



2.5 Deep Edge™ Service Pack 2 Administrator's Guide

Next Generation Firewall Protection



Network Security

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

<http://docs.trendmicro.com/en-us/home.aspx>

© 2014 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro Antivirus, Deep Discovery, TrendLabs, TrendEdge, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: CTEM26692_140930

Release Date: November 2014

Protected by U.S. Patent No.: Patents pending.

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

About This Manual

About This Manual	ix
Deep Edge Documentation	x
Audience	xi
Document Conventions	xi
About Trend Micro	xii

Chapter 1: Deep Edge Next Generation Firewall

Deep Edge Overview	1-2
What's New	1-2
Main Features	1-9
Security Protection	1-9
Operations Control	1-10
Visibility and Monitoring	1-10
Network Connectivity	1-11

Chapter 2: Getting Started

Logging on to the Web Console	2-2
Accessing the Setup Wizard	2-2
Changing the Deep Edge System Password	2-3
Configuration Overview	2-4
Summary of Operations	2-5

Chapter 3: Processing and Identifying Traffic

Network Traffic Overview	3-2
Interfaces	3-2
Editing Network Interfaces	3-2

Monitoring Hosts	3-5
Interface Bandwidth Settings	3-5
About VLANs	3-5
DNS	3-7
DNS Best Practice Suggestions	3-7
Configuring DNS Settings	3-8
Addresses	3-8
About Addresses and Address Objects	3-9
Address Object Parameters	3-9
Adding Address Objects	3-10
Configuring Address Objects	3-11
Viewing Address Objects	3-11
Deleting Address Objects	3-11
Deployment Settings	3-12
About Deployment Modes	3-12
Bridging Interfaces	3-20
Important Notes About Bridging Interfaces	3-20
Adding a Bridge	3-21
Removing a Network Bridge	3-23
Routing Traffic	3-25
About Static Routes	3-25
About Policy-based Route Management	3-28
About Dynamic Route Management	3-31
Network Address Translation (NAT)	3-45
NAT Rules	3-46
Services	3-50
About DNS Forwarding	3-50
About DHCP	3-51
About Dynamic DNS	3-54
Virtual Private Network	3-58
User VPN	3-58
Secure Socket Layer Virtual Private Network	3-62
Mobile VPN	3-79
Customizing the VPN Portal	3-103

Site-to-Site VPN	3-104
IPsec Connections	3-104
Site-to-site VPN Policies	3-107
Advanced IPsec Configuration	3-110
IPSec Status	3-111
IPsec Troubleshooting	3-111

Chapter 4: Policies, Objects, and Security

About Policies	4-2
How Firewall Policies Work	4-2
About Policy Rules	4-2
About Policy Objects	4-10
About Addresses and Address Objects	4-11
About Zones and Zone Objects	4-11
About Services and Service Objects	4-13
About Applications and Application Objects	4-15
About URL Category Objects	4-17
About Schedules and Schedule Objects	4-29
About Action Profiles	4-30
About Security Settings	4-34
Network Intrusion Protection	4-35
IPS Security	4-36
Anti-Malware Security	4-38
Anti-Spam Security	4-47
WRS Profiles	4-53
About HTTPS Inspection	4-54
General Settings for HTTPS Inspection	4-55
About Digital Certificates	4-56
About Bandwidth Control	4-60
Adding Bandwidth Rules	4-61
Enabling/Disabling Bandwidth Rules	4-67
About Approved/Blocked URLs	4-67
Configuring Approved or Blocked URLs	4-67
Enabling/Disabling the Approved List or Blocked List	4-68

About Anti-DoS	4-69
Configuring Flood Protection	4-70
Adding Address Exceptions	4-70
Modifying Address Exceptions	4-71
Deleting Address Exceptions	4-71
About Authentication	4-72
User Identification Methods	4-73
Adding Authentication Rules	4-73
About Captive Portal	4-74
About User Notifications	4-76
Configuring WRS Violation Notifications	4-76
Configuring URL Filtering Violation Notifications	4-77
Configuring Application Control Violation Notifications	4-78
Configuring Anti-Malware Violation Notifications	4-79
Configuring Blocked URL Violation Notifications	4-79
Configuring File Extension Violation Notifications	4-80
Configuring IPS Violation Notifications	4-81
Certificate Failure Notifications	4-81

