKS 4**, or **SOCKS 5** for the protocol.
4. Type the **Server name** or **IP address** and the **Port**.
5. Type the **User name** and **Password** under **Proxy server authentication** if the proxy server requires authentication.
6. Click **Save**.

Note: To ensure that Network VirusWall Enforcer connects to the designated update source directly, without going through the proxy server, select **Do not use the proxy server to download updates**. This option does not affect Pattern Release History downloads.

Specifying the Update Source

By default, Network VirusWall Enforcer obtains updates from Trend Micro ActiveUpdate servers, but you can configure the device to connect to a local update source.

Use the Update Settings screen to set the update source from which Network VirusWall Enforcer obtains the latest components.

To set the update source:

1. Click **Update Source** from the **Update**s menu.
2. Select **Trend Micro ActiveUpdate Server** or select **Other update source** and type the URL of the update source.

Note: The update source must be a valid URL that begins with `http` or `https`. When using a URL with a literal IPv6 address, enclose the IPv6 address in square brackets.

Activating the Device License

For continuous protection, ensure that your Network VirusWall Enforcer license has been activated and that it remains valid.

To activate your device license:

1. Click **Product License** in the **Administration** menu.
2. Click **Update Information** to get the latest license information for your device.
3. If your license has not been activated or it has expired, supply a new Activation Code by clicking **New Activation Code**.

Updatable Components

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

TABLE 2-2. Updatable components

COMPONENT	DESCRIPTION
Network Virus Engine	Scans all packets passing through Network VirusWall Enforcer. The Network Virus Engine specifically searches for network viruses.
Network Virus Pattern	Contains a regularly updated database of network virus packet information. Trend Micro often updates the network virus pattern file to help ensure Network VirusWall Enforcer can identify new network viruses.
Damage Cleanup Engine (32-bit and 64-bit)	Scans endpoints for and repairs damage caused by malware. The Damage Cleanup Engine can also check for vulnerabilities.
Damage Cleanup Pattern	Contains cleanup information that is used by the Damage Cleanup Engine to identify malware and remove them from endpoints.
Vulnerability Pattern (32-bit and 64-bit)	Contains information about vulnerabilities in popular software products and is used to identify vulnerabilities in endpoints.
Forensic Clean Template	Contains information used by the Forensic Clean Engine to locate and remove threats detected by Threat Discovery Appliance.
Forensic Clean Engine	Locate and removes threats detected by Threat Discovery Appliance.
Anti-rootkit Driver (32-bit and 64-bit)	Detects rootkits, sophisticated malware programs that are able to hide from Windows APIs and the detection tools that leverage them.

TABLE 2-2. Updatable components (Continued)

COMPONENT	DESCRIPTION
Pattern Release History	Contains information about the latest patterns for supported antivirus products. Network VirusWall Enforcer uses this information to check whether endpoints are running the latest patterns. **Note:** You can specify a different update schedule for updating the Pattern Release History.
Antivirus Product Detection Engine	Scans endpoints to determine whether they are running supported antivirus software.
Threat Management Agent	The main component of the agent, which is used by Network VirusWall Enforcer to perform certain tasks on the endpoint.
Program file	**Note:** The Network VirusWall Enforcer program, also referred to as the image, which includes the operating system, system programs, and all components necessary to get Network VirusWall Enforcer functioning properly. When you manually update the program file, Network VirusWall Enforcer prompts you to reboot the device if necessary. Otherwise, for scheduled program file updates, the device automatically reboots after the update when necessary.

Tip: Use the Summary screen on the Network VirusWall Enforcer web console to check whether selected components have been updated.

Updating Components

For optimum security and product performance, ensure that all components are current by performing a manual update.

To perform a manual update:

1. Click **Manual** in the **Updates** menu.
2. Select the **Component** check box to update all components.
3. Click **Update**.

Note: If the Program file component is updated, you may be prompted to reset the device.

Scheduling Component Updates

Set an update schedule to allow Network VirusWall Enforcer to update and obtain the latest components automatically from the update source.

To set an update schedule:

1. Click **Scheduled** in the **Updates** menu.
2. Select the components to automatically update.
3. Specify the update schedule for the selected components.
4. Specify the update schedule for the Pattern Release History.

Note: Consider any bandwidth issues that may occur during scheduled updates. Trend Micro recommends updating pattern files at least once a day.

5. Click **Save**.

Installing Hot Fixes, Patches, and Service Pack

Trend Micro may provide the following releases to fix bugs or enhance the device:

- Hot fix—a small release designed to address a few very specific issues
- Patch—a compilation of earlier hot fix releases; may provide minor enhancements
- Service pack—designed to provide several enhancements; earlier hot fix or patch releases may also be included

To apply a hot fix, a patch or a service pack:

1. Click **Patch** in the **Updates** menu.
2. Specify the **Installation file**. Click **Browse** to navigate to the file.
3. Click **Install**.

To view installed hot fixes:

1. Click **Patch** in the **Updates** menu.
2. Refer to the information displayed under **Patching History**.

Registered Devices

This page displays the IP addresses and host names of the Threat Discovery Appliance (TDA) or Deep Discovery Inspector devices that are registered to Network VirusWall Enforcer. TDA and DDI devices work with Network VirusWall Enforcer to provide Threat Mitigation, which can identify new threats in suspicious endpoints and clean infected endpoints.

Chapter 3

Preparing for Policy Enforcement

After setting up the device, prepare Network VirusWall Enforcer for policy creation and deployment. This chapter discusses the following topics:

Configuring HTTP Detection Settings

Provide the ports used in your network for HTTP communication. The specified ports allow Network VirusWall Enforcer to block or monitor HTTP traffic.

Note: Network VirusWall Enforcer checks ports 80, 443, and 8080 by default.

To add an HTTP detection port:

1. Click **Policy Enforcement** > **HTTP Detection Settings**.
2. Type a number to specify a port.
3. Type a description of the port under **Comment**.
4. Click **Add to** to add the specified port.
5. Click **Save**.

Configuring LDAP Authentication Settings

LDAP settings define how Network VirusWall Enforcer authenticates endpoint users for policy enforcement.

Before configuring LDAP settings, note the following:

- 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 and the LDAP server is not encrypted.
- Kerberos authentication is not supported in IPv6 networks. When using Kerberos authentication, both the LDAP and the KDC server addresses must be IPv4 addresses.

To configure LDAP server settings:

1. Click **LDAP Settings** in the **Administration** menu. The LDAP Settings screen displays.
2. Select **Use Microsoft Active Directory** or **Use OpenLDAP**.

Note: Network VirusWall Enforcer supports single sign-on (SSO) to the Internet if you select **Use Microsoft Active Directory**.

---

3. Select the authentication method. OpenLDAP supports Simple, Kerberos, and Digest MD5 authentication, while Active Directory only supports Simple and Kerberos authentication.
4. Specify the following:
   - **LDAP server location**—type an FQDN, such as www.trendmicro.com, or an IP address
   - **LDAP server port**—for example, 389
   - **Base distinguished name**—type the DN setting, for example, dc=trend and dc=com
   - **KDC server location**—type an FQDN, such as www.trendmicro.com, or an IP address
   - **Default realm**—for example, TREND.COM
   - **Default domain**—for example, TREND.COM
   - **KDC principal name**—KDC principal name. This setting is only used for Microsoft Active Directory 2008.
   - **KDC server port**— provide if applicable; for example, 88
5. Depending on your security policies, select **Enable single sign-on (SSO) to the Internet**. This option is available only if you are using Active Directory.
6. Click **Save.**

About Single Sign-On (SSO)

Depending on your security policy settings, you can configure Network VirusWall Enforcer to allow single sign-on to the Internet for users using their Active Directory account. This means that once a user signs on to their computer with their Active Directory credentials, they no longer need to sign on through Network VirusWall Enforcer to connect to the Internet.

Keep the following in mind when enabling single sign-on (SSO):

- SSO only works with a persistent agent deployment.
- SSO does not work when an endpoint is new to Network VirusWall Enforcer and it has no records on the device. This occurs when the agent has not been installed on the endpoint. Users of these endpoints will continue to see the authentication page when attempting to access the Internet.
- SSO does not support LDAP referrals.

Defining URL Lists

During policy creation, you can specify URL lists as exceptions to enforcement. URLs in these lists remain accessible even to endpoints found in violation of the policy.

Before creating policies, define the URL lists that you will need. URL lists typically include URLs of update sites for security software and Microsoft products. It can also include the download or installation page for the security software required on your network. Each list can include up to 64 URLs.

To add a URL List:

1. Click **Policy Enforcement > URL Lists**.
2. Click **Add**. The Add URL List screen displays.
3. Type up to 30 characters for the name of the URL list.
4. Type an optional comment. Comments can be up to 50 characters long.
5. Type a valid IPv4 or IPv6 URL. Use wildcards (*) to specify multiple URLs.

Note: When specifying an IPv6 URL with a literal IP address, enclose the IP address in square brackets.

6. Click **Add to** to add the specified URL to the list.
7. Add more URLs to the list as necessary.
8. Click **Save**.

Defining Network Zones

Network zones are predefined IP and MAC address groupings that allow you to manage policy coverage. If you want to apply different security policies to different sets of endpoints, organize these endpoints into different network zones. During policy creation, you can specify whether to apply a policy to all endpoints or specific network zones.

To create a network zone:

1. Click **Network Zones** in the **Policy Enforcement** menu.
2. Click **Add**. The Add Network Zone screen displays.
3. In the **General** tab, type up to 30 characters for the name of the network zone.
4. Type an optional comment. Comments can be up to 50 characters long.
5. Specify the IP or MAC addresses for the network zone.

Note: Use a comma to separate each address or range. You can specify up to 64 IP or MAC addresses or address ranges.

---

6. Click **Add to**. The IP or MAC address is added to the list.
7. Add more IP or MAC addresses as necessary.
8. Click the **Interfaces/VLANs** tab to bind zones to VLANs and device specific interface ports.
   a. Select interface ports to bind the zone to.

Note: Selecting no ports is the same as selecting all ports. If no port is selected or all ports are selected, the zone is not bound to particular ports.

---

   b. Specify the VLAN Settings. Select from all tagged and untagged VLAN IDs, all tagged VLAN IDs, or specific VLAN IDs.

Note: When specifying multiple VLAN IDs, separate each ID with a comma. You can specify up to 32 VLAN IDs.

9. Click the **Exception** tab to specify exceptions to this network zone. Exceptions are MAC or IP addresses that are not covered by the network zone, even when you have added them implicitly as part of an address range in the **General** tab.

Note: You can add up to 64 IP or MAC addresses or address ranges to the exception list.

10. Click **Save**.

Specifying Globally Exempted Endpoints

The global endpoint exception list identifies the endpoints that are not assessed against any policy. Use the list to ensure that certain endpoints are not blocked by the device. You can add up to 64 global endpoint exceptions.

To add to the global endpoint exception list:

1. Click **Policy Enforcement** > **Global Endpoint Exceptions** in the **Policy Enforcement** menu. The Global Endpoint Exceptions screen displays.
2. Select **IP address/range** or **MAC address**.
3. Type the IP or MAC addresses or the range in the text box.

Note: Use a comma (,) to separate each address or address range. To specify a range, use a hyphen (-).

4. Click **Add to**. The specified address or range is added to the list.
5. Add more addresses or ranges as needed.
6. Click **Save**.

Specifying OfficeScan Detection Ports

If your organization has Trend Micro™ OfficeScan™ deployed, specify the port or ports used by OfficeScan clients to listen for server commands. These ports can be used by Network VirusWall Enforcer to detect the OfficeScan client on endpoints.

To specify the OfficeScan detection ports:

1. Click **OfficeScan Settings** in the **Policy Enforcement** menu.
2. Specify the port numbers for detecting OfficeScan. You can specify up to 10 ports, separating each port with a comma (,).
3. Click **Save**.

Specifying Remote Login Accounts

To allow Network VirusWall Enforcer to remotely log on to endpoints and install the agent silently, you must configure remote login accounts. You can add up to five remote login accounts, which will be authenticated using the configured LDAP settings.

Note: To ensure that Network VirusWall Enforcer successfully installs the agent, use an account that has administrator rights on protected endpoints, such as a domain administrator account.

To add a remote login account:

1. Click **Policy Enforcement** > **Remote Login Accounts**.
2. Click **Add**.
3. Select **Enable this account**.
4. Type the following information:
   - **User ID**—user name of the account
   - **Password**—password of the account
   - **Confirm**—retype the password
   - **Comment**—add an optional note about the account
5. Click **Save**.

Configuring Notifications

Network VirusWall Enforcer can send notifications using the following media to inform either endpoint users or administrators about policy violations or related events.

TABLE 3-1. Notification media

MEDIA	TARGET	DESCRIPTION
Web	Endpoint user	Web notifications are displayed when a blocked or quarantined endpoint attempts to access a web page or other remote resources using their web browser.
Popup	Endpoint user	Popup notifications are displayed at the endpoint immediately after a policy is violated, regardless of the action that Network VirusWall Enforcer is set to take. Popup notifications can be set to display as a standard Windows message box or a balloon notification from the agent icon on the taskbar. Whether or not popup notifications display can be configured individually for each section of a policy.
Email	Administrators	Email notifications are sent to inform administrators about quarantined endpoints. Email notifications are centrally enabled or disabled and apply to all policies.

Web Notifications

When a quarantined or blocked endpoint attempts to access a web page or other remote resources using a web browser, Network VirusWall Enforcer can display one of the following notifications on the web browser.

TABLE 3-2. Types of web notifications

NOTIFICATION	PURPOSE
User Login	Prompts the endpoint user to specify domain credentials.
Performing Endpoint Assessment	Indicates that the endpoint is being assessed against applicable policies.
Network Worm	Indicates that the endpoint has been quarantined due to malicious code detected in its outgoing traffic.
Outbreak Prevention Policy Started	Indicates that the endpoint is being blocked due to a violation of the Outbreak Prevention Policy that has been deployed by Control Manager.
No Antivirus Product Detected	Indicates that the endpoint is being blocked because it does not have supported antivirus software.
Registry Key Scan	Indicates that the endpoint is being blocked because it does not have required registry entries or contains unwanted entries.
Antivirus Product Has Outdated Pattern	Indicates that the endpoint is being blocked because it has an outdated antivirus pattern
Vulnerability Detected	Indicates that the endpoint is being blocked because it has unpatched software vulnerabilities.
Threat Detected	Indicates that the endpoint is being blocked because it has actively running malware.

TABLE 3-2. Types of web notifications

NOTIFICATION	PURPOSE
User Login Unsuccessful	Informs the endpoint user that the attempt to log on to the domain has failed.
Threat Mitigation	Indicates that the endpoint is being blocked because of suspicious network activity detected by Threat Discovery Appliance.
Manual Quarantine	Indicates that the endpoint has been manually placed in quarantine by an administrator.

Popup Notifications

Network VirusWall Enforcer can be configured to display the following popup notifications on the endpoint whenever a policy violation is detected.

TABLE 3-3. Types of popup notifications

NOTIFICATION	PURPOSE
Antivirus Program Scan	Indicates that the endpoint has violated policy by not having supported antivirus software.
Antivirus Version Scan	Indicates that the endpoint has violated policy by having an outdated antivirus pattern.
System Threat Scan	Indicates that active malware has been found on the endpoint.
Vulnerability Scan	Indicates that unpatched software vulnerabilities have been found on the endpoint.
Registry Key Scan	Indicates that the endpoint is missing required registry entries or contains unwanted entries.

TABLE 3-3. Types of popup notifications

NOTIFICATION	PURPOSE
Network Virus Scan	Indicates that malware code has been found in network traffic from the endpoint.
Threat Mitigation	Indicates that suspicious network activity by an application on the endpoint has been detected by Threat Discovery Appliance.
ARP Spoofing Monitoring	Indicates that ARP spoofing malware has been found on the endpoint.

Email Notifications

Network VirusWall Enforcer currently supports the following email notification:

- Quarantined for TDA—indicates that an endpoint has been quarantined in response to suspicious activity detected by Threat Discovery Appliance.

Enabling or Disabling Notifications

The following table summarizes the default notification enable/disable settings and how you can change these settings.

TABLE 3-4. Enable/Disable Settings of Notifications

NOTIFICATION MEDIUM	DEFAULT SETTING	MODIFYING THE DEFAULT SETTING
Web	Enabled	Cannot be disabled; displayed during web access if endpoint is blocked or quarantined
Popup	Disabled	Independently enabled or disabled for each section of every policy; see *Overview of Policy Sections* on page 4-8.
Email	Disabled	Enable or disable each email notification type under **Notifications > Administrators**. **Note:** For email notifications to be sent successfully, email settings must be properly configured. See *Email notification settings* on page 3-19.

Notification Tags

To customize notification format and content, use the supported formatting and variable tags.

Formatting Tags for Web Notifications

The following table lists the supported HTML formatting tags for web notifications.

TABLE 3-5. Supported formatting tags for web notifications

TAG	DESCRIPTION
<blockquote>	Defines a long quotation
<p>	Defines a paragraph
 	Inserts a single line break
<pre>	Defines preformatted text
	Makes text bold
	Aligns the text to the center
	Allows the hooking of a string of text and applying styles to the text
	Defines an unordered list
	Defines an ordered list
	Defines a list item
<table>	Defines a table
<tr>	Defines a table row
<th>	Defines a table header
<td>	Defines a table cell
<a>	Defines an anchor
<img>	Defines an image object

TABLE 3-5. Supported formatting tags for web notifications

TAG	DESCRIPTION
<i>	Renders text in italics
<b>	Renders text in bold
<font>	Changes the font face, size, and color of the text

Variable Tags for Web Notifications

Use the following variable tags to customize the content of web notifications.

TABLE 3-6. Supported variable tags for web notifications

TAG	DESCRIPTION
<%=PRODUCT_NAME%>	Name of the product
<%=BTN_REASSESS%>	Reassess button
<%=NETWORK_WORM%>	Name of the malware detected by Network Virus Scan
<%=IP%>	Endpoint IP address
<%=HOSTNAME%>	Endpoint host name
<%=MAC%>	Endpoint MAC address
<%=REG_KEY_MISSING%>	Missing registry key
<%=REG_KEY_EXIST%>	Unwanted registry key
<%=AV_PRODUCT%>	Antivirus software found
<%=AV_PATTERN_VER%>	Current antivirus pattern version
<%=AV_BASELINE_PATTERN_VER%>	Oldest allowable pattern version

TABLE 3-6. Supported variable tags for web notifications

TAG	DESCRIPTION
<%=VA_PATCH_REQUIRE%>	Missing software patch
<%=DCS_NOT_CLEAN_VIRUS%>	Uncleanable active malware
<%=AUTH_RESULT_MSG%>	Authentication result

Variable Tags for Popup Notifications

You can customize the content of popup notifications using the following variable tag:

<%=SERVER_HOSTNAME%>

This variable tag is replaced with the IP address of the Network VirusWall Enforcer device.

Variable Tags for Email Notifications

Use the following variable tags to customize the content of email notifications.

TABLE 3-7. Supported variable tags for email notifications

VARIABLE TAG	DESCRIPTION
<%=ENDPOINT_IP%>	Endpoint IP address
<%=ENDPOINT_HOSTNAME%>	Endpoint host name
<%=ENDPOINT_MAC%>	Endpoint MAC address
<%=BLOCK_TIME%>	Date and time endpoint was quarantined
<%=VLAN_ID%>	Endpoint VLAN
<%=DETECT_NAME%>	Name of the detected threat
<%=DETECT_ENGINE%>	Detection engine used

TABLE 3-7. Supported variable tags for email notifications

VARIABLE TAG	DESCRIPTION
<%=TRAFFIC_DIRECTION%>	Whether traffic is incoming or outgoing relative to the endpoint
<%=RISK_TYPE%>	Threat type
<%=RISK_PROTOCOL%>	Port where the malicious packet was found
<%=RULE_ID%>	Rule used to detect the threat
<%=SUSP_BEHAVIOR%>	Suspicious network activity
<%=SOURCE_IP%>	IP address of the traffic source
<%=SOURCE_HOSTNAME%>	Host name of the traffic source
<%=SOURCE_PORT%>	Port of source traffic
<%=SOURCE_MAC%>	MAC address of the traffic source
<%=SOURCE_GROUP%>	Workgroup of the traffic source
<%=DEST_IP%>	IP address of the traffic destination
<%=DEST_HOSTNAME%>	Host name of the traffic destination
<%=DEST_PORT%>	Port of traffic destination
<%=DEST_MAC%>	MAC address of the traffic destination
<%=DEST_GROUP%>	Workgroup of the traffic destination
<%=NVWE_IP%>	IP address of the Network VirusWall Enforcer device

Customizing Notification Content

Customizing Web and Popup Notification Content

Both web and popup notifications are targeted at endpoint users. Customize these notifications if you want to provide information that is important to endpoint users in your organization.

Tip: For the list of formatting and variable tags that you can use with notifications, see *Notification Tags* on page 3-12.

To customize web and Popup notification content:

1. Click **Policy Enforcement** > **Notifications**. The **Endpoint** tab is selected by default.
2. Click the type of web or popup notification you want to customize. For descriptions of each notification type, see *Table 3-2. Types of web notifications* and *Table 3-3. Types of popup notifications*.
3. Modify the message. For web notifications, you can use up to 4096 characters. For popup notifications, you can use up to 130 bytes. Alphanumeric characters consume one byte, while special and East Asian characters can require up to four bytes.

   Note: If you use double-byte characters, particularly characters from East Asian languages, in your notification messages, ensure that you select the appropriate encoding method.

4. Click **Save**.

Customizing Email Notification Content

Email notifications are targeted at administrators. Customize these notifications if you want to provide information that can be important particularly to administrators in your organization.

Tip: For the list of variable tags that you can use with notifications, see *Notification Tags* on page 3-12.

To customize email notification content:

1. Click **Policy Enforcement** > **Notifications**.
2. Click the **Administrator** tab.
3. Click the type of email notification you want to customize. For descriptions of each notification type, see *Email Notifications* on page 3-11.
4. Modify the message.
5. Click **Save**.

Configuring Notification Settings

To help ensure that your notifications are delivered as expected, configure the following notification settings before using the device for policy enforcement:

- *Web notification settings* on page 3-18
- *Popup notification settings* on page 3-19
- *Email notification settings* on page 3-19

Note: Notification settings are global. These settings apply to all notification types and all policies.

Web notification settings

You can configure the following web notification settings:

- **Trend default look and feel—**select this option to use the default message appearance.

- **Custom**—select this option to specify the **Page title**, **Title text color**, and **Banner color**.
- **Display the assessment screen**—select this option to display the assessment page whenever the endpoint attempts to opens a web page while it is being assessed.

To configure web notification settings:

1. Click **Policy Enforcement** > **Notifications**. The **Endpoint** tab is selected by default.
2. In the **Web Notifications** section, click **Settings**.
3. Specify your preferred settings and click **Save**.

Popup notification settings

You can configure the following web notification settings:

- **Encoding method**—select the encoding method that closely matches the language of your popup notifications. **English, German, French (ISO-8859-1)** is selected by default.
- **Popup method**—select whether to display a standard Windows message box or a notification from the agent icon on the taskbar. The **Windows message box** option is selected by default.

Note: If you have selected to hide the agent icon, any popup messages from the agent will not be displayed.

To configure popup notification settings:

1. Click **Policy Enforcement** > **Notifications**. The **Endpoint** tab is selected by default.
2. In the **Popup Notifications** section, click **Settings**.
3. Specify your preferred settings and click **Save**.

Email notification settings

Note: Email notification settings must be configured before any email notifications can be sent.

Configuring email notification settings lets you define:

- Recipient addresses—the notification recipients
- Sender address—the email address to use for sending notifications
- Character encoding—the encoding method that best matches the language of your email notifications. UTF-8 can cover most languages and character sets; however, select another encoding method if notification recipients are using email clients that do not support UTF-8.
- SMTP server address and port—the address or name of the server and the port used by the server for SMTP communication
- User name and password—credentials for sending mail through the specified SMTP server

To configure email notification settings:

1. Click **Policy Enforcement** > **Notifications**.
2. Click the **Administrator** tab.
3. In the **Email Notifications** section, click **Settings**.

Tip: You can access the same screen through **Administration > Email Settings**.

4. Specify all the settings.

Note: Email notifications are sent only if *all* the settings are specified.

5. Click **Test Connection** to verify whether Network VirusWall Enforcer can access the specified SMTP server. If the test fails, check network connectivity and the specified settings. Make necessary changes and rerun the test until it succeeds.
6. Click **Save**.

Configuring ARP Spoofing Protection

Network VirusWall Enforcer prevents Address Resolution Protocol (ARP) spoofing by broadcasting legitimate ARP information associated with your critical nodes. Network VirusWall Enforcer also monitors endpoints for ARP spoofing malware.

To understand the threat posed by ARP spoofing, see *ARP Spoofing Prevention* on page 1-8.

Monitoring for ARP Spoofing Malware

To detect and terminate ARP spoofing malware on endpoints, Network VirusWall Enforcer monitors applications for outgoing ARP traffic. If an application is found to be sending more than 100 ARP packets per second, Network VirusWall Enforcer considers the application ARP spoofing malware and can terminate the application.

To enable and configure malware monitoring:

1. Click **Policy Enforcement > ARP Spoofing Prevention**.
2. Under **Malware Monitoring Settings**, select **Monitor for suspicious ARP traffic from endpoints**. With this option selected, Network VirusWall Enforcer automatically monitors endpoints for ARP traffic.
3. To terminate endpoint applications exhibiting ARP spoofing behavior, select **Stop endpoint processes that send suspicious ARP traffic**.
4. Click **Save**.

ARP Spoofing Prevention

By broadcasting legitimate ARP information, Network VirusWall Enforcer allows endpoints to correct spoofed ARP information from malware or other sources.

Note: When configuring ARP spoofing prevention, specify MAC and IP address information of your critical nodes, including gateways and servers. This information helps prevent misdirection of network traffic to critical nodes.

To enable and configure ARP spoofing prevention:

1. Click **Policy Enforcement > ARP Spoofing Prevention**.
2. Under **Spoofing Prevention Settings**, select **Enable ARP spoofing prevention**.

3. Specify the IP and MAC addresses of your critical nodes to help ensure that traffic to these nodes are not affected by ARP spoofing. To do this:
   a. Type a valid IP address.

   Note: ARP spoofing prevention only supports IPv4 addresses.

   b. Type a valid MAC address.
   c. Use the comment field to provide additional information about the node you are adding.
   d. Click **Add to**.
4. Click **Save**.

Configuring Agent Settings

Network VirusWall Enforcer uses the Threat Management Agent (TMAgent) to perform certain policy enforcement tasks. You can configure the following agent settings:

- **Threat Management Agent port**—specify the port that the agent uses to communicate with Network VirusWall Enforcer. By default, the agent uses port 5091.
- **Hide the agent system tray icon**—selecting this option prevents the agent icon from displaying on the system tray of endpoints. This option also prevents agent-based popup notifications from displaying.
- **Poll Network VirusWall Enforcer periodically**—select this option to automatically send updates to Network VirusWall Enforcer if requests from the device are not received.

To configure agent settings:

1. Click **Policy Enforcement** > **TMAgent Settings.**
2. Specify your preferred settings.
3. Click **Save**.

Configuring the C&C Block List

Network VirusWall Enforcer can detect and block any known C&C server by integrating with Deep Discovery Inspector (DDI). This dynamic list monitors the network and checks all IP addresses against the DDI Virtual Analyzer C&C server list. If the Network VirusWall Enforcer Threat Mitigation feature is enabled, any detected C&C server will be added to the C&C Block List. Network VirusWall Enforcer will then block all subsequent connections to and from the C&C server.

If necessary, servers can be removed from the block list or added to the Approved list. Deleting a server from the block list may temporarily allow connections, but if Threat Mitigation is enabled, it will continue to detect the C&C server and add it to the list again. Adding a server to the Approved means all connections to and from the server are allowed.

WARNING! Add only critical servers or nodes to the Approved List.

To enable C&C blocking:

1. Register Deep Discovery Inspector or TDA to your Network VirusWall Enforcer device.
2. Enable Threat Mitigation in Policy Enforcement. Refer to *Step 6: Specify Threat Mitigation Rules* on page 4-18.
3. Click **Policy Enforcement** > **Block C&C Connections**. The Block List screen appears.
4. Enable the **Block connections to and from C&C servers detected by Deep Discovery Inspector** option.
5. Click **Save**.

To add critical servers to the Approved List:

1. Go to **Policy Enforcement** > **Block C&C Connections**.
2. Click the **Approved List** tab.
3. Specify the IP address or IP address range. Optionally, add a comment to indicate why this was added to the Approved List.
4. Click **Add to >**.
5. Click **Save**.

Chapter 4

Policy Creation and Deployment

This chapter describes how to define policies for enforcement by Trend Micro™ Network VirusWall™ Enforcer. It also discusses different deployment scenarios and how you can create policies to match these scenarios.

This chapter discusses the following topics:

Policy Enforcement Features

Network VirusWall Enforcer provides the following policy enforcement capabilities.

TABLE 4-1. Policy enforcement features

FEATURE	CHECKS FOR	DETECTION METHOD	SUPPORTED ACTIONS
Antivirus Product Scan	Compliance to antivirus software policy	Agent performs assessment **Note:** The device may also check for port activity to confirm the presence of security software.	• Monitor endpoint • Block endpoint • Redirect web traffic
Antivirus Version Scan	Compliance to pattern update policy	Agent performs assessment	• Monitor endpoint • Block endpoint • Redirect web traffic
System Threat Scan	Presence of active threats in memory	Agent performs assessment	• Clean up endpoint (automatic) • Monitor endpoint • Block endpoint • Redirect web traffic
Vulnerability Scan	Unpatched Microsoft software with known vulnerabilities	Agent performs assessment	• Monitor endpoint • Block endpoint • Redirect web traffic

TABLE 4-1. Policy enforcement features

FEATURE	CHECKS FOR	DETECTION METHOD	SUPPORTED ACTIONS
Registry Scan	Missing or unwanted registry entries	Agent performs assessment	• Monitor endpoint • Block endpoint • Redirect web traffic
Network Virus Scan	Malware code in packets	Real-time detection by device	• Monitor endpoint • Drop packets • Quarantine endpoint • Clean up endpoint
Application Protocol Detection	Traffic in specified ports	Real-time detection by device	• Monitor endpoint • Reject packets • Drop packets
Instant Messaging Detection	Traffic from popular instant messaging software	Real-time detection by device	• Monitor endpoint • Reject packets • Drop packets
File Transfer Detection	File transfers using Windows shares, FTP, or HTTP	Real-time detection by device	• Monitor endpoint • Reject packets
Threat Mitigation	Potentially infected endpoints	Threat Discovery Appliance	• Monitor endpoint • Quarantine endpoint

Actions and Remediation Methods

The following table describes the actions and remediation methods that Network VirusWall Enforcer can perform in response to policy violations.

TABLE 4-2. Supported actions and remediation methods

METHOD	TARGET	DESCRIPTION
Monitor	Endpoint	Tags the endpoint as noncompliant and applies a more aggressive assessment schedule
Block	Endpoint	Blocks endpoint traffic until the next assessment
Redirect to URL	Web traffic	Opens a specified URL when a blocked or quarantined endpoint attempts to open a website; with this method selected, you can also specify: • Allow off-page navigation—select this option to allow endpoint users to follow links from the specified URL. • Link depth—this value serves as a limit to the number of links endpoint users can navigate away from relative to the specified URL. You can use this option to prevent unprotected endpoints from reaching harmful or compromised pages.
Quarantine	Endpoint	Blocks endpoint traffic until the endpoint is released through the console

TABLE 4-2. Supported actions and remediation methods

METHOD	TARGET	DESCRIPTION
Reject	Application- or protocol-specific packets	Prevents packets from passing and sends a reset packet (RST) to the source
Drop	Application- or protocol-specific packets	Prevents packets from passing
Clean up	Endpoint	Attempt to stop malware and remove its components from the endpoint

Policy Matching Overview

Network VirusWall Enforcer allows you to create multiple policies for different network segments and different types of endpoints and traffic. Network VirusWall Enforcer follows a first-match rule—once the device matches a policy to a communication session, it stops checking for additional policy matches.

First-Match Rule

Keep broad policies at the bottom of the policy list and specific policies higher in the list. Consider the three policies in the following table:

TABLE 4-3. Example of correctly prioritized policies

Priority	Endpoint	Destination	Assessment Criteria
1	RD, Marketing	Sales	Antivirus Product Scan, System Threat Scan, Vulnerability Scan, Network Virus Policy
2	RD, Marketing	*	Antivirus Product Scan, Network Virus Policy
3	*	*	Network Virus Policy

In *Table 4-3*, placing broader policies lower in the list prevents situations where specific and more stringent policies are never matched.

In *Table 4-4*, placing broader polices higher in the priority list prevents other policies from being enforced. The broadest policy, which matches communication sessions from any source or to any destination, prevents enforcement of the second and third policies. Also, even if the first policy is removed, the third policy is still never enforced, since the destination of the third policy is more specific than that of the second policy.

TABLE 4-4. Example of incorrectly prioritized policies

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

Policy Enforcement Best Practices

Before creating policies for enforcement, review the following best practices:

- Carefully set policy priority based on the first-match rule.
- Traffic from a targeted endpoint must pass through Network VirusWall Enforcer or the device will not recognize 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 have a DNS server on your network, ensure the following:
  - Add the Gateway and DNS IP addresses to **Global Endpoint Exceptions**.
  - Specify the DNS server IP addresses in the Preconfiguration console to allow the device to relay DNS queries for blocked endpoints.
- If you use a proxy server, include the Proxy port in HTTP detection settings.

- If you select **ActiveX** as 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. Ensure that endpoint firewalls do not block the agent installation.
- 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 the ActiveX deployment option and select to assess only Trend Micro products using networking protocols, the Threat Management Agent (TMAgent) will not install on endpoints.
- If you want endpoints to access the URL exception page, do not specify TCP port 80 under **Application Protocol Detection**.
- If you select the **Reject packet** action in **Application Protocol Detection** the following occurs:
  - TCP: TCP reset
  - UDP: ICMP destination port unreachable
  - ICMP: ICMP destination port unreachable
- If you select the **Drop packet** action in **Application Protocol Detection**, applications waiting for responses to dropped packets may appear unresponsive.
- If you select the **File Transfer Detection** service:
  - HTTPS traffic is not scanned.
  - ASP uploads are 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 to 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 **Display the assessment screen** under **Endpoint Notifications** and select a short reassessment interval during policy creation, endpoint users will frequently see the assessment screen while waiting to access the network. Consider disabling the assessment screen to make assessments transparent to end users.

Overview of Policy Sections

Each Network VirusWall Enforcer policy comprises of the following sections.

TABLE 4-5. Policy sections

SECTION	DESCRIPTION
Endpoint Settings	Agent deployment options and endpoint reassessment intervals
Authentication and Network Zones	• User authentication requirements for accessing the network • Policy coverage, specifically endpoint IP/MAC addresses (network zones), ports, and enforcement schedule
Enforcement Policy	Antivirus product and pattern checking, malware scans, vulnerability checks, and registry checks
Network Virus Policy	Packet-level scanning for network viruses and other malware

TABLE 4-5. Policy sections

SECTION	DESCRIPTION
Network Application Policy	Regulation of port activity, instant messaging, and file transfers
Threat Mitigation Rules	Enforcement of detections from Threat Discovery Appliance, which monitors for suspicious network activity
URL Exceptions	URLs that are always accessible to all endpoints, including noncompliant endpoints

Creating a Policy

Network VirusWall Enforcer secures your network by checking network traffic and endpoints based on predefined policies. This approach provides the flexibility of implementing different assessment criteria for different devices as well as implementing different actions when these criteria are violated. For more information about Network VirusWall Enforcer policies, see *Policy Enforcement Features* on page 4-2.

Policy creation is done through a wizard in the web console. It involves the following steps:

- *Step 1: Specify Endpoint Settings* on page 4-10
- *Step 2: Specify Authentication and Network Zones* on page 4-11
- *Step 3: Specify Enforcement Policy* on page 4-12
- *Step 4: Specify Network Virus Policy* on page 4-15
- *Step 5: Specify Network Application Policy* on page 4-15
- *Step 6: Specify Threat Mitigation Rules* on page 4-18
- *Step 7: URL Exceptions* on page 4-18
- *Step 8: Review, Enable, and Save the Policy* on page 4-18

Tip: For detailed information about a wizard screen, click the Help button while on that screen. For important information about policy rules and priorities before you create a policy, see *Policy Enforcement Best Practices* on page 4-6.

Step 1: Specify Endpoint Settings

1. Click **Policy Enforcement** > **Policies**. The **Policies** screen displays.
2. Click **Add to** to start the wizard.
3. Type a policy name. Comments are optional.
4. Select one of the options for agent deployment. See *Agent Deployment Options* on page 1-10.
5. Specify the agent installation method by selecting one of the following:
   - **ActiveX**—endpoint users must click a confirmation message to run ActiveX to install TMAgent.
   - **Remote login, ActiveX**—endpoint users do not need to click a confirmation message when installing TMAgent using remote login. To use this feature, you need to configure remote login accounts for accessing endpoint computers on your network. If remote login does not complete successfully, the assessment continues using ActiveX.

   Note: Windows XP Home does not support remote login. For operating systems that do not support remote login, use the ActiveX only deployment method.

6. Specify preferences for non-Windows or unidentifiable operating systems. The options are:
   - Disable endpoint detection for non-Windows operating systems
   - Disable endpoint detection for unidentifiable operating systems
7. Specify reassessment time intervals for compliant and noncompliant endpoints. Set a shorter reassessment interval for noncompliant endpoints.
8. Click **Next**.

Step 2: Specify Authentication and Network Zones

1. Specify optional authentication settings by selecting the **Enable user authentication**. This option lets you select whether to apply the policy to authenticated users or to guest users.

   Note: Configure LDAP settings if you select **Enable user authentication**. See *Configuring LDAP Authentication Settings* on page 3-2 for more information. If you create one policy for authenticated users, create another policy that applies to users that are not authenticated.