Chapter 5: Intelligent Daily Monitoring

Dashboard and Widgets	5-2
About Tabs	5-2
About Widgets	5-4
Using Widgets	5-8
Analysis and Reports	5-30
Log Analysis	5-30
Log Favorites	5-35
Reports	5-35
Managing Report Templates	5-37
Log Settings	5-39
Configuring Global Log Settings	5-39
Device Logs	5-40
Audit Logs	5-41
System Event Logs	5-41
VPN Logs	5-42

Querying Logs	5-43
Querying the Audit Log	5-43
Querying the System Events Log	5-44
Querying the VPN Log	5-44

Chapter 6: Administration

Switching the Language Settings	6-2
Configuring Getting Started Settings	6-2
System Settings	6-3
General System Settings	6-3
About Console Settings	6-4
About Proxy Settings	6-4
Experience Improvement	6-5
Device Management	6-5
Administrative Access	6-5
Configuring SNMP Settings	6-6
Administrative Accounts	6-7
Web Shell	6-9
End User Management	6-9
About General Settings	6-9
LDAP User Identification	6-11
Local User and Group Management	6-14
About Notifications	6-19
System Notifications and Alerts	6-20
SMTP Settings for Notifications	6-24
Product License	6-25
Updates	6-25
Device Logs	6-25
Mail Quarantine	6-25
Querying the Mail Quarantine	6-26
Configuring Mail Quarantine Settings	6-27
System Maintenance	6-27
Performing System Maintenance	6-27

Configuration Backup and Restore	6-28
Diagnostics	6-29
Packet Capture	6-30
Traffic Tracing	6-32
Generating Diagnostic Files	6-33
Support	6-33
About Deep Edge	6-34
Smart Protection Network: Cloud-based Services	6-34

Chapter 7: Keeping Updated

Updateable Program Components	7-2
Anti-Malware Virus Pattern File	7-2
Anti-Malware Protocol Pattern File	7-3
C&C Contact Information Pattern	7-3
IPS Pattern and Engine	7-3
Virus Scan Engines and Pattern	7-3
IntelliTrap Pattern and Exceptions	7-3
Spyware Pattern	7-4
Anti-Spam Pattern and Engine	7-4
Web Reputation Services	7-4
URL Database	7-4
Email Reputation Database	7-5
Incremental Updates of the Pattern Files	7-5
Component Version Information	7-5
ActiveUpdate	7-6
About Updating from the Web Console	7-6
Configuring Proxy Settings for Updates	7-6
Selecting the Update Source	7-7
Manual Updates	7-8
Applying a Software Patch	7-8
Updating Components	7-9
Verifying a Successful Update	7-9
About Update Maintenance	7-10
Scheduled Updates	7-11
Scheduling Component Updates	7-11

Update Notifications	7-12
Configuring Notifications for Scheduled Updates	7-12

Chapter 8: Product Maintenance

Maintenance Agreement	8-2
Renewing the Maintenance Agreement	8-2
Product License	8-3
License Expiration Warnings	8-3
Obtaining a Registration Key	8-4
Registering Deep Edge	8-4
Obtaining the Activation Code	8-5
Updating the License	8-5
Renewing the Maintenance Agreement	8-6

Appendix A: Technical Support

Troubleshooting Resources	A-2
Trend Community	A-2
Using the Support Portal	A-2
Security Intelligence Community	A-3
Threat Encyclopedia	A-3
Contacting Trend Micro	A-3
Speeding Up the Support Call	A-4
Sending Suspicious Content to Trend Micro	A-5
File Reputation Services	A-5
Email Reputation Services	A-5
Web Reputation Services	A-5
Other Resources	A-6
TrendEdge	A-6
Known Issues	A-6
TrendLabs	A-6

Appendix B: Detailed Logs

Policy Enforcement Logs	B-2
Application Bandwidth Logs	B-3

Internet Security Logs B-4

Internet Access Logs B-6

VPN Logs B-8

System Event Logs B-9

Audit Logs B-11

 Audit Log Objects B-12

Index

Index IN-1

Preface

About This Manual

Welcome to the Trend Micro™ Deep Edge 2.5 Administrator's Guide. This guide provides detailed information about the Deep Edge next-generation firewall configuration options. Topics include managing updates to stay protected against the latest risks, using policies to support security objectives, configuring scanning and URL filtering, and understanding logs and reports.