2. Specify Endpoint Network Zone settings. This option lets you select the endpoints groups or network zones that need to be assessed against the policy. Click **Add** if you need additional network zones. For information about adding network zones, see *Defining Network Zones* on page 3-5.
3. Click **Show Details** to modify more specific settings.
   a. Specify packet destination network zones. This option lets you apply the policy to traffic headed for certain endpoints only.
   b. Specify TCP/UDP protocol ports. This option lets you apply the policy to traffic at certain ports only. You can specify up to 64 TCP or UDP ports.
   c. Specify a schedule for the policy. The policy will only apply during the specified schedule.
4. Click **Next**.

Step 3: Specify Enforcement Policy

Specify the services by selecting the checkbox next to the scan type:

1. **Antivirus Product Scan**—use this feature to scan for antivirus software on endpoints.
   a. Select **Antivirus Product Scan**.
   b. Select the products to detect.

Note: To detect antivirus products using only protocol activity, select **Only use networking protocols to assess Trend Micro products**. Selecting this option will allow you to detect certain Trend Micro products without an agent.

---

   c. Specify the **Endpoint Action** by selecting one of the following:
      - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
      - **Block endpoints—**you can select a remedy from **None** or **Redirect to URL**, which redirects endpoint users to a page where they may rectify policy violations.

        If you select **Redirect to URL**, you have the option of limiting the number of pages endpoint users can navigate to by selecting **Allow off-page navigation** and **Link depth**.
2. **Antivirus Version Scan**—use this feature to require endpoints to keep their antivirus patterns updated.
   a. Select **Antivirus Version Scan**.
   b. Specify the acceptable pattern version by selecting one of the following:
      - **Require the latest virus pattern file**—require the endpoint to keep the virus pattern updated.
      - **Allow virus pattern files that are**—you can specify whether to allow patterns that are up to four versions old.
   c. Specify the **Endpoint Action** by selecting one of the following:
      - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.

- **Block endpoints—**you can select a remedy from **None** or **Redirect to URL**, which redirects endpoint users to a page where they may rectify policy violations.

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

3. **System Threat Scan**—use this feature to scan for system threats. This feature does not scan files. Instead, it scans memory for threats.

Note: If you select persistent agent deployment and the system threat scan service, the device may not check the endpoint more than once. However, if you select the single-use agent deployment option, the device checks the endpoint during each reassessment.

---

   a. Select **System Threat Scan**.

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

      - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
      - **Block endpoints—**you can select a remedy from **None** or **Redirect to URL**, which redirects endpoint users to a page where they may rectify policy violations.

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

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 **Vulnerability Scan**.

   b. Select the type of vulnerabilities to scan. Click on the vulnerability risk rating to select individual vulnerabilities. For more information about vulnerability risk ratings, see *Vulnerabilities* on page 1-12.

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

- **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
- **Block endpoints—**you can select a remedy from **None** or **Redirect to URL**, which redirects endpoint users to a page where they may rectify policy violations.

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

5. **Registry Scan**—use this feature to scan for required and prohibited software by using registry key information.
   a. Select **Registry Scan**.
   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.
   e. Type the **Registry Key**.
   f. Under **Registry key value**, specify the following optional criteria:
      - **Name**—specify the value name.
      - **Type/Data**—specify the data type (**String** or **DWord**) and the actual value of the data. If you do not specify a value name, you will be limited to string data types.
   g. Click **OK**. The window closes and the registry key displays in the list.
   h. Specify the **Endpoint Action** by selecting one of the following:
      - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
      - **Block 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 the endpoint can navigate by selecting **Allow off-page navigation** and **Link depth**.
6. Select **Send policy violation data to syslog** to record related events to logs.

7. Select **Notify endpoints about policy violations** to display popup messages on endpoints that violate this section of the policy.
8. Click **Next**.

Step 4: Specify Network Virus Policy

1. Select the **Enable Network Virus Scan** to detect network viruses in packets that pass through the device.
2. Specify the action to perform when a network virus is detected by selecting one of the following:
   - **Monitor endpoints—**flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
   - **Drop packets**—drop the packet.
   - **Quarantine endpoints—**blocks the endpoint from accessing the network until it is released through the console.
3. Specify the **Remedy** by selecting one of the following:
   - **None**
   - **Clean up**—remove components of the detected malware from the endpoint.
4. Select **Send policy violation data to syslog** to record related events to logs.
5. Select **Notify endpoints about policy violations** to display popup messages on endpoints that violate this section of the policy.
6. 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**—select this option to regulate activity on certain TCP and UDP ports. Select ICMP to regulate ICMP activity.
   a. Select the **Application Protocol Detection**.
   b. Under **TCP port**, type the TCP ports or port ranges to scan.
   c. Under **UDP port**, type the UDP ports or port ranges to scan.

d. Select **ICMP** to regulate ICMP activity.

Note: To use ICMP, ensure you select **All ports** in the **TCP/UDP Protocol Ports** settings in *Step 2: Specify Authentication and Network Zones* on page 4-11.

---

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

- **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
- **Reject packets—**return a reset packet (RST) to inform the source endpoint that the connection has been broken.
- **Drop packets—**close the connection to prevent the packets from passing.

2. **Instant messaging detection**—use this feature to regulate instant messenger activity.

a. Select **Instant messaging detection**.

b. Select the instant messaging software to regulate:

- **MSN**—select to check MSN or Windows Live Messenger traffic. You can regulate only file transfer activity or all activities.
- **Yahoo**—select to check Yahoo! Messenger traffic. You can regulate only file transfer activity or all activities.
- **ICQ/AIM**—select to check ICQ or AOL Instant Messenger (AIM) traffic. You can regulate only file transfer activity or all activities.
- **IRC**—select to regulate all Internet Relay Chat (IRC) activity

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

- **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
- **Reject packets—**return a reset packet (RST) to inform the source endpoint that the connection has been broken.
- **Drop packets—**close the connection to prevent the packets from passing.

3. **File transfer detection**—use this feature to regulate file transfer activity.

   WARNING! Avoid overly broad wildcard entries such as *.* or *.htm for the files to assess. These entries can completely block access to the Internet.

   a. Select **File transfer detection**.

   b. Select the types of file transfer activities to assess:

      - **Windows file transfer**—select this option to assess CIFS and Samba protocol file transfers. Most of these file transfers occur when files are copied to and from shared folders.
      - **HTTP file transfer**—select this option to assess HTTP file transfers.
      - **FTP file transfer**—select this option to assess FTP file transfers.

   c. Type the files to check under **Files to assess** and the files to allow under **Exception**.

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

      - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
      - **Reject packets—**return a reset packet (RST) to inform the source endpoint that the connection has been broken.

4. Select **Allow Control Manager to modify Network Application Policy settings when an outbreak occurs** if you use a Control Manager server to manage Trend Micro products. The device temporarily enforces the Outbreak Prevention Policy during an outbreak and reverts to this policy afterwards.
5. Select **Send policy violation data to syslog** to record events to logs.
6. Click **Next**.

Step 6: Specify Threat Mitigation Rules

1. Select **Enable Threat Mitigation** to enforce Deep Discovery Inspector (DDI) detections. DDI analyzes network activity to identify endpoints that may be infected with malware.

   Note: Enabling this feature also enables C&C server detection and blocking.

2. Select the action to apply on endpoints exhibiting suspicious network activity:
   - **Monitor endpoints**—flag the endpoint as "noncompliant", but allow endpoint traffic to pass.
   - **Quarantine endpoints—**blocks the endpoint from accessing the network until it is released through the console.
3. Select **Send policy violation data to syslog** to record events to logs.
4. Select **Notify endpoints about policy violations** to display popup messages on endpoints that exhibit suspicious network activity.
5. Click **Next**.

Step 7: URL Exceptions

1. Specify URL exceptions by selecting from the existing URL lists, or add a new URL list by clicking **Add**. Excepted URLs remain accessible to blocked endpoints.

   Tip: For information on creating URL lists for use in policy exceptions, see *Defining URL Lists* on page 3-4.

2. Click **Next**.

Step 8: Review, Enable, and Save the Policy

At the review screen:

- Review the policy. Click **Edit** if you need to modify a policy section.
- Enable or disable the policy. To save this change, click **Save**.

Sample Policy Creation

With Network VirusWall Enforcer, administrators create policies to determine whether endpoints sending traffic through the device threaten the security of the network. 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 a group need to have antivirus software (the corresponding service is **Antivirus Product Scan**), while endpoints in another group need to update all security patches to prevent vulnerabilities (the corresponding service is **Vulnerability Scan**).

Scenario 1: Different Policies for Different Users

In this scenario, we define three policies: a policy for authenticated users, a policy for guest users, and a catch-all policy to be triggered if neither of the two policies is triggered. We want to enforce the following:

- Authenticated users must have recommended antivirus software.
- Guest users must have a certain registry key.
- All other users must have recommended antivirus software and a certain registry key.

Policy for Authenticated Users

This policy ensures that all authenticated users have recommended antivirus software installed.

1. Create a network zone.

   Before creating the first policy, create a network zone that includes all IP addresses in the network. Call this zone "Internal endpoints".

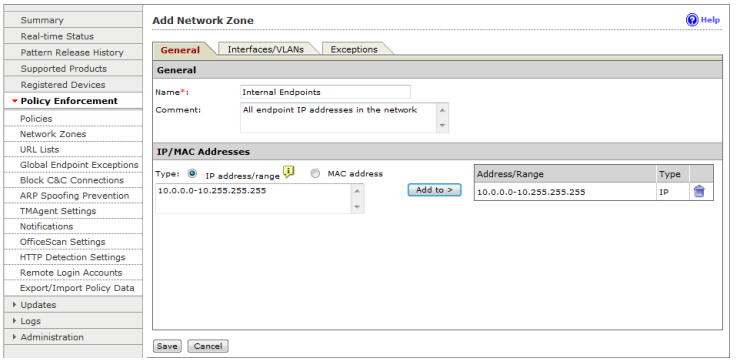


FIGURE 4-1. Adding the network zone

2. Create the "Authenticated users" policy.

Add a policy and specify the name "Authenticated users". Ensure that the persistent agent deployment option is selected.

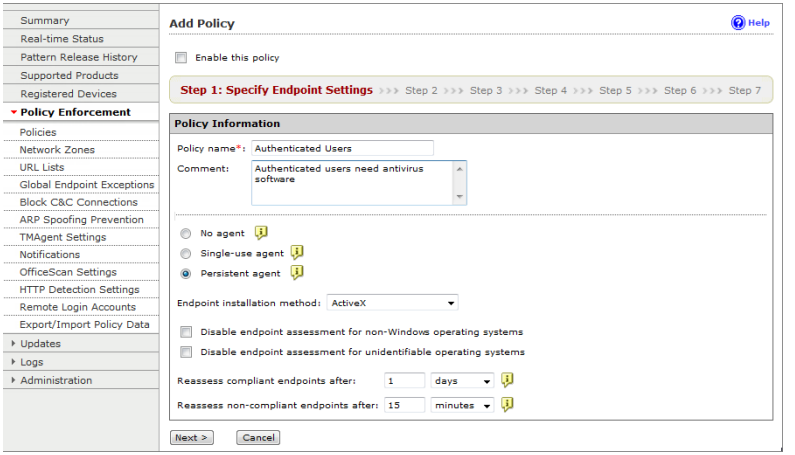


FIGURE 4-2. Adding the policy

3. Specify the network zone and authentication settings.

   Select **Enable user authentication** and then select **Apply policy to authenticated users**. This ensures that the policy applies to endpoints whose current users have authenticated either locally or to the domain.

   Choose to specify a network zone and add the **Internal endpoints** network zone to the list of selected network zones.

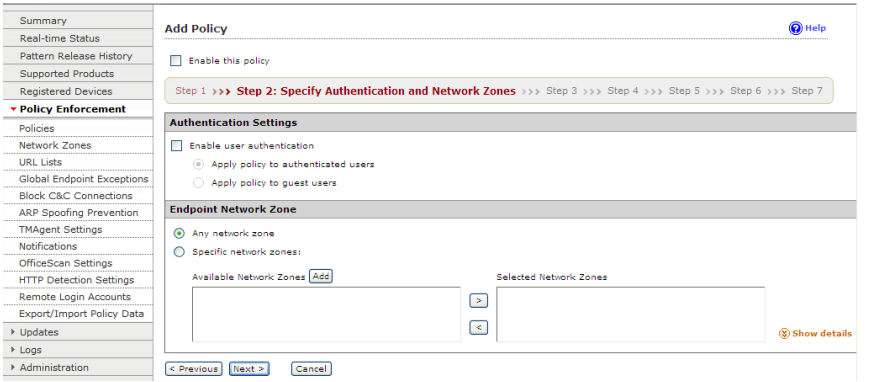


FIGURE 4-3. Specifying authentication and network zones

4. Specify the enforcement policy.

   Select **Antivirus Product Scan**. By default, Network VirusWall Enforcer will check whether any of the supported antivirus products are installed on endpoints.

To ensure logging and to notify end users when this particular criteria is violated, select **Send policy violation data to syslog** and **Notify endpoints about policy violations**.

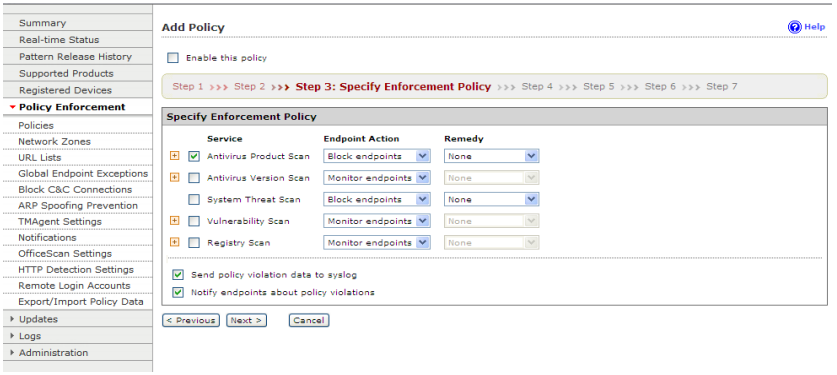


FIGURE 4-4. Specifying enforcement policy

5. Complete the policy.

   Click **Next** until you reach the policy review screen. Review the policy before enabling and saving it.

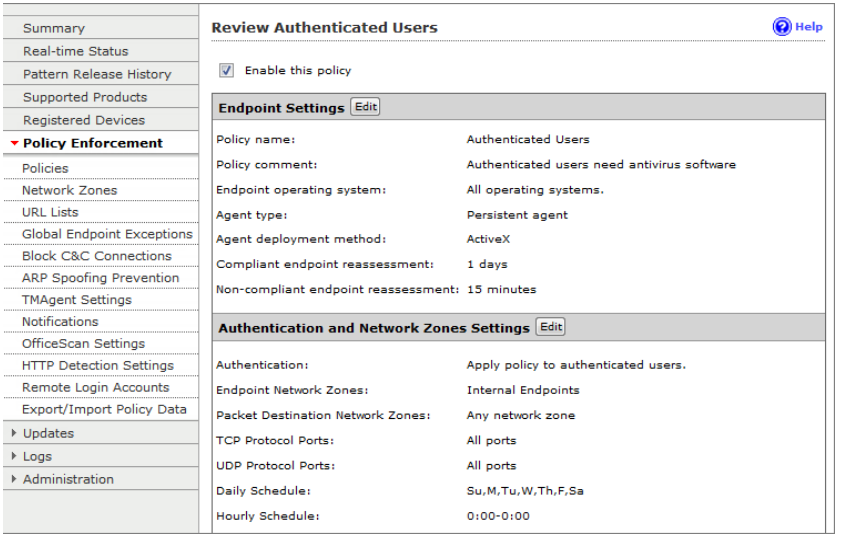


FIGURE 4-5. Reviewing the policy and enabling it

Note: Network Virus Scan is enabled by default on all policies.

Policy for Guest Users

This policy ensures that all guest users have a certain registry key.

1. Create the "Guest users" policy.

   Add a policy and specify the name "Guest users". Ensure that the persistent agent deployment option is selected.

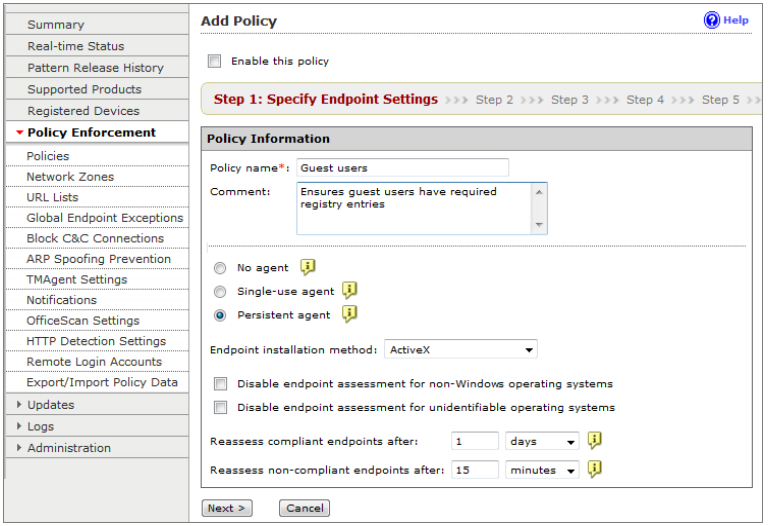


FIGURE 4-6. Adding the policy

2. Specify the network zone and authentication settings.

   Select **Enable user authentication** and then select **Apply policy to guest users**. This ensures that the policy applies to endpoints whose current users are guest users.

Click **Show details** to show more options. Choose to specify a network zone for the packet destinations and add the **Internal endpoints** network zone to the list of selected network zones. Note that you do not specify an endpoint network zone.

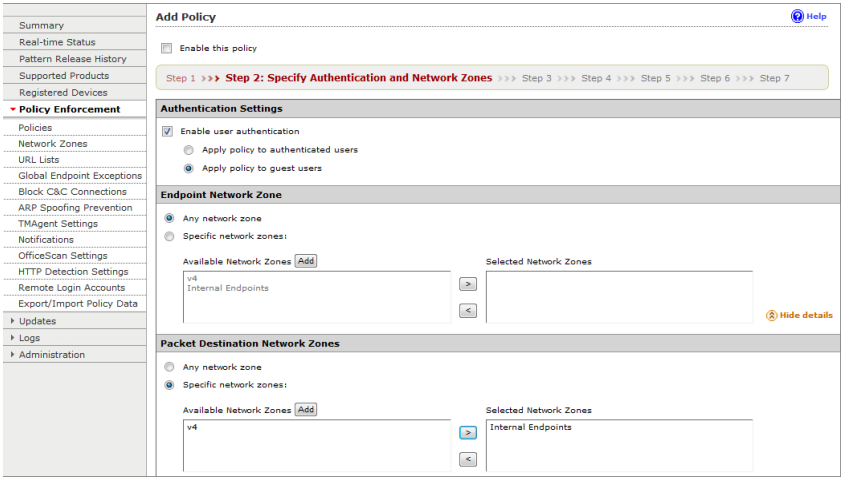


FIGURE 4-7. Specifying authentication and network zones

3. Specify the enforcement policy.

   Select **Registry Scan**. Expand the section and click **Add** to specify the registry keys to check. You can check for registry keys that indicate whether required applications or product upgrades are installed.

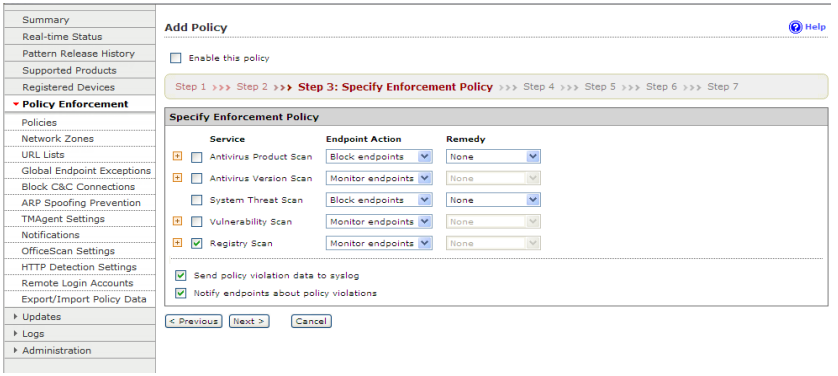


FIGURE 4-8. Specifying enforcement policy

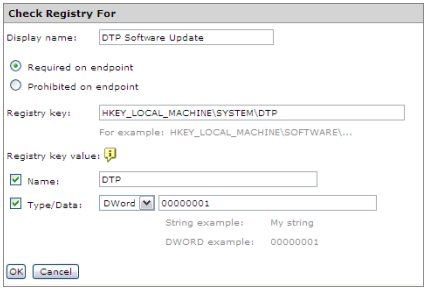


FIGURE 4-9. Adding the registry key

To ensure logging and to notify end users when this particular criteria is violated, select **Send policy violation data to syslog** and **Notify endpoints about policy violations**.

4. Complete the policy.

Click **Next** until you reach the policy review screen. Review the policy before enabling and saving it.

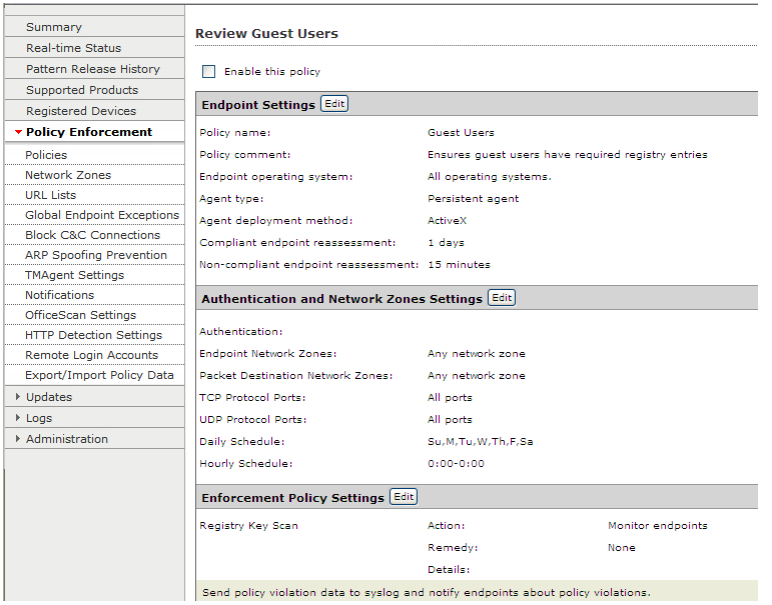


FIGURE 4-10. Reviewing the policy and enabling it

Note: Network Virus Scan is enabled by default on all policies.

Catch-All Policy

When you create this policy, note the following:

- Do not select **Enable user authentication** in **Step 2** of the policy creation wizard.
- Ensure that settings are configured to apply to **Any** or **All**.
- Enable all the policy enforcement criteria enabled in the policy for authenticated users (see *Policy for Authenticated Users* on page 4-19) and the policy for guest users (see *Policy for Guest Users* on page 4-25).
- Specify the lowest priority (priority number 3) for this policy to ensure that it only applies to endpoints that are not matched against other policies. For more information on how Network VirusWall Enforcer performs policy matching, see *First-Match Rule* on page 4-5.

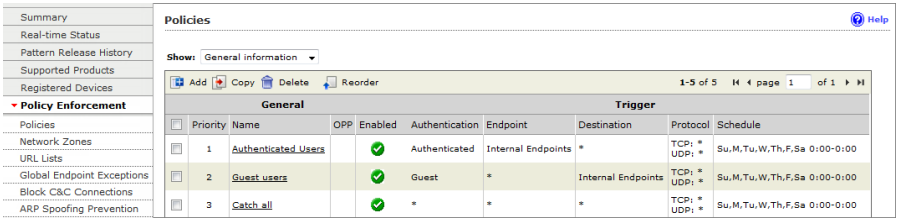


FIGURE 4-11. Policies and their priority

Scenario 2: Ensuring Platform Compliance

In this scenario, create a policy that ensures that endpoints are running Windows XP and have Service Pack 2 installed.

To create this policy:

1. Create a policy that deploys a persistent agent on endpoints.

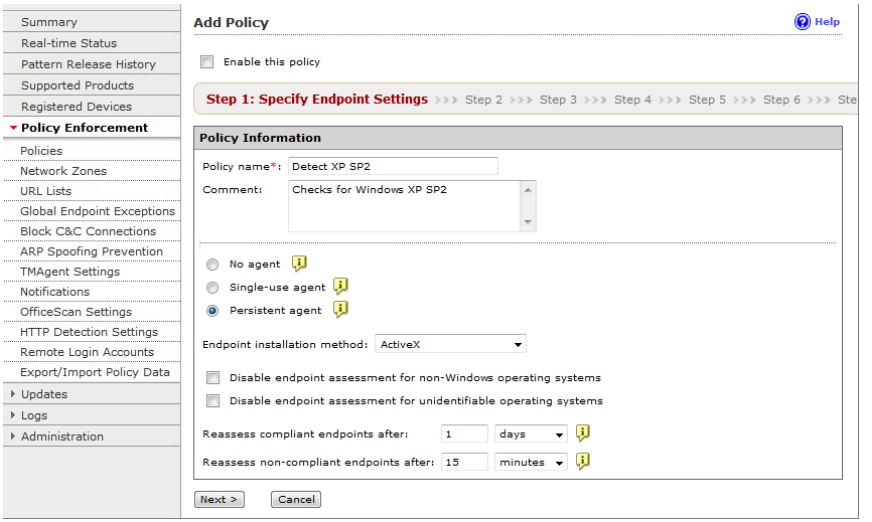


FIGURE 4-12. Adding the policy

2. Like the first sample scenario (see *Scenario 1: Different Policies for Different Users* on page 4-19), configure a network zone that includes all IP addresses of endpoints. Call this network zone "Internal endpoints".

3. Specify the network zone and authentication settings.

   Ensure that **Enable user authentication** is not selected. Choose to specify a network zone and select the **Internal endpoints** network zone as the source and destination zone.

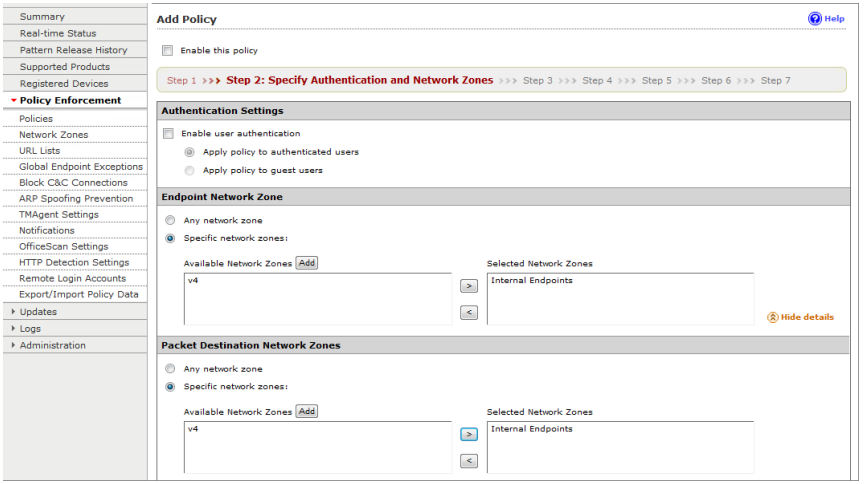


FIGURE 4-13. Specifying the network zone

4. Specify the enforcement policy.

Select **Registry Scan**. Expand the section and click **Add** to specify the registry keys to check.

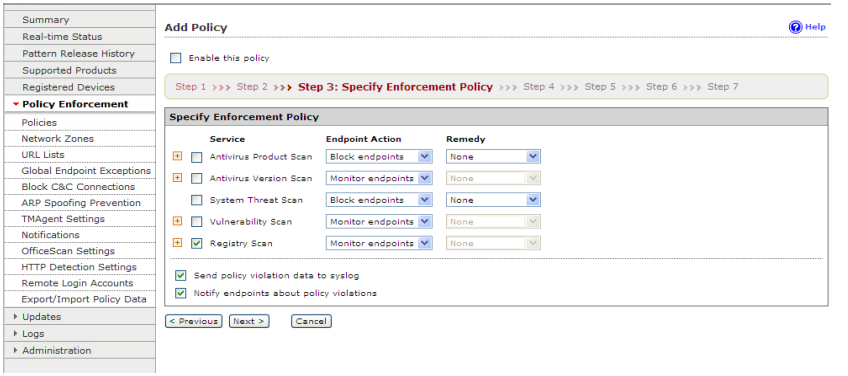


FIGURE 4-14. Selecting registry scan

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

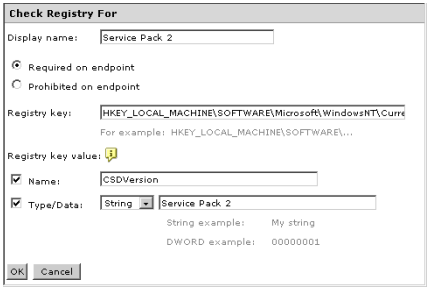


FIGURE 4-15. Adding the Windows XP SP2 Registry key

6. To ensure logging and to notify end users when this particular criteria is violated, select **Send policy violation data to syslog** and **Notify endpoints about policy violations**.
7. Complete the policy.

   Click **Next** until you reach the policy review screen. Confirm that the required registry key displays in the **Registry Key Scan** list.

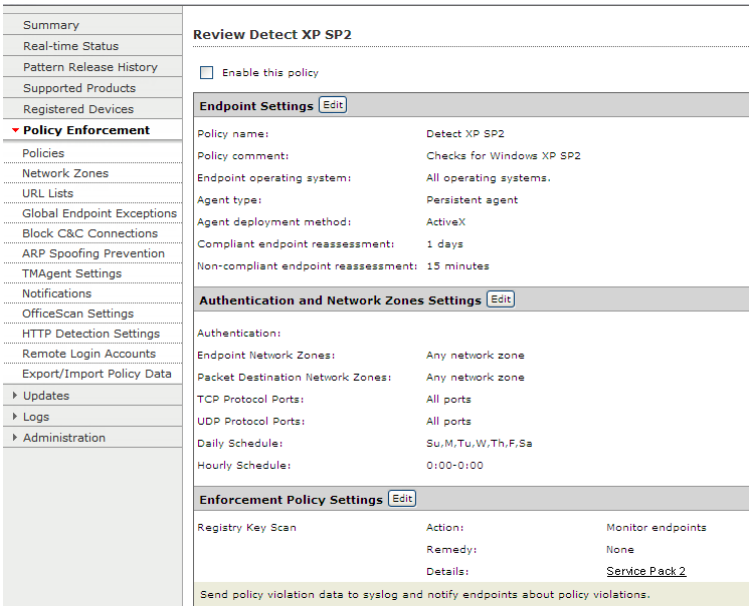


FIGURE 4-16. Reviewing the policy and enabling it

8. Enable the policy and save it.

Sample Deployment Scenarios

Network VirusWall Enforcer deployment needs to be tailored to the topology of your network. It is usually placed between a switch that leads to the public network and an edge switch that defines a network segment. You can also place it between an edge switch and a hub. This section includes three sample deployment scenarios and one sample policy configuration based on the first deployment scenario.

Deployment Scenario I: Standard Network

In this sample deployment scenario, Network VirusWall Enforcer:

- Protects the public server farm by scanning all traffic for network viruses and enforcing a policy for remote endpoints. Network VirusWall Enforcer also applies a remedy to endpoints that violate the policy.
- Protects an internal server farm by scanning all traffic for network viruses.
- Is located between the distribution switch and access switch. Network VirusWall Enforcer scans all traffic for network viruses and enforces a policy for all endpoints.
- Protects a small branch office by scanning all traffic for network viruses and enforcing a policy for all endpoints in the branch office.

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

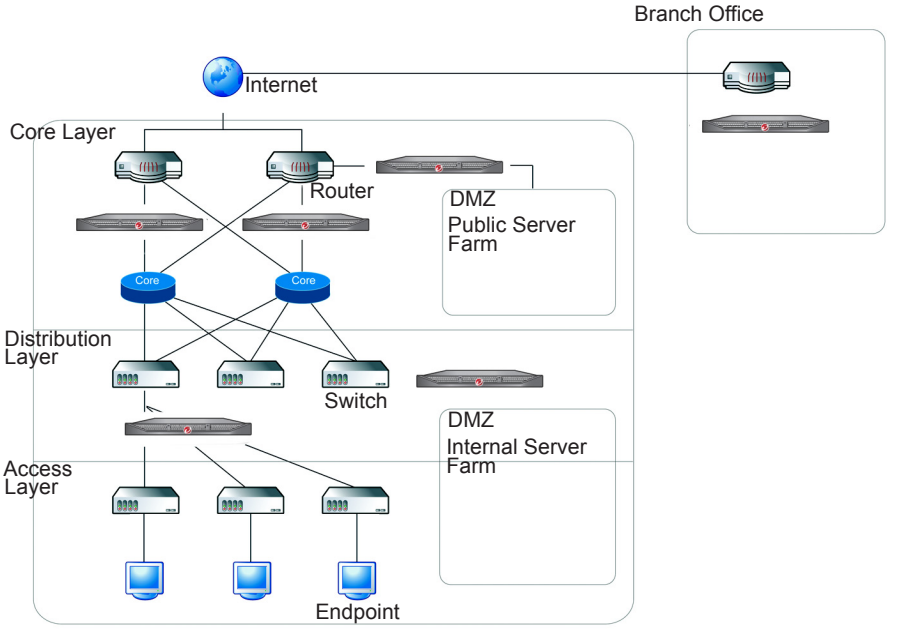


FIGURE 4-17. Standard network mode scenario

Deployment Scenario II: Global Site

In this sample deployment scenario, Network VirusWall Enforcer:

- Protects the data center by scanning all traffic for network viruses and enforcing a policy for remote endpoints. Network VirusWall Enforcer also applies a remedy to endpoints that violate policy.
- Is located between the core switch and access switches. Network VirusWall Enforcer scans all traffic for network viruses and enforces a policy for all endpoints.

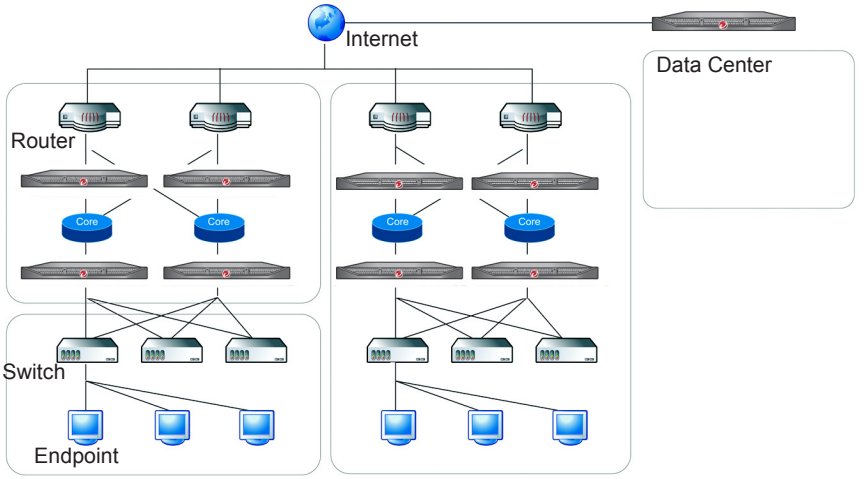


FIGURE 4-18. Global site scenario

Sample Policy Configuration

This section provides three sample policy configurations for *Deployment Scenario I: Standard Network* on page 4-33. To protect each area of the network, create different policies based on area and type of access. For this example:

- Configure policies to protect the public server farm
- Configure policies to scan packets going between the distribution switch and the 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 4-6*, specifically handles all traffic originating from payment processing since the public server farm can be used for billing purposes.

TABLE 4-6. Priority 1 policy for public server farm scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Priority Connection to Farm • **Policy Comment**: Set higher priority than "Server Farm" policy. • **Agent Type**: Single-use agent • **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

TABLE 4-6. Priority 1 policy for public server farm scenario (Continued)

SETTINGS	DETAILS
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Drop packet **Remedy**: None • **Send policy violation data to syslog**

The second policy, *Table 4-7*, is necessary to handle all other traffic.

TABLE 4-7. Priority 2 policy for public server farm scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Server Farm • **Policy comment**: Set lower priority than "Priority Connection to Farm". • **Agent type**: Single-use agent • **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**: Clean up • **Send policy violation data to syslog**

The last policy, *Table 4-8*, handles all cases not covered by the other policies.

TABLE 4-8. Priority 3 policy for public server farm scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Catch All • **Policy comment**: Set with the lowest priority. • **Agent type**: Single-use agent • **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**: Clean up • **Send policy violation data to syslog and notify endpoints about policy violations**

Note: Once an endpoint matches a trigger for a policy, the device does not apply any other policies to that endpoint.

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 device is between the core switch and WAN module.

The first policy, *Table 4-9*, specifically handles all traffic from guest endpoint. It redirects users to the page where they can obtain installers for the recommended antivirus product.

TABLE 4-9. Priority 1 policy for the distribution and access switch scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Guest • **Policy comment**: If you plan to use protocol-based antivirus product detection, specify a higher priority for this policy than the policy for authenticated users. • **Agent type**: Single-use agent • **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 guest 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
Enforcement Policy Settings	• **Antivirus Product Scan:** **Action**: Block endpoints **Remedy:** Redirect to URL • **Details**: All antivirus products • **System Threat Scan** **Action**: Block endpoints • **Vulnerability Scan** **Action**: Block endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Send policy violation data to syslog and notify endpoints about policy violations**

TABLE 4-9. Priority 1 policy for the distribution and access switch scenario (Con-

SETTINGS	DETAILS
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Clean up • **Send policy violation data to syslog and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, HTTP file transfer • **Send policy violation data to syslog and notify endpoints about policy violations**

The second policy, *Table 4-10*, specifically handles all traffic from Authenticated hosts. These are hosts that regularly access the network.

TABLE 4-10. Priority 2 policy for the distribution and access switch scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Authenticated users • **Policy comment**: This policy should have lower priority than the policy for guest users. • **Agent type**: Persistent agent • **Agent deployment method**: Remote login, ActiveX • **Compliant endpoint reassessment**: 1 day • **Noncompliant 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 4-10. Priority 2 policy for the distribution and access switch scenario (Con-

SETTINGS	DETAILS
Enforcement Policy Settings	• **Antivirus Product Scan** **Action**: Block 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 endpoints • **Vulnerability Scan** **Action**: Block endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Registry Scan** **Action**: Block endpoints **Remedy:** None **Details**: Windows Firewall, Prohibited • **Send policy violation data to syslog and notify endpoints about policy violations**
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Clean up • **Send policy violation data to syslog and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, FTP file transfer • **Send policy violation data to syslog and notify endpoints about policy violations**

The last policy, *Table 4-11*, handles all cases not covered by the other policies.

TABLE 4-11. Priority 3 policy for the distribution and access switch scenario

SETTINGS	DETAILS
Endpoint Settings	• **Policy name**: Catch-all • **Policy comment:** Since this policy is designed to check endpoints that do not violate any other policies, this policy should have the lowest priority. • **Agent type**: Single-use agent • **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 Product Scan** **Action**: Block endpoints **Remedy**: Redirect to URL **Details**: 56 Antivirus Products • **System Threat Scan** **Action**: Block endpoints • **Vulnerability Scan** **Action**: Block endpoints **Remedy:** Redirect to URL **Details**: Highly critical vulnerabilities, Critical vulnerabilities, and Important vulnerabilities • **Registry Scan** **Action**: Block endpoints **Remedy:** None **Details**: Windows Firewall, Prohibited • **Send policy violation data to syslog and notify endpoints about policy violations**

TABLE 4-11. Priority 3 policy for the distribution and access switch scenario (Con-

SETTINGS	DETAILS
Network Virus Policy Settings	• **Network Virus Scan** **Action**: Quarantine endpoint **Remedy**: Clean up • **Send policy violation data to syslog and notify endpoints about policy violations**
Network Application Settings	• **File Transfer Detection** **Action**: Reject packet **Details**: Windows file transfer, FTP file transfer • **Send policy violation data to syslog and notify endpoints about policy violations**

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 while the lower priority policy does, no hosts will match the second policy.

Exporting and Importing Policy Data

You can export policy data for backup purposes or for deploying policy data to another Network VirusWall Enforcer device. Import policies from another Network VirusWall Enforcer 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 > Export/Import Policy Data**.
2. Click **Export** under Export Policies. A File Download screen displays.
3. Click **Save** and specify where to save the policy data.
4. Click **Save**.

To import policies:

1. Click **Policy Enforcement** > **Export/Import Policy Data**.
2. Click **Browse** under Import Policies. The Choose File screen displays.
3. Select a file to import and then click **Open**.
4. Click **Import Policy**.

Note: Network VirusWall Enforcer may reset after importing policies.

Chapter 5

Maintaining the Device

This chapter describes maintenance options for Network VirusWall Enforcer. It discusses the following topics:

Configuring Administrative Accounts

Configure administrative accounts to manage Network VirusWall Enforcer. You can create new accounts or use default accounts or AD groups to manage Network VirusWall Enforcer. There are two kinds of accounts in Network VirusWall Enforcer:

- **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 > Account Management** from the main menu. The **Administrative Accounts** screen displays.
2. Click **Add**. The **Add Administrative Account** screen displays.
3. Type the user ID and password for the account.
4. Select the account privilege.
5. Click **Save**.

To add an AD Group:

1. Click **Administration > Account Management** from the main menu. The **Administrative Accounts** screen displays.
2. Click the **AD Groups** tab. The AD Groups screen displays.
3. Click **Add**. The Add AD Group screen displays.
4. Type a name for the AD group.
5. Select the account privilege for the AD group.
6. Click **Save**.

Backing Up Device Settings

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

Note: For instructions on how to export or import policy data only, see *Exporting and Importing Policy Data* on page 4-43.

To backup the configuration file:

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

To restore the configuration file:

1. Click **Administration** from the side menu. A drop down menu displays.
2. Click **Configuration Backup** from the drop down menu.
3. Click **Browse** under **Restore Configuration File**. The **Choose File** screen displays.
4. Select the file to import and click **Open**. Network VirusWall Enforcer 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 configuration. This allows easy replication of existing Network VirusWall Enforcer settings from one Network VirusWall Enforcer to other devices of the same model and locale settings.

Note: You can import or export configuration information only when locally accessing the Preconfiguration console. You cannot use this feature while accessing the console remotely using SSH.

To import the configuration file:

1. Prepare a copy of the configuration file on a USB flash drive.
2. Attach the flash drive to Network VirusWall Enforcer.
3. Access the Network VirusWall Enforcer Preconfiguration console (see the *Installation and Deployment Guide* for instructions).
4. Type `7` in the main menu. The System Tasks submenu appears.
5. Type `3` to import the configuration file. A confirmation screen appears.
6. Type `y` to continue.

Note: Refer to the *Installation and Deployment Guide* for detailed information on using the Preconfiguration console.

To export the configuration file:

1. Attach a USB flash drive for saving the configuration file to Network VirusWall Enforcer.
2. Access the Network VirusWall Enforcer Preconfiguration console (see *Installation and Deployment Guide* for instructions).
3. Type `7` in the main menu. The System Tasks submenu appears.
4. Type `4` to export the configuration file. A confirmation screen appears.
5. Type `y` to continue.

Note: Refer to the *Installation and Deployment Guide* for detailed information on using the Preconfiguration console.

Performing Device Tasks

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

Locking the Device

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

To set the network traffic lock:

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

Note: The network traffic lock does not take effect if the device has been powered off. If the device has been powered off, failopen allows traffic to pass even when network traffic has been locked.

Resetting the Device

Reset Network VirusWall Enforcer if you experience any problems or if the Control Manager management console prompts you to perform a reset. You can manually reset the device through the:

- Preconfiguration console (see page 5-6)
- Power button on the front panel of the device (see page 5-6)
- Web console (see page 5-6)

Any of the following actions can automatically invoke a device reset:

- Importing the configuration file through the Preconfiguration console or the web console.
- Updating the Network VirusWall Enforcer program file (some versions can require a reset).

If the device detects any of the above actions and failopen is in use, the device temporarily disconnects the failopen ports for approximately thirty seconds.

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

To reset the device through the Preconfiguration console:

1. Access the Preconfiguration console (see *Installation and Deployment Guide* for instructions).
2. Select item 7 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.

To reset the device using the power button:

Press the power button on the front panel of the device. After the device fully powers off, press the power button again to restart the device.

To reset the device through the web console:

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

Shutting Down the Device

You can power off the device through the web or the Preconfiguration console.

Note: To power the device back on, you need to press the physical power button.

To shut down the device through the Preconfiguration console:

1. Access the Preconfiguration console (see *Installation and Deployment Guide* for instructions).
2. Select item 7 in the main menu. The System Tasks submenu appears.
3. Select item 7 to shut down the device. A confirmation screen appears.
4. Select OK to continue.

To shut down the device through the web console:

1. Click **Device Tasks** on the **Administration** menu.
2. Click **Shut Down**.
3. Confirm the shut down when prompted.

Replacing the HTTPS Certificate

To secure access to the console using your own HTTPS certificate, replace the certificate.

To replace the HTTPS Certificate:

1. Click **Administration** > **HTTPS Certificate**.
2. Click **Replace HTTPS Certificate**.
3. Click **Browse** to specify the location of the certificate.
4. Click **Import Certificate**.

Generating a Certificate

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

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

Configuring SNMP Settings

Configure the SNMP settings from the web console after downloading the MIB file and configuring your MIB browser. See *SNMP Support* on page 1-19 for more information about SNMP features in Network VirusWall Enforcer.

To configure the SNMP settings:

1. Click **Administration**. A drop down menu displays.
2. Click **SNMP Settings** from the drop down menu. The **SNMP Settings** screen displays.
3. Select the **Enable SNMP Trap** check box under **SNMP Trap**.
4. Type the community name and the server IP address under **SNMP Trap**.
5. Select the **Enable SNMP Agent** check box under **SNMP Agent**.
6. Type the system location and the 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**. A 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. Specify the location and file name. Click **Save**.

Using Tools

Use the **Case Diagnostic Information** from **Administration > Tools** for troubleshooting purposes. The Case Diagnostic Information feature downloads all information required for use with the Case Diagnostic Tool, a product debug tool.

Restoring Default Settings

If you experience any issues during configuration, you can initialize Network VirusWall Enforcer through the Preconfiguration console. This restores settings to the factory defaults.

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

To initialize Network VirusWall Enforcer:

1. In the **Main Menu**, select **System Tasks**.
2. On the System Tasks submenu, select restore default settings.
3. Type y to continue.

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

Table 5-1 lists the default settings.

TABLE 5-1. Network VirusWall Enforcer default settings

SETTING	DEFAULT VALUE
Network VirusWall Enforcer host name	none
IP address type	Dynamic
IP address	none
Netmask	none
Default gateway	none
Primary DNS server	none
Secondary DNS server	none
Operation mode	none
Interface speed and duplex mode	Auto

System Recovery

You can perform pattern and engine rollbacks using the Preconfiguration console. You also have the option to reinstall the Network VirusWall Enforcer from an image file.

Pattern and Engine Rollback

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

Reinstalling the Device Image

WARNING! **Reinstalling the device image will delete all configuration and policy information. Export this information to another computer through the web console before attempting to reinstall the device image. For more information see** *Backing Up Device Settings* **on page 5-2 and** *Exporting and Importing Policy Data* **on page 4-43.**

Reinstalling with the Provided USB Flash Drive

1. Insert the flash drive to an available USB port.
2. Restart the device.
3. Press **F11** to go to the boot menu.
4. Select to boot from a hard drive and then select the USB flash drive.
5. Select to install the system image (Install NVWE1500i). The device will restart and display the Preconfiguration console.
6. Configure the newly installed device.

Reinstalling with Program Rescue

Note: To perform this procedure, you need the Trivial File Transfer Protocol (TFTP) tool in the provided USB flash drive.

1. Ensure that the device is connected to a network.
2. Restart the device.
3. Press ESC when prompted with the message **Press ESC to enter the menu**.
4. Select the option **3) Boot Rescue System** to start program rescue.
5. Obtain the IP of the device.
6. From another computer on the same subnet, run the TFTP tool to connect to the device and reinstall the image.

Chapter 6

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 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.

This chapter discusses the following topics:

Viewing Summary Information

When you open the web console, the **Summary** screen appears. This screen provides information about the general status of device components and policy enforcement through the following fields:

- **Policy Enforcement Status**—provides statistics on policy compliance and violations. Click the number under **Violations** for more information.
  - **Antivirus product scan**—checks the endpoint to determine if there is an antivirus application installed.
  - **Antivirus version scan**—checks the endpoint to determine if the antivirus pattern version is current.
  - **System threat scan**—checks the endpoint for viruses/malware and spyware/grayware.
  - **Vulnerability scan**—checks the endpoint to determine if it has the patches to known security vulnerabilities.
  - **Registry key scan**—checks the endpoint for required or prohibited registry entries.
  - **Network virus scan**—checks endpoint traffic for packets associated with network viruses and fast-spreading malware.
- **Threat Mitigation Events**—provides statistics on the results of mitigation efforts. Click the number to view additional information.
- **Top 5 Policies with Violations**—use this information to determine the most common policy violations. Click the number under Violations to view additional information.
- **Endpoint Summary**—provides statistics on the number of endpoints that are compliant, noncompliant, or quarantined.
- **AV Product Detection Status**—provides statistics on the number of endpoints with antivirus products. Click **Export** to save the information to a file.
  - **Protected Endpoints**—number of endpoints with installed antivirus software.
  - **Undetectable Endpoints**—includes endpoints that do not have antivirus software installed, endpoints that are running an operating system other than Windows, and endpoints that have a firewall that prevents assessment.
  - **Total Endpoints**—number of endpoints that the device attempted to assess.

  - **Virus Protection Ratio**—the percentage of endpoints with antivirus software in relation to the total number of endpoints.
- **Check endpoint status**—specify the IP address of an endpoint to check its status.
- **Component Status**—lists the Network VirusWall Enforcer components, allowing you to determine whether they are current. After an update, use this information to determine whether all components are current.

Viewing Real-Time Status Information

The Real-time Status screen lets you monitor device performance and ensure that port settings are correct. The Real-time Status screen displays the following information:

- **Performance Status**—displays CPU usage, memory usage, and concurrent connections
- **Interface Configuration Status**—displays a graphical view of the current port settings that corresponds to the physical port layout

Viewing the Pattern Release History

Network VirusWall Enforcer checks the update centers of different security vendors to obtain the version number of their latest antivirus patterns. It uses this information to determine whether endpoints patterns are up to date.

The Pattern Release History screen displays the version information that Network VirusWall Enforcer has obtained. It displays the version number of the latest pattern and up to four previous versions.

Viewing Supported Products

The Supported Antivirus Products screen lists all the antivirus products that Network VirusWall Enforcer can recognize for the purposes of policy enforcement. Network VirusWall Enforcer can identify and block endpoints that do not have any of the supported antivirus products installed. This screen also displays vendor and version information of the listed products.

Using Logs

Network VirusWall Enforcer generates log entries after updates and when policies are matched. Use the logs to help you analyze network protection, troubleshoot, and manage security risks in your network.

Overview of Log Types

Network VirusWall Enforcer maintains several log types.

Tip: For detailed information about each log field, click the Help button while on the log screen.

TABLE 6-1. Log types

LOG	DESCRIPTION
Event log	Network VirusWall Enforcer generates an entry in the event log every time it detects an event, such as a virus outbreak, or performs an action, such as a reset or a component update. If you register the device to Control Manager, it automatically sends event log entries to the Control Manager server.
Network virus log	Whenever Network VirusWall Enforcer detects a network virus, it creates a network virus log entry. If you register the device to Control Manager, it automatically sends network virus log entries to the Control Manager server.
ARP spoofing log	Whenever Network VirusWall Enforcer detects a malware associated with ARP spoofing, it generates an entry on the ARP spoofing log. Consult this log regularly to address any occurrences of this serious security breach.

TABLE 6-1. Log types (Continued)

LOG	DESCRIPTION
Threat mitigation log	Whenever Network VirusWall Enforcer attempts to respond to a detection by Threat Discovery Appliance (TDA), it generates an entry in the threat mitigation logs.
Endpoint history	When Network VirusWall Enforcer matches a policy to an endpoint, it creates an endpoint history entry. If you register the device to Control Manager, you can configure the time interval for sending endpoint history entries to the Control Manager server.

Viewing and Exporting 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 are sent to the Control Manager server immediately.

The event log displays the following information.

TABLE 6-2. Event log fields

FIELD	DESCRIPTION
Date/Time	Date and time the event occurred
Severity	How critical the event information is under Severity
Event	Nature of the event
Description	Detailed information about the event

To view and export the Event Log:

1. Click **Logs > Event Log** to open the Event Log screen.
2. To export the contents of the log, click **Export All to CSV**.

Viewing and Exporting the Network Virus Log

When the device detects a network virus, it creates a network virus log entry. If you register the device to Control Manager, entries from this log are sent to the Control Manager server immediately.

The network virus log displays the following information.

TABLE 6-3. Network virus log fields

FIELD	DESCRIPTION
Date/Time	Date and time of the detection
Endpoint IP Address	IP address of the endpoint associated with the detection
Endpoint Host Name	Host name of the endpoint
Endpoint MAC Address	MAC address of the endpoint
Network Virus Name	Name of the network virus
Scan Action	Action performed (this is the action specified in the policy)
Engine Version	Version of the Network Virus Engine used to detect this virus
Pattern Version	Version of the Network Virus Pattern used to detect the virus

To view the Network Virus Log:

1. Click **Logs > Network Virus Log** to open the Network Virus Log screen.
2. To export the contents of the log, click **Export All to CSV**.

Viewing and Exporting the ARP Spoofing Log

Whenever Network VirusWall Enforcer detects a malware associated with ARP spoofing, it generates an entry on the ARP spoofing log. Consult this log regularly to address any occurrences of this serious security breach.

The ARP spoofing log displays the following information.

TABLE 6-4. ARP spoofing log fields

FIELD	DESCRIPTION
Date/Time	Date and time of the detection
Endpoint IP Address	IP address of the endpoint associated with the detection
Endpoint Host Name	Host name of the endpoint
Endpoint MAC Address	MAC address of the endpoint
Process ID	Process ID of the detected malware
File Name	File name of the detected malware

To view the ARP spoofing log:

1. Click **Logs > ARP Spoofing Log** to open the ARP Spoofing Log screen.
2. To export the contents of the log, click **Export All to CSV**.

Viewing and Exporting the Threat Mitigation Log

When the device attempts to respond to a detection by Threat Discovery Appliance (TDA), it generates an entry in the threat mitigation logs.

The threat mitigation log displays the following information.

TABLE 6-5. Threat mitigation log fields

FIELD	DESCRIPTION
Date/Time	Date and time the threat mitigation event occurred
IP Address	IP address of the endpoint
Host Name	Host name of the endpoint
Threat Event	Event type
Mitigation Status	Results of the mitigation attempt

To view and export the threat mitigation log:

1. Click **Logs > Threat Mitigation Log** to open the Threat Mitigation Log screen. By default all entries in the log are listed.
2. To export the threat mitigation log, click **Export All to CSV**.

> **Note:** The exported CSV contains all log entries that are listed in the table. Use the search criteria to narrow down the list.

Viewing and Exporting the Endpoint History

When Network VirusWall Enforcer matches a policy to an endpoint, it creates an endpoint history entry for the noncompliant endpoint. It also logs other policy violations by the same endpoint or changes to the status of the endpoint. If you register the device to Control Manager, you can configure the time interval for sending endpoint history entries to the Control Manager server.

The endpoint history displays the following information.

TABLE 6-6. Endpoint history fields

FIELD	DESCRIPTION
Date/Time	Date and time the policy violation occurred
Endpoint IP Address	IP address of the endpoint
Endpoint Host Name	Host name of the endpoint
Endpoint MAC Address	MAC address of the endpoint
Service	Violated enforcement criterion
Quarantined	Whether or not the endpoint has been isolated from the network

To view and export the endpoint history:

1. Click **Logs > Endpoint History** to open the Endpoint History screen. By default all entries in the log are listed.
2. To export the endpoint history, click **Export All to CSV**.

Note: The exported CSV contains all log entries that are listed in the table. Use the search criteria to narrow down the list.

Endpoint Details

Clicking an endpoint in the Endpoint History screen displays additional information about the endpoint as shown in the following table.

TABLE 6-7. Endpoint details

FIELD, SECTION, OR TAB	DESCRIPTION
Host name	Endpoint host name
IP address	Endpoint IP address
MAC address	Endpoint MAC address
Operating system	Endpoint platform
AV product installed	Supported antivirus product currently installed on the endpoint
Pattern version	Version of the pattern used by the installed antivirus product
Vulnerability list	Vulnerabilities found on the endpoint.
System threat list	Malware programs found on the endpoint
Registry key list	Prohibited entries in or entries missing from the system registry of the endpoint
Passed Policies	This section includes information about policies to which the endpoint is compliant
Policy Violations	This section includes information about policies that the endpoint has violated
Related Threat Mitigation Logs	This tab contains information on Threat Discovery Appliance detections that are associated with the endpoint

Releasing or Quarantining an Endpoint

In the Endpoint History screen, you can release an endpoint from being quarantined or you can quarantine an endpoint.

To release or quarantine an endpoint:

1. In the Endpoint History screen, locate and select the endpoint.
2. Click one of the following
   - **Release**—releases the endpoint from quarantine. If the endpoint is compliant, traffic from the endpoint can now pass the device.
   - **Quarantine**—places the endpoint under quarantine. The device starts to block traffic from the endpoint to isolate it from the network.

About Syslog Servers

Syslog is a standard for forwarding log messages to an IP network. Because it is a multi-platform standard supported by multiple device types, it can be used to consolidate log data from different sources to a central repository. In a syslog system, syslog servers are server-side applications that are able to receive and process the log messages.

Network VirusWall Enforcer can send logs to up to two syslog servers. Modify log settings to enable this functionality and specify the addresses of the syslog servers.

Additionally, Network VirusWall Enforcer can save logs on the disk. These logs will be collected by the Case Diagnostic Tool. Afterwards, the **Delete Logs on Disk** button can be used to delete logs saved in the hard disk.

For all these logs, adjust the log level to determine how much or how little information the system should provide. Level 6 is the lowest with Level 10 providing the most detailed information.

Using the System Log Viewer

The System Log Viewer is a user-friendly, stand-alone application that displays system debug log information in real-time as Network VirusWall Enforcer 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 and contact Trend Micro support, you may be asked to use the System Log Viewer.

Chapter 7

Troubleshooting and FAQs

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

This chapter discusses the following topics:

Troubleshooting

The section covers the following troubleshooting topics:

Hardware Issues

TABLE 7-1. Troubleshooting hardware issues

#	ISSUE	CORRECTIVE ACTION
1	Failopen does not work after I changed the speed of the regular port	Enable auto-negotiation for the devices connected to the Ethernet cables.

Configuration Issues

TABLE 7-2. Troubleshooting configuration issues

#	ISSUE	CORRECTIVE ACTION
Issues with Trend Micro Control Manager		
1	Network VirusWall Enforcer is unable to register with the Control Manager server.	Check all network connections and ensure you have correctly performed preconfiguration (refer to the *Installation and Deployment Guide* for more information). Network VirusWall Enforcer only registers to Control Manager through port 443. If Control Manager is installed on Windows 2003, configure the firewall to allow port 443 to communicate with Network VirusWall Enforcer. If the operating system on which Control Manager resides is Windows Server 2003, Network VirusWall Enforcer 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:** 1. Install Active Directory on the Windows Server 2003 server so Network VirusWall Enforcer 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 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 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 displays a **sync time** error and is unable to register to Control Manager server.	A sync time error displays when Network VirusWall Enforcer is unable to synchronize with the Control Manager server. To remedy this problem, click **Administration > Time Settings on** the web console. Then, select **Use a NTP server to update the time**.

TABLE 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
3	The Network VirusWall Enforcer icon on the Control Manager management console appears as active even when the device is offline.	When Network VirusWall Enforcer is turned off, or is disconnected from the network, the Control Manager agent for Network VirusWall Enforcer (MCP agent) 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 sent its last heartbeat. See the *Introducing Trend Micro Control Manager™* on page A-1 and the online help for information on changing heartbeat settings.
4	The icon and user name for a Network VirusWall Enforcer 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 device (see *Introducing Trend Micro Control Manager™* on page A-1 and online help for information on adding and removing products).
5	Network VirusWall Enforcer does not register to Control Manager even when Network VirusWall Enforcer 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 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 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
7	Network VirusWall Enforcer 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 can quarantine a maximum of 4096 endpoints and can drop all network traffic from more endpoints (over 4096). Reconsider your deployment plan based on the number of endpoints in your network.
8	A endpoint that was blocked because it does not have the latest Windows patch remains blocked even after running Windows Update.	On the endpoint, open the "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. Reassess the endpoint through the agent icon or open a web browser to display the assessment page and click the "reassess" button.
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, select **Display the assessment screen**.

TABLE 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
11	Network VirusWall Enforcer Policy Enforcement does not correctly identify noncompliant endpoints.	An HTTP proxy server located between Network VirusWall Enforcer and endpoints on the network may prevent Network VirusWall Enforcer 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 Policy Enforcement may not be able to detect the status of endpoints on the network.
12	Network VirusWall Enforcer is unable to implement Outbreak Prevention Policies to block endpoint ports.	If an endpoint routes its traffic through a proxy server, it 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 does not block the endpoint traffic.
13	When Kerberos authentication is used, user authentication does not function as expected.	Check the clock sync between the authentication server and Network VirusWall Enforcer. The authentication server and Network VirusWall Enforcer should have the same time setting. For Kerberos and MD5 authentication, users only need to provide account information (without the domain) and password.
14	An endpoint in a different subnet does not match user authentication.	Add a bridge IP address that is in the same subnet as the endpoint.
15	Network VirusWall Enforcer cannot update the endpoint status using the TMAgent.	Add a bridge IP address that is in the same subnet as the endpoint and bind it to a port.
16	An error displays about not being able to run ActiveX when the endpoint tries to access the Internet.	Locate the %windir%\PEAgent folder and remove the PEAgentSFX.exe file on the endpoint computer.
Other issues		

TABLE 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
17	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.
18	Network VirusWall Enforcer is either unable to obtain, or gets incorrect, DNS server information.	This occurs if the DHCP server that assigns the Network VirusWall Enforcer IP address does not specify a DNS server. Confirm your network DHCP and DNS server settings are correct (see *Management IP Address* on page 2-7).
19	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.
20	Exporting the configuration file display garbled characters.	This is a known issue. The garbled characters do not cause any adverse effects on the exported configuration file.
21	When a NAT device resides between Control Manager server and the bridge port of the device and if the device uses a dynamic IP address to register to Control Manager, the network administrator may need to change port forwarding settings often.	Set Network VirusWall Enforcer to use a static IP address.

TABLE 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
22	Users cannot see popup messages on endpoints with 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 exceptions in the Windows Firewall may not be present. Network VirusWall Enforcer uses ports TPC 139 and UDP 137 to deliver popup messages through the Messenger service. If at any point a user clicks **Restore Defaults** on the Windows Firewall, the necessary exceptions are removed. **To re-enable the necessary ports:** 1. Go to **Windows Security Center** > **Windows Firewall** > **Exceptions** > **File and Printer Sharing**. 2. Check to see if "TCP 139 Port" and "UDP 137 Port " are selected in the Windows Firewall exceptions list. If these ports are not selected, select them. 3. Click **Save**.
23	The root domain controller cannot be deployed.	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
24	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.
25	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.
26	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.

TABLE 7-2. Troubleshooting configuration issues (Continued)

#	ISSUE	CORRECTIVE ACTION
27	Unable to perform scheduled update correctly.	Ensure that the scheduled update configurations for updating the Pattern Release History and other pattern/engines are not set to update at the same time.
28	Unable to see blocking page when the endpoint and Network VirusWall Enforcer 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 its default gateway. 2. If the endpoint can reach its 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.
29	Automatically logged off the Preconfiguration console	If you change the current window size, Network VirusWall Enforcer automatically logs off.
30	Unable to download Pattern Release History using DNS	Try to use a different DNS server.
31	Unable to ping the device	You may have outdated address resolution information. Use the "arp -d"command to clear the ARP table on the computer from which you are pinging the Network VirusWall Enforcer device.

Control Manager Communication Issues

When troubleshooting Control Manager and Network VirusWall Enforcer integration and communication, check whether you have the correct time server settings.

Checking the Time Server Settings

Depending on the characteristics of your network, use a Windows Network Time Protocol (NTP) server or a Control Manager server as your time server. Windows NTP requires Active Directory and can provide additional features for Active Directory endpoints.

To check time server settings:

On the web console, click **Time Settings** on the **Administration** menu.

Frequently Asked Questions (FAQs)

This section answers the following common questions about Network VirusWall Enforcer.

Hardware and Deployment

Does Network VirusWall Enforcer support Gigabit Ethernet?

Yes, all Network VirusWall Enforcer ports support Gigabit Ethernet.

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

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

When I shutdown Network VirusWall Enforcer, the LEDs of the bypass cards are not on. Does this mean that the bypass feature does not work?

The bypass feature passes traffic even if the LEDs are not lit as long as failopen is enabled.

I have disabled ports from the Preconfiguration console, but the LEDs for these ports are still on. Does this mean that they are not disabled?

The LEDs stay on even when the ports are disabled.

What features and functionality are not supported on IPv6 networks?

The following features are not supported on IPv6 networks:

- Threat mitigation with Threat Discovery Appliance
- Policies that require user authentication using Kerberos
- Program rescue
- Enforcement of network application policies (port activity, instant messengers, file transfers, and Outbreak Prevention Policy)
- Remote detection of endpoint operating systems for policy enforcement
- ActiveUpdate through Network Address Translation/Protocol Translation (NAT-PT)
- Addressing:
  - Dynamic addressing from a Windows DHCPv6 server
  - Limited Linux DHCPv6 support; the device can obtain an IP address, a prefix, and a DNS from a Linux DHCPv6 server, but it will not be able to obtain gateway settings.
- Specifying a link-local IP address as the update source

Network

Does Network VirusWall Enforcer support Spanning Tree Protocol (STP)?

Network VirusWall Enforcer does not support STP traffic. STP traffic, however, bypasses Network VirusWall Enforcer.When using STP, ensure that STP is enabled on your L2 or L3 device. Otherwise, if one of the links fails in a port redundancy deployment, Network VirusWall Enforcer will be unable to route STP traffic. Refer to the *Installation and Deployment Guide* for details.

Does Network VirusWall Enforcer ignore Voice over Internet Protocol (VoIP) packets in a network with VoIP?

Network VirusWall Enforcer scans every packet that passes through it in real time. However, Network VirusWall Enforcer ignores VoIP packets because the data transmitted by these packets is very small.

Does Network VirusWall Enforcer pass all non-IP traffic?

Yes, Network VirusWall Enforcer passes all non-IP traffic.

How does Network VirusWall Enforcer 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.

Does the device block HTTP uploads?

This version of the device does not support this feature.

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

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

How does Network VirusWall Enforcer handle EtherChannel?

Network VirusWall Enforcer supports EtherChannel configurations. It also supports trunked gigabit lines.

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

Network VirusWall Enforcer does not amplify signals or packets.

Why am I unable to access the device when I set it to use a static IP address?

This can occur if the IP address has been duplicated in the network. Ensure that no other host is using the same IP address.

Why does the dynamic IP address remain changed after I change the subnet?

The device should dynamically get an IP address on the new subnet when the lease to its current IP address expires. To immediately get a new IP address, restart the device or set a static IP address and then change settings back to "dynamic IP address".

Why am I unable to log on to the domain from a new endpoint?

If you have a policy that requires user authentication, new endpoints are automatically blocked from the network, including the LDAP server. This will prevent users from logging on to the domain. As a workaround, add your LDAP server to the global exception list so that all authentication packets directed at the server are bypassed.

Why are the host names of some endpoints not listed in the endpoint history?

To help ensure that endpoints are detected and their host names are listed:

- Enable host name resolution in the log settings.
- Consider stopping firewall on the endpoints. Firewalls can prevent remote detection of antivirus products on endpoints.

I configured Network VirusWall Enforcer to use an IPv6 address, but now it is unable to locate endpoints.

If configured to use an IPv6 address, Network VirusWall Enforcer resolves host names using the specified IPv6 DNS server. To help ensure that Network VirusWall Enforcer can locate all endpoints, synchronize the records on your DNS servers, particularly between the DNS server specified for use by Network VirusWall Enforcer and all your other IPv6 and IPv4 servers.

Network VirusWall Enforcer is unable to connect to an endpoint in another segment and is using its link-local address to reach the endpoint. How do I resolve this?

When configured to use an IPv6 address, Network VirusWall Enforcer automatically uses its link-local address to connect to an endpoint on a different network segment. To allow Network VirusWall Enforcer to reach an endpoint behind a router in another network segment, ensure that you create a static route to the segment where the endpoint resides.

Agent

Can an agent that has been removed be reinstalled?

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

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

Check for the following:

- If the endpoint is running Windows 98, ME, or XP Home, remote login is not supported.
- In Windows XP Professional, endpoint users need to disable simple file sharing.
- Endpoint firewall filters blocking remote login installation must be disabled.
- Ensure the endpoint user account has administrator privileges and that ActiveX controls can be downloaded.

What can prevent successful deployment of the agent?

Assuming that the endpoint platform is supported, the following can prevent successful deployment of agent:

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

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

The default Internet Explorer security settings prevent deployment. Change the security settings on the endpoint's Internet Explorer to enable JavaScript, signed ActiveX download/execute.

Why is the agent unable to install successfully?

Network VirusWall Enforcer does not support installation of agents on non-Windows platforms or on Windows NT, 95, 98, and ME.

Endpoints

Does Network VirusWall Enforcer support endpoints running Windows 95, 98, and ME?

These platforms are not supported for policy enforcement using the persistent and single-use agent deployment options. Network VirusWall Enforcer, however, can still perform some agent-free enforcement actions on these endpoints, including network virus scanning.

Does the "Remote login, ActiveX" agent deployment option be used on endpoints that are behind a NAT?

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

Can the device detect file transfers on all kinds of endpoints?

The device cannot detect file transfers on Windows Vista and Windows Server 2008 endpoints.

When a noncompliant endpoint is blocked and the endpoint user clicks the "reassess" button on the blocking page, why is the requested page allowed to display?

If you select to display the assessment screen under endpoint notification settings, packets are bypassed during assessment. This allows the requested page to display.

User Authentication

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

In this release, Network VirusWall Enforcer 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.)

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.

Antivirus Product Scan

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.

Does Network VirusWall Enforcer support antivirus program scan for Kaspersky Chinese version 5.0.388?

Please refer to the list of supported products on the web console for the latest information.

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

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

Instant Messengers

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

If you enforce a policy that assesses ICQ activity, the ICQ status on a matched endpoint will change to offline if the endpoint sends a file through ICQ.

Can Network VirusWall Enforcer block files shared through Windows Live (MSN) Messenger shared folder?

Yes, Network VirusWall Enforcer supports blocking of files in the Windows Live Messenger shared folder.

Will Network VirusWall Enforcer block activities through SOCKS 4 and SOCKS 5 proxy servers?

This version of the device does not block instant messenger activities through SOCKS 4 and SOCKS 5 proxy servers.

Why is Windows Live (MSN) Messenger blocked?

If the HTTP file blocking settings match `gateway.dll`, Windows Live Messenger will be blocked. Avoid using `*.dll` when specifying files to block.

Does instant messenger assessment support Live Communications Server?

This version of the device does not support Live Communication Server.

URL Redirection

Why can't the endpoint access the Redirect URL?

If you have configured the redirect URL in capital letters, endpoints are not able to access the URL. The URL scan feature is case sensitive and Internet Explorer automatically converts the URL to lowercase so the endpoint cannot access the Redirect URL.

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 redirect or exception URLs have double-byte characters?

Yes, Network VirusWall Enforcer supports double-byte characters in these URLs.

Why is HTTPS traffic not redirecting to the blocking page?

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

Why is an HTTPS page being blocked?

This can occur when the HTTPS page request triggers an assessment. The device cannot decrypt information from HTTPS packets and cannot push the page back as a response.

To allow the HTTPS page to display, the endpoint user can first access an HTTP page to trigger the assessment. As soon as the assessment completes, the endpoint will be able to access any HTTPS page.

Why are my endpoints prevented from accessing a redirect URL?

It is best practice to add a redirect URL to the URL exceptions. This allows endpoints to bypass the particular policies that have this URL as an exception. However, when an endpoint accesses a redirect URL, another policy may be triggered. If this secondary policy does not have the redirect URL in its exception list, the endpoint may be blocked from accessing the URL. This can occur, for example, if a policy for IPv4 traffic redirects endpoints to an IPv6 URL, triggering another policy for IPv6 traffic.

To avoid this issue, try to maintain the same set of URL exceptions in all your policies. Or ensure that, if in case a redirect URL can trigger another policy, that the policy that may be triggered has the redirect URL as an exception.

Configuration Backup

How can I back up Network VirusWall Enforcer configuration information?

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

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

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

Yes, the **System Tasks** option on the Preconfiguration console allows you to import and export the Network VirusWall Enforcer configuration information.

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

What is the name of the exported configuration file?

When you export configuration information, Network VirusWall Enforcer exports the information to a file named "NVWECONF".

Preconfiguration and Web Consoles

Why does the endpoint browser display "Page not found" after Network VirusWall Enforcer performs an assessment of the endpoint?

If you use a proxy script in your network, Network VirusWall Enforcer 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 will not assess endpoints that use that proxy server.

Why does the popup window display the Network VirusWall Enforcer logon screen?

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

How many concurrent HTTP, HTTPS, and SSH sessions on the management consoles are allowed?

The device supports up to 10 concurrent HTTP and 10 concurrent HTTPS sessions. It can support more than 10 concurrent SSH sessions.

After restarting the device, are network services immediately available as soon as the Preconfiguration console displays?

Network services, such as SSH and HTTP, will be unable to respond for about 33 seconds.

Why is the logon screen displayed again?

You have timed out of the session and will need to log on again.

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

You can add new administrator and power user accounts through the web console. Administrator accounts have full access to the Preconfiguration console, while power user accounts have read-only access to the Preconfiguration console.

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.

Why did my session terminate while downloading case diagnostic information?

When multiple requests are made to download case diagnostic information, the first session terminates when the second session begins the download. No error message displays.

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

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

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

You may need to add the Network VirusWall Enforcer IP address to the trusted sites list on Internet Explorer.

Why does the web console stop displaying after I modify the management IP address?

The web console IP address also changes when you modify the management IP address. To access the console, access it using the new IP address.

Logs

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

Network VirusWall Enforcer sends its normal logs to the Control Manager server. Alternatively, Network VirusWall Enforcer can send system logs (which also include debug information) to any computer on the network. See *Using Logs* on page 6-4 for more information.

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

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

Can I configure the time interval for logs?

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

Where can I find information on endpoints running non-Windows and unknown operating systems?

They are included in the violation count.

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.

Are logs deleted when the device resets?

When the device resets, data in the Event Log, the Network Virus Log, and the Threat Mitigation Log is deleted from the device.

Why does the total number of successful cleanup actions in the Threat Mitigation Log not match detailed cleanup information?

The total does not include registry cleanup results. Detailed information reveals registry cleanup results that are not reflected in the total.

Control Manager

Can I use another Control Manager account to register and manage Network VirusWall Enforcer devices?

You can use any Control Manager account in place of the root account user ID. However, Trend Micro recommends using the root account because if you delete the user ID specified during registration, you will have difficulty managing the device.

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

No, you cannot register a device to more than one Control Manager server. You can use the Preconfiguration console to register devices to a Control Manager server.

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

Yes, changing the Network VirusWall Enforcer IP address through the Preconfiguration console will temporary disconnect the device from the Control Manager server.

Why am I not receiving Control Manager notifications for network virus detections?

Ensure that you have registered the device to Control Manager and have configured network virus alerts on Control Manager.

If you still do not receive notifications, there are several possible reasons:

- To avoid spamming recipients, Control Manager sends notification messages only every two minutes. No notifications are triggered until after two minutes since the last notification.
- The Control Manager has rules for triggering notifications. Check whether the notification triggers are set too high.

Other Questions

Why is preconfiguration not discussed 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 *Installation and Deployment Guide*.

When can Damage Cleanup Services be deployed with remote login?

Damage Cleanup Services can be deployed with remote login when the network virus action is drop or quarantine.

Can blocked files be transferred?

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

How do I enter boot menu to perform a rescue or rollback?

When the device starts, press ESC as soon the message **Press ESC to enter the menu** displays. Note that this message will display only within a very short period (approximately one second).

Why is the authentication page displayed repeatedly?

If Internet Explorer is configured to use a proxy server and the matching policy performs user authentication, the authentication page may display repeatedly.

You can perform the following workaround:

- Modify your proxy exception list to include IP address of the device.
- In the web console, modify the global exception list to include the IP address of the proxy server.

WARNING! **Adding a proxy server to the global exception list prevents Network VirusWall Enforcer from scanning HTTP traffic handled by this server and can severely affect security on your network.**

Chapter 8

Getting Support

This chapter contains information on how you can get technical support. Register your product to be eligible for support.

This chapter discusses the following topics:

Before Contacting Technical Support

Before contacting technical support, see if these resources can help you address your problem:

- **Product documentation**—the *Administrator's Guide*, *Installation and Deployment Guide*, and *Online Help* provide comprehensive information about Network VirusWall Enforcer. Search these documents for helpful information.
- **Knowledge Base**—a key part of our technical support website, the Trend Micro Knowledge Base contains the latest information about Trend Micro products.

  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

- Online Help—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, visit:

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

Having the following information ready before you contact our support staff can help them resolve problems faster:

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

Sending Infected Files to Trend Micro

If you suspect an undetected file to be malware, submit the suspicious file to Trend Micro using the following website:

http://subwiz.trendmicro.com/SubWiz/Default.asp

Please provide a brief description of the symptoms you have witnessed. Our team of virus engineers will analyze the file to identify and characterize any viruses it may contain.

Introducing TrendLabs

Trend Micro TrendLabs[SM] 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:

www.trendmicro.com/en/security/trendlabs/overview.htm

Other Useful Resources

Trend Micro offers a host of services from its website:

http://www.trendmicro.com

Internet-based tools and services include:

- HouseCall™ — Trend Micro online virus scanner
- Virus risk assessment—the Trend Micro online virus protection assessment program for corporate networks

Appendix A

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.

This chapter discusses the following topics:

Control Manager Standard and Advanced

Control Manager is available in two versions; Standard and Advanced. Control Manager Advanced includes features that Control Manager Standard does not. For example, Control Manager Advanced supports a cascading management structure. This means the Control Manager network can be managed by a parent Control Manager Advanced server with several child Control Manager Advanced servers reporting to the parent Control Manager Advanced server. The parent server acts as a hub for the entire network.

Note: Control Manager 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 5.0 Standard servers cannot be child servers.

How to Use Control Manager

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

TABLE A-1. Control Manager features

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/malware and content security policies.

TABLE A-1. Control Manager features (Continued)

FEATURE	DESCRIPTION
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/malware 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 through 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 managed products in real-time. Control Manager immediately sends configuration modifications made on the management console to the managed products. System administrators can run manual scans from the management console. This command system is indispensable during a virus/malware outbreak.

TABLE A-1. Control Manager features (Continued)

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 products are up-to-date.
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.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy. Refer to *Table A-2* on page A-5 for a list of components Control Manager uses.

TABLE A-2. Control Manager components

COMPONENT	DESCRIPTION
Control Manager server	Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features: An SQL **database** that stores managed product configurations and logs Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. A **web server** that hosts the Control Manager **management console** A **mail server** that delivers event **notifications** through email messages Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure **Event Center** to send notifications through email messages, Windows event log, MSN Messenger, SNMP, syslog, pager, or any in-house/industry standard application used by your organization to send notification.

TABLE A-2. Control Manager components (Continued)

COMPONENT	DESCRIPTION
Control Manager server	A **report server**, *present only in the Advanced Edition*, that generates antivirus and content security product reports A Control Manager report is an online collection of figures about virus/malware and content security events that occur on the Control Manager network.
Trend Micro Management Communication Protocol	MCP handles the Control Manager server interaction with managed products that support the next generation agent MCP is the new backbone for the Control Manager system. MCP agents install with managed products and uses one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.
Trend Micro Infrastructure	Handles the Control Manager server interaction with older managed products The Communicator, or the Message Routing Framework, was the communication backbone of the Control Manager system. The communicator is a component of the Trend Micro Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. The communicator interacts with Control Manager 2.x agents to communicate to older managed products.

TABLE A-2. Control Manager components (Continued)

COMPONENT	DESCRIPTION
Control Manager 2.x Agents	Receives commands from the Control Manager server and sends status information and logs to the Control Manager server The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Hence, install agents on the same computer as managed products.
Web-Based Management Console	Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™ The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.

Registering Network VirusWall Enforcer to Control Manager

Before registering a Network VirusWall Enforcer device to a Control Manager server, you must ensure that both the device and the Control Manager server belong to the same network segment.

To register Network VirusWall Enforcer to Control Manager:

1. Log on to the Preconfiguration console.
2. On the **Main Menu** of the Preconfiguration console, select **Register to Trend Micro Control Manager** and press **Enter**.

Note: Control Manager uses the name specified in the Host name field to identify Network VirusWall Enforcer 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**, and 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 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, 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, click **Products**. The Product Directory screen appears.
10. The Network VirusWall Enforcer appears in the Product Directory tree.

Control Manager User Access

Access to the Control Manager web console and Control Manager features depends on your user account and account type.

For detailed information about creating new user accounts or account types, see the *Control Manager Administrator's Guide* or the *Control Manager Tutorial*.

Control Manager 5.0 user access control provides greater flexibility than previous versions of Control Manager. Control Manager administrators can now restrict user access to the following:

- Control Manager menu items and screens
- Managed products and all information relating to the managed products
- Specific Control Manager features

This means that not all Control Manager screens, features, or managed products and their information are available for all users.

User access is split into the following sections:

TABLE A-3. Control Manager user access options

SECTION	DESCRIPTION
My Account	The My Account screen contains all the account information Control Manager has for a specific user. The information on the My Account screen varies from user to user.
User Accounts	The User Accounts screen displays all Control Manager users. The screen also provides functions allowing you to create and maintain Control Manager user accounts. Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are: Execute Configure Edit Directory

TABLE A-3. Control Manager user access options (Continued)

SECTION	DESCRIPTION
User Groups	The Group Accounts screen contains Control Manager groups and provides options for creating groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow Control Manager administrators to create a group that shares the same access rights.
User Types	The Account Types screen displays all Control Manager user roles. The screen also provides functions allowing you to create and maintain Control Manager user roles. User roles define which areas of the Control Manager web console a user can access.

Network VirusWall Enforcer User Access

Network VirusWall Enforcer user access is similar to Control Manager user access. Administrators can control which parts of the Network VirusWall Enforcer web console users can access (Power User, Operator, or Administrator).

All user accounts created in Control Manager have administrator access to any managed product to which the user has access. This creates a problem if an administrator wants to restrict a user's access to Power User on Network VirusWall Enforcer devices while allowing access to Control Manager.

Managed Product MCP Agent Heartbeat

To monitor the status of Network VirusWall Enforcer devices, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the Network VirusWall Enforcer device and to check for commands to the Network VirusWall Enforcer device from Control Manager. The Control Manager web console then presents the product status. This means that the Network VirusWall Enforcer device 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 device in a sequential manner in the background. Control Manager changes the status of Network VirusWall Enforcer devices to offline, when a fixed period of time elapses without a heartbeat from the Network VirusWall Enforcer device.

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

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

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 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 device activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Agent/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 Agent/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.

Note: The default setting for all managed products registered to Control Manager is 24 hours.

To configure the communication schedule for a Network VirusWall Enforcer device:

1. Mouseover **Administration > Settings** from the Control Manager web console. A drop-down menu appears.
2. Click **Agent Communication Schedule**. The Agent Communication Schedule screen appears.
3. Click the link for the Network VirusWall Enforcer device to modify. The Set Communicator Schedule screen appears.

4. Specify the time that the Network VirusWall Enforcer device communicates with Control Manager.
5. Click **Save**.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest managed product 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:

TABLE A-4. Control Manager heartbeat intervals

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.

WARNING! Modification to the heartbeat settings are global and affect all managed products registered to Control Manager.

To configure heartbeat settings:

1. Mouseover **Administration > Settings** from the Control Manager web console. A drop-down menu appears.
2. Click **Heartbeat Settings**. The Heartbeat Settings screen appears.
3. On the working area, leave the default values or specify new settings for the following:
   - **Report managed product status every:** Defines how often the managed product responds to Control Manager server messages. Valid values are between 5 to 480 minutes
   - **If no communication, set status as abnormal after:** Specifies how long Control Manager waits for a response from the managed product before changing its management console status to (inactive). Valid values are between 15 and 1440 minutes.

   Note: The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

4. Click **Save**.

Managing Network VirusWall Enforcer from Control Manager

A managed product refers to a Network VirusWall Enforcer 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 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. The following table lists the menu items and buttons on the Product Directory screen:

TABLE A-5. Control Manager product directory items

MENU ITEMS	DESCRIPTION
Advanced Search	Click this button to specify search criteria to perform a search for one or more managed products.
Configure	Click this button, after selecting a managed product/directory, to log on to the web-based console and configure a managed product.
Tasks	Click this button, after selecting a managed product/directory, to perform specific function (such as deploying the latest components) to a specific or groups of managed product or child servers. Initiating a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Logs	Click this button after selecting a managed product/directory to query and view product logs. If you select a managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the directory.
Directory Management	Click this button to open the Directory Management screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.
BUTTONS	**DESCRIPTION**
Search	Click this button, after typing a managed product's name, to perform a search for the specified managed product.

TABLE A-5. Control Manager product directory items (Continued)

MENU ITEMS	DESCRIPTION
Status	Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.
Folder	Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product clients found in the directory.

Understanding Product Directory

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

- Configuring managed products
- Request products to perform a Scan Now (if this command is supported)
- View product information, and details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on)
- View product-level logs
- Deploy virus pattern, scan engine, anti-spam rule, and program updates

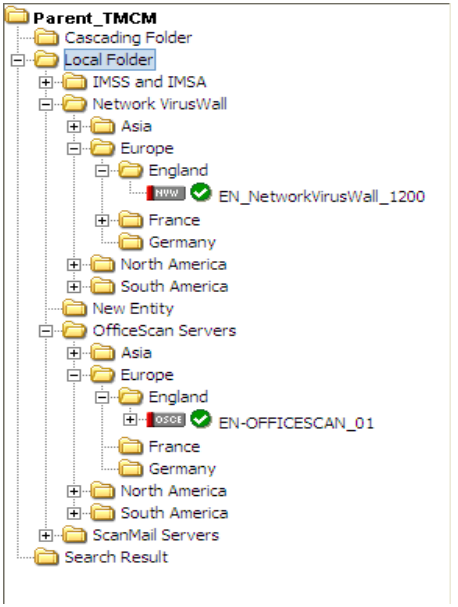
Plan the structure carefully, because the structure also affects the following:

TABLE A-6. Planning the product structure

1. Consideration	2. Impact
3. User access	4. When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire Directory. Granting access to a specific managed product only grants access to that specific product.
5. Deployment planning	6. Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
7. Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments	8. OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

Note: Managed products belonging to child Control Manager servers cannot have tasks applied to them by the parent Control Manager server.

A sample Product Directory appears below:



Managed products identify the registered antivirus or content security product, as well as provide the connection status.

Refer to the Control Manager *Understanding Product Directory* online help topic for the list of Product Directory icons.

Access the Product Directory

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

Note: Viewing and accessing the folders in the Product Directory depends on the user account folder access rights.

To access the Product Directory:

- Click **Products** on the main menu. The Product Directory screen appears.

Deploy Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your Network VirusWall Enforcer devices and other managed products on demand.

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

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. Mouseover **Tasks**. A drop down menu appears.
3. Select **Deploy <component>** from the menu. The **Deploy <component>** screen appears in the Product Directory work area.
4. Click **Deploy Now** to start the manual deployment of new components.
5. Monitor the progress using Command Tracking.
6. Click **Command Details** to view details for the task.

View Network VirusWall Enforcer Status Summaries

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

There are two ways to view the Network VirusWall Enforcer 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. Select the desired folder or Network VirusWall Enforcer device.

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 list.

Configure Network VirusWall Enforcer Devices and Managed Products

Depending on the product and agent version you can configure the managed product from the managed product's web console or through a Control Manager-generated console.

To configure a product:

1. Access the Product Directory.
2. Select the desired managed product from the product tree. The product status appears in the right-hand area of the screen.
3. Mouseover **Configure** from the product tree menu. A drop-down menu appears.
4. Select one of the following:

   Configuration Replication: The Configuration Settings screen appears.

   a. Select the folder to which the selected managed product's settings replicate from the Product Directory structure.

   b. Click **Replicate**. The selected managed product's settings replicate to the target managed products.

   <Managed Product Name> Single Sign On: The managed product's web-based console or Control Manager-generated console appears.

   a. Configure the managed product from the web console.

Issue Tasks to Network VirusWall Enforcer Devices and Managed Products

Use the options under the Tasks menu item to start actions on a group or specific Network VirusWall Enforcer device or managed product. You can perform the following tasks on Network VirusWall Enforcer devices:

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

To issue tasks to Network VirusWall Enforcer devices:

1. Click **Products** on the main menu.
2. Mouseover **Tasks**. A drop down menu appears.
3. Select a task from the menu. A screen appears in the Product Directory work area.
4. Initiate the task from the work area.
5. Monitor the task's progress using Command Tracking.
6. Click **Command Details** to view details for the task.

Query and View Network VirusWall Enforcer and Managed Product Logs

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

For detailed information about querying logs or data views, see the *Control Manager Administrator's Guide* or the *Control Manager Tutorial*.

To query and view Network VirusWall Enforcer device logs:

1. Click **Products** on the main menu.
2. Select the desired Network VirusWall Enforcer device or folder from the Product Directory tree.
3. Click **Logs** from the Product Directory menu. The Ad Hoc Query Step 2: Data View screen appears.

4. Select the data to query by specifying a data view for the log.
5. Click **Next**. The Step 3: Query Criteria screen appears.
6. Specify the data to appear in the log and the order in which the data appears:
   a. Click **Change column display**. The Select Display Sequence screen appears.

      Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.

   b. Select a query column from the Available Fields list. The selected item highlights.

   c. Select multiple items using the `Shift` or `CTRL` keys.

   d. Click **>** to add items to the Selected Fields list.

   e. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

   f. Click **Back** when the sequence fits your requirements.
7. Specify the filtering criteria for the data:

Note: When querying for summary data, users must specify the items under **Required criteria**.

Required criteria:

- Specify a Summary Time for the data or whether you want COOKIES (spyware data only) to appear in your reports.

Custom criteria:

a. Specify the criteria filtering rules for the data categories:
   - **All of the criteria:** This selection acts as a logical AND function. Data appearing in the report must meet all the filtering criteria.
   - **Any of the criteria:** This selection acts as a logical OR function. Data appearing in the report must meet any of the filtering criteria.

b. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

Tip: If you do not specify any filtering criteria, the Ad Hoc query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

---

8. To save the query:

Saving queries allows you to reuse them or to share them with others.

a. Click **Save this query to the saved Ad Hoc Queries list**.

b. Type a name for the saved query in the **Query Name** field.

9. Click **Query**. The Results screen appears.

Tip: To display more results on a single screen select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

---

10. To save the settings for the query:

a. Click **Save query settings**. A confirmation dialog box appears.

b. Type a name for the saved query in the **Query Name** field.

c. Click **OK**. The saved query appears on the Saved Ad Hoc Queries screen.

Recover Network VirusWall Enforcer Devices Removed from the Product Directory

The following scenarios can cause Control Manager to delete Network VirusWall Enforcer 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 the Network VirusWall Enforcer device using the Directory Manager

If a Control Manager server's Network VirusWall Enforcer device 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 devices removed from the Product Directory:

- Restart Trend Micro Control Manager service on the managed product server.
- Manually re-register to Control Manager. MCP agents do not re-register automatically and need to be manually re-registered to the Control Manager server.

Stopping and Restarting Control Manager Services

Use the Windows Services screen, on the server where Control Manager installs, to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro CCGI
- Trend Micro Control Manager

Note: These are the services that run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services, Damage Cleanup Services).

To restart Control Manager services:

1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click **<Control Manager service>**, and then click **Stop**.
3. Right-click **<Control Manager service>**, and then click **Start**.

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

Use the Search button to quickly find and locate a specific managed product in the Product Directory.

To search for a folder or managed product:

1. Access Product Directory.
2. Type the entity display name of the managed product in the Find Entity field.
3. Click **Search**.

To perform an advanced search:

1. Access Product Directory.
2. Click **Advanced Search**. The Advanced Search screen appears.
3. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
4. Click **Search** to start searching. Search results appear in the **Search Result** folder of the Product Directory.

Refresh the Product Directory

To refresh the Product Directory:

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

Understanding the Directory Management Screen

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

Use the Directory Management screen 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).

The Directory allows you to create, modify, or delete folders, and move managed products between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the managed products belonging to each folder. Consider the following factors when planning and implementing your folder and managed product structure:

- Product Directory
- User Accounts

- Deployment Plans
- Ad Hoc Query
- Control Manager reports

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

TABLE A-7. Control Manager product grouping types

GROUPING TYPE	ADVANTAGES	DISADVANTAGES
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

Using the Directory Management Screen Options

Directory Manager provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products/directories in the Product Directory

> **Note:** The **Permission Keep** check box allows a folder to keep its source permission when moved.

- Remove managed products/directories from the Product Directory

Use these options to manipulate and organize managed products in your Control Manager network

To use and apply changes in the Directory Management screen:

- Select a managed product/directory and click **Rename** to rename a managed product/directory
- Click + or the folder to display the managed products belonging to a folder
- Drag-and-drop managed products/directories to move the managed products/directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory

Accessing Directory Management

Use Directory Management to group managed products together.

To access the Directory Management:

1. Click **Products** from the main menu. The Product Directory screen appears.
2. Click **Directory Management** from the Product Directory menu. The Directory Management screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Management screen.
2. Select **Local Folder**. The Local Folder highlights.
3. Click **Add Folder**. The Add Directory dialog box appears.
4. Type a name for the new directory in the **Directory name** field.
5. Click **Save**.

Note: 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 alphabetic characters (a/A to z/Z).

Renaming Folders or Managed Products

Rename directories and managed products from the Directory Manager.

To rename a folder or managed product:

1. Access the Directory Management screen.
2. Select the managed product/directory to rename. The item highlights in the Product Directory.
3. Click **Rename**. The Rename Directory dialog box appears.
4. Type a name for the managed product/directory in the **Directory name** field.
5. Click **Save**. A confirmation dialog box appears.
6. Click **OK**. The managed product/directory displays in the Product Directory with the new name.

Note: Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

Moving Folders or Managed Products

When moving folders pay special attention to the **Keep the current user access permissions when moving managed products/folders** check box. If you select this check box and move a managed product/folder, the managed product/folder keeps the permissions from its source folder. If you clear the **Permission Keep** check box, and then move a managed product/folder, the managed product/folder assumes the access permissions from its new parent folder.

To transfer or move a folder or managed product to another location:

1. Access the Directory Management screen.
2. On the working area, select the folder or managed product to move.
3. Drag-and-drop the folder or managed product to the target new location.
4. Click **Save**.

Deleting User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a managed product which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a managed product which causes it to unregister from the Control Manager server.

Note: You cannot delete the New entity folder.

To delete a user-defined folder:

1. Access the Directory Management screen.
2. Select the managed product/directory to delete. The item highlights.
3. Click **Delete**. A confirmation dialog box appears.
4. Click **OK**.
5. Click **Save**.

WARNING! Take caution when deleting user-defined folders, you may accidentally delete a managed product that you do not want to remove.

Downloading and Deploying New Components

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:** Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections.
- **Anti-spam rules:** Anti-spam rules are the Trend Micro-provided files used for anti-spam and content filtering.

- **Engines:** Engines refer to virus/malware scan engines, damage cleanup engine, VirusWall engines, the spyware/grayware engine and so on. These components perform the actual scanning and cleaning functions.
- **Product program:** Product specific components (for example, Service Pack releases)

Note: Only registered users are eligible for components update. To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

The Component List screen presents a full list of all components Control Manager has available for managed products. The list also matches components with managed products that use the component. Click **Updates > Component List** to open the Component List screen.

The Control Manager server only retains the latest component version. You can trace a component's version history by viewing <root>:\Program Files\Trend Micro\Control Manager\AU_log\TmuDump.txt entries. TmuDump.txt generates when ActiveUpdate debugging is enabled.

Tip: To minimize Control Manager network traffic, disable the download of components that have no corresponding managed products or services. When you register managed products or activate services at a later time, be sure to configure the manual or scheduled download of applicable components.

Manually Downloading Components

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.

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. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Deployment Plan** from the drop-down menu. The Deployment Plan screen appears.
3. Click **Add**. The **Add New Plan** screen appears.
4. On the Add New Plan screen, type a deployment plan name in the **Name** field.
5. Click **Add** 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. Mouseover **Administration**. A drop-down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.
4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
6. Type the host name or IP address of the server in the **Server name or IP address** field.
7. Type a port number in the **Port** field.
8. Type a log on name and password if your server requires authentication.
9. Click **Save**.

Step 3: Select the components to update

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.
3. 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 components to download. To select all components for a group, select:
      - **All Pattern files/Cleanup templates**
      - **All Anti-spam rules**
      - **All Engines**
      - **Product programs**

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 Connection 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.

Accessing Manual Download

Use the Manual Download screen to immediately obtain new components.

To access the Manual Download screen:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.

Configuring Manual Download Settings

The Download Settings group defines the components Control Manager manually downloads and the download method.

To configure manual download settings:

1. Access the Manual Download screen.
2. On the working area under Download Settings:
   a. Select components that you want to download.
   b. Select the update source:
      - **Internet:** Trend Micro update server to 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.

   c. 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.

---

   d. 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 Connection Settings screen.
3. Click **Save**.

Configuring Manual Download and Automatic Deployment Settings

Use the Automatic Deployment Settings group to set how Control Manager deploys updates.

To configure manual download Automatic Deployment Settings:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.

3. Select when to deploy downloaded components from the Schedule area:
   - **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.

---

4. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
5. Click **Save**.

Note: The settings in Automatic Deployment Settings only apply to components used by managed products.

For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

Configuring 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 is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

Note: Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

Example: The administrator decides that they do not want Control Manager to download components on weekends or after working hours throughout the week. The administrator enables **Daily Schedule Exception** and selects **Saturday** and **Sunday**. The administrator then enables **Hourly Schedule Exception** and specifies the hours of **00:00 to 9:00** and **18:00 to 24:00**.

To configure scheduled download exceptions:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Scheduled Download Exceptions**. The Scheduled Download Exceptions screen appears.
4. 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, Control Manager blocks all downloads for the selected day(s).
   - 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, Control Manager blocks all downloads for the selected hours.
5. 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 updates
- **Enabled:** Indicates if the schedule for the component is 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

Configuring Scheduled Downloads and Enabling Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Deployment Plan** from the drop down menu. The Deployment Plan screen appears.
3. Click **Add**. The **Add New Plan** screen appears.
4. On the Add New Plan screen, type a deployment plan name in the **Name** field.
5. Click **Add** 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. Mouseover **Administration**. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.
4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
6. Type the host name or IP address of the server in the **Server name or IP address** field.
7. Type a port number for the proxy server in the **Port** field.
8. Type a logon name and password if your server requires authentication.
9. Click **Save**.

Step 3: Select the components to update

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.

3. 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 components to download. To select all components for a group, select:
      - **All Pattern files/Cleanup templates**
      - **All Anti-spam rules**
      - **All Engines**
      - **Product programs**

      The <Component Name> screen appears, where <Component Name> represents the name of the selected component.

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 by minutes, hours, days, or weeks.
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 Connection 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, and deploy to managed products when new components are available from the update source

---

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 **Enable** column.
2. Click **Save**.

Configuring Scheduled Download Schedule and Frequency

Specify how often Control Manager obtains component updates at the Schedule and Frequency group.

To configure scheduled download schedule and frequency:

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. 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 components to download. To select all components for a group, select:
      - **All Pattern files/Cleanup templates**
      - **All Anti-spam rules**
      - **All Engines**
      - **Product programs**

      The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.
4. Under Schedule and frequency:
   a. 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 minutes, hours, days, or weeks.
   b. Use the **Start time** drop-down menus to specify the date and time the schedule starts to take effect.
5. Click **Save**.

Configuring Scheduled Download Settings

The Download Settings group defines the components Control Manager automatically downloads and the download method.

To configure scheduled download settings:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. 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 components to download. To select all components for a group, select:
      - **All Pattern files/Cleanup templates**
      - **All Anti-spam rules**
      - **All Engines**
      - **Product programs**

      The <Component Name> screen appears. Where <Component Name> represents the name of the selected component.

Under Download settings:

4. Under Source, select one of the following update sources:
   - **Internet: Trend Micro update server** — (default setting) Control Manager downloads latest components from the Trend Micro ActiveUpdate server.
   - **Other Internet source** — specify the URL of the latest component source, for example, your company's Intranet server

     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.
5. Select **Retry frequency** to instruct Control Manager to retry downloading latest components. Specify the number of attempts and the frequency of each set of attempts in the appropriate fields.

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

6. If you are using a proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings from the Connection Settings screen.
7. Click **Save**.

Configuring Scheduled Download Auto-Deploy Settings

Use the Auto-deploy Setting group to set how Control Manager deploys updates.

To configure scheduled download auto-deploy settings:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. 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 components to download. To select all components for a group, select:
      - **All Pattern files/Cleanup templates**
      - **All Anti-spam rules**
      - **All Engines**
      - **Product programs**

      The <Component Name> screen appears, where <Component Name> represents the name of the selected component.

Under Automatic deployment settings

4. 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.

5. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
6. Click **Save**.

Note: The settings in Automatic Deployment Settings only apply to components used by managed products.

For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

Understanding Deployment Plans

A Deployment Plan allows you to set the order in which Control Manager updates your groups of managed products. With Control Manager, you can implement multiple deployment plans to different managed products at different schedules. For example, during an outbreak involving an email-borne virus, you can prioritize the update of your email message scanning software components such as the latest virus pattern file for Trend Micro ScanMail for Microsoft Exchange.

The Control Manager installation creates two deployment plans:

- **Deploy to All Managed Products Now (Default):** default plan used during component updates
- **Deploy to All Immediately (Outbreak-Prevention):** default plan for the Outbreak Prevention Services, Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately.

Select or create plans from the Manual and Scheduled download pages. Customize these plans, or create new ones, as required by your network. For example, create Deployment Plans according to the nature of the outbreak:

- Email-borne virus
- File sharing virus

Deploying updates to the Product Directory is separate from the download process.

Control Manager downloads the components and performs the deployment plan according to manual or scheduled download settings.

When creating or implementing a deployment plan, consider the following points:

- Assign deployment schedules to folders, not specific products.

  Planning the contents of the Product Directory folders, therefore, becomes very important.
- You can only include one folder for each deployment plan schedule.

  However, you can specify more than one schedule per deployment plan.
- Control Manager bases the deployment plan delays on the completion time of the download, and are independent of each other.

  For example, if you have three folders that you want to update at five minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders.

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Deployment Plan** from the drop down menu. The Deployment Plan screen appears.
3. Click **Add**. The **Add New Plan** screen appears.
4. On the Add New Plan screen, type a deployment plan name in the **Name** field.
5. Click **Add** 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.

Configuring Proxy Settings

Configure proxy server connection for component downloads and for license updates.

To configure proxy server settings:

1. Mouseover **Administration**. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.
4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
6. Type the host name or IP address of the server in the **Server name or IP address** field.
7. Type a port number in the **Port** field.
8. Type a log on name and password if your server requires authentication.
9. Click **Save**.

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (http://cm5-p.activeupdate.trendmicro.com) or other Internet source provides a more secure method for retrieving components.

Downloading components from a shared folder in a network requires setting the local Windows and Remote UNC authentications.

The local Windows authentication refers to the active directory user account in the Control Manager server. The account should have:

- Administrator privilege
- *Log on as a batch job* policy set

The Remote UNC authentication is any user account from the component source server that has permission to share a folder where Control Manager will download updates.

To enable HTTPS download:

1. Mouseover **Updates** from the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Update/Deployment Settings**. The Update/Deployment Settings screen appears.
4. Select **Enable HTTPS for the default update download source**.
5. Click **Save**.
6. Access Manual Download or Scheduled Download.
7. On the working area under **Download settings > Source group**, select **Internet: Trend Micro update server** or specify your organizations component source server in the **Other Internet source** field.
8. Click **Save**.

To enable UNC download:

1. Mouseover **Updates** from the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Update/Deployment Settings**. The Update/Deployment Settings screen appears.
4. Type the **Local Windows Authentication** and **Remote UNC Authentication** user names and passwords.

5. Click **Save**.
6. Access Manual Download or Scheduled Download.
7. On the working area under **Download settings > From group**, select **File path** and then specify the shared network folder.
8. Click **Save**.

Setting "Log on as batch job" Policy

The local Windows authentication refers to the active directory user account in the Control Manager server. The account should have:

- Administrator privilege
- "Log on as a batch job" policy set

To verify the user is on the "Log on as batch job" list:

1. Click **Start> Settings > Control Panel**.
2. Click **Administrative Tools**.
3. Open **Local Security Policy**. The Local Security Settings screen appears.
4. Click **Local Polices > User Rights Assignment**.
5. Double-click **Log on as a batch job**. The Log on as a batch job Properties dialog box appears.
6. Add the user if they do not appear on the list.

Using Logs

Although Control Manager receives data from various log types, Control Manager now allows users to query the log data directly from the Control Manager database. The user can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

Understanding Managed Product Logs

Managed product logs provide you with information about the performance of your managed products. You can obtain information for specific or groups of products administered by the parent or child server. With Control Manager's data query on logs and filtering capabilities, administrators can now focus on the information they need.

Querying Log Data

Control Manager now supports gathering only the data an administrator needs from Control Manager and managed product logs. Control Manager supports this through the use of Ad Hoc queries. Ad Hoc queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Using Ad Hoc queries to pull data directly from the database provides a very powerful tool for administrators.

While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML for further analysis, or save the query for future use. Control Manager also supports sharing Saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc query consists of the following process:

Step 1: Select the managed product or current Control Manager server for the query

Step 2: Select the Data View to query

Step 3: Specify filtering criteria, and the specific information that displays

Step 4: Save and complete the query

Step 5: Export the data to CSV or XML

Note: Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Logs/Reports > Saved Ad Hoc Queries** screen.

Understanding Data Views

A Data View is a table consisting of clusters of related data cells. Data Views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager separates Data Views into two major categories: Product Information and Security Threat Information. The major categories separate further into several sub-categories, with the sub-categories separated into summary information and detailed information.

The Control Manager web console displays the Data Views and the information available from each Data View.

TABLE A-8. Data views on the Control Manager web console

MAJOR DATA VIEW CATEGORY	DESCRIPTION
Product Information	Displays information about: • Control Manager • Managed products • Managed product components • Product license information
Security Threat Information	Displays information about security threats that managed products detect: • Overall Security Risks • Malware/viruses • Spyware/grayware • Content violations • Spam • Web content violations • Policy/Rule violations • Suspicious threats

Working with Reports

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduces radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 5.0 continues to support report templates from previous Control Manager versions, however Control Manager 5.0 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager 5.0 categorizes report templates according to the following types:

- **Control Manager 5.0 templates:** User-defined customized report templates that use direct database queries (database views) and report template elements (charts/graphs/tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions. For more information on Control Manager 5.0 templates, see *Understanding Control Manager 5.0 Templates* on page A-53.
- **Control Manager 3.0 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3.0 templates, see *Understanding Control Manager 3.0 Templates* on page A-54.

Understanding Control Manager 5.0 Templates

Control Manager 5.0 report templates use database views as the information foundation for reports. For more information on data views, see *Understanding Data Views* on page A-51. The look and feel of generated reports falls to the report elements. Report elements consist of the following:

TABLE A-9. Control Manager report template elements

TEMPLATE ELEMENT	DESCRIPTION
Page break	Inserts a page break for a report. Each report page supports up to three report template elements.
Static text	Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.
Bar chart	Inserts a bar chart into a report template.
Line graph	Inserts a line graph into a report template.
Pie chart	Inserts a pie chart into a report template.
Dynamic table	Inserts a dynamic table/pivot table into a report template.
Grid table	Inserts a table into a report template. The information in a grid table will be the same as the information that displays in an Ad Hoc Query.

Each Control Manager 5.0 template can contain up to 100 report template elements. Each page in the report template can contain up to three report template elements. Use page breaks to create report template pages.

Adding a Control Manager 5.0 custom template requires the following steps:

1. Access the Add Report Template screen and name the template.
2. Specify the template component to add to the report template.
3. Specify the data view for the template.
4. Specify the query criteria for the template.

5. Specify the data to appear in the report and the order in which the data appears.
6. Complete report template creation.

Understanding Control Manager 3.0 Templates

Trend Micro Control Manager 3.0/3.5 added 65 pre-generated report templates divided into six categories: Desktop, File Server, Gateway, Mail Server, Executive Summary, and Network Products.

Note: In Control Manager 3.5 spyware/grayware were no longer considered viruses. This change affects the virus count in all original virus related reports.

Adding One-time Reports

Control Manager supports generating one-time reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a one-time report is similar for all report types and involves the following:

1. Access the Add One-time Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a scheduled report is similar for all report types:

1. Access the Add Scheduled Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Glossary

TERM	DEFINITION
ActiveUpdate server	The Trend Micro server hosting the Network VirusWall Enforcer components. The ActiveUpdate™ server can be set as the update source.
Automatic switch-back	A mode that allows the management device to automatically switch-back to the default primary device once it becomes online.
Assessment	The process of checking an endpoint for compliance to policy.
BPDU	Short for bridge protocol data unit. 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.
Block	To prevent endpoint traffic from passing until the next assessment.
Bridge	The connection between two network segments.
Cleanup	The removal of malware and malware components from an endpoint.

TERM	DEFINITION
Control Manager	Trend Micro management product for different enterprise security applications.
Directory Manager	A feature of Control Manager that lets you to customize the Product Directory structure to suit your administration needs.
Drop	To prevent a specific communication session from passing the device.
Email notifications	Email messages sent through a specified SMTP server for certain detection events.
Failopen	A fault-tolerance solution that allows the Network VirusWall Enforcer device to continue to pass traffic in an event when a software or hardware failure occurs within the device.
Formatting tags	HTML tags that can be used to control the appearance of notifications.
Image	Refers to the Network VirusWall Enforcer firmware or program file.
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 networks (VPNs).
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 2 Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).

TERM	DEFINITION
Malware	Malicious code or files containing malicious code; includes Trojans, worms, network viruses, and other threats.
Managed product	Refers to any software program or hardware device managed by Control Manager.
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.
Management ports	Device ports that can only be used for accessing the console or providing mirror, sniffer, or failover functionality
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 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 device, such as the number of packets received or memory utilization statistics.
Monitor	To tag the endpoint as noncompliant and apply a more aggressive assessment schedule to that endpoint.

TERM	DEFINITION
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 to 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.

TERM	DEFINITION
Network virus	The type of threat that Network VirusWall Enforcer 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.
Network Virus Engine	The antivirus component that checks network packets for viruses and other threats.
Network zones	A user-defined set of endpoint IP or MAC addresses for the purposes of enforcement. Each policy can be defined to apply only to specific network zones.
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.
NTP	See Network Time Protocol.

TERM	DEFINITION
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 works with L2 and L3 devices.
Popup notifications	Notifications displayed as message boxes or balloon popups from the agent icon. These messages are designed to inform endpoint users that they have violated a policy.
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 supports port-based VLAN with port grouping.
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.

TERM	DEFINITION
Preconfiguration	The process of preparing the product for management through the web console through a much simpler console. Preconfiguration typically includes setting port functions and the management IP address.
Preconfiguration console	The console used to preconfigure a Network VirusWall Enforcer device. Preconfiguring a Network VirusWall Enforcer device allows you to modify the basic Network VirusWall Enforcer default settings, perform network configuration, and set the operation mode.
Product directory	The product directory is a logical grouping of managed products accessible from the Control Manager management console.
Quarantine	To prevent an endpoint from accessing the network until it is explicitly released by an administrator through the web console.
Regular ports	Ports that are used for enforcement, in contrast to management ports. Also called bridge ports since these ports are typically supplied bridge addresses to communicate with endpoints in protected segments.
Reject	To block a communication session by stopping packets and sending a reset packet (RST) to the source
Remote login	Remotely logging on to an endpoint to silently install the agent.
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.

TERM	DEFINITION
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 (STP)	Also known as STP. This term 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.
Switched Ethernet LANs	Ethernet networks that use switches to join segments.
TMAgent/Agent	Called the Threat Management Agent, the device installs this application on protected endpoints to perform certain enforcement functionality
Trap	Notifications sent by managed devices to the NMS when certain events occur, such as a shutdown or authentication error.
Variable tags	Tags used to control the content of notifications; these tags are replaced with actual values on the notifications.

TERM	DEFINITION
VLAN	Short for virtual LAN. A network consisting of clients that are not necessarily 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.
Web console	The web-based interface for managing policies and the device
Web notifications	Notifications that are shown to endpoint users when they attempt to access a web page. Most notifications are displayed to inform users of policy violations.
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.

Index

A

B

C

D

E

F

L

M

N

O

P

Q

R

S

T

U

V

W

Y

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: NVEM05896/130315