Topics include:

- *Deep Edge Documentation on page x*
- *Audience on page xi*
- *Document Conventions on page xi*
- *About Trend Micro on page xii*

Deep Edge Documentation

The documentation set for Deep Edge includes the following:

TABLE 1. Deep Edge Document Set

DOCUMENT	DESCRIPTION
Administrator's Guide	This guide provides detailed information about the Deep Edge next-generation firewall configuration options. Topics include managing updates to stay protected against the latest risks, using policies to support security objectives, configuring scanning and URL filtering, and understanding logs and reports.
Deployment Guide	This guide explains the Deep Edge appliance deployment modes and initial policy configurations. It also describes post-upgrade configurations, testing the installation, troubleshooting, and accessing Technical Support.
Quick Start Guide	This guide gives information about unpacking, setting up, and logging into a new Deep Edge appliance.
Online Help	The online help provides the same content as the <i>Administrator's Guide</i> and is accessible from the Deep Edge web console.
Readme File	This file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.
Knowledge Base	The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to: http://esupport.trendmicro.com/

DOCUMENT	DESCRIPTION
TrendEdge	TrendEdge provides Trend Micro employees, partners, and other interested parties with information about unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics. To access TrendEdge, go to: http://trendedge.trendmicro.com

The latest versions of the documentation is available in electronic form at:

<http://docs.trendmicro.com/en-us/home.aspx/>

Audience

The Deep Edge documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of network schemas and network fundamentals.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output

CONVENTION	DESCRIPTION
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

<http://www.trendmicro.com>

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Chapter 1

Deep Edge Next Generation Firewall

Topics include:

- *Deep Edge Overview on page 1-2*
- *What's New on page 1-2*
- *Main Features on page 1-9*

Deep Edge Overview

Deep Edge offers a new level of simplicity for deployment, configuration, and management of a next-generation firewall solution. Its all-functions-turned-on high performance scanning intelligently protects the network, endpoint, and server environments from web, email, and other network-based malicious activity including viruses, worms, spyware, bots, Trojans and phishing scams. Deep Edge also offers VPN connectivity to secure connections from mobile devices, corporate sites, and remote employees. All advanced security capabilities are easily configured, deployed, and viewed on an intuitive and flexible web-based console.

What's New

TABLE 1-1. New Features in Deep Edge 2.5 Service Pack 2

FEATURE	DESCRIPTION
Setup Wizard	The Deep Edge Setup Wizard provides a step-by-step interface to configure and deploy the Deep Edge appliance. The Setup Wizard enhances the configuration flow by providing contextual information about each configuration to help system administrators make informed decisions about the deployment. The Setup Wizard automatically initiates after logging on the appliance for the first time. Access the Setup Wizard by clicking Wizard from the web console's top menu.

FEATURE	DESCRIPTION
Network Diagnostics	The Network Diagnostics tool helps troubleshoot common connectivity issues, including: • Internet access • DNS configuration • Traffic routing • Trend Micro ActiveUpdate access • Trend Micro Web Reputation Service (WRS) access Access the Network Diagnostics tool by clicking Network Diagnostics from the web console's top menu.
Integration with Deep Discovery Inspector	Configure Deep Discover Inspector integration as part of an advanced anti-malware protection strategy. Trend Micro Deep Discovery Inspector is a separately licensed product that provides advanced network monitoring and threat intervention. With 360-degree monitoring of network traffic, Deep Discovery Inspector provides network-wide visibility and intelligence to detect and respond to targeted attacks. Deep Discovery Inspector enables administrators to select, create, configure, import, and export IP addresses, URLs, and domains as lists of denied or allowed objects. Deep Discovery Inspector can also add IP addresses, URLs, and domains from Virtual Analyzer feedback or from behavior or pattern matching scans. Deep Edge uses the Deep Discovery Inspector deny lists to block connections from denied IP addresses, URLs, and domains.

FEATURE	DESCRIPTION
Policy validation and checking	Deep Edge enhances policies by validating already configured policies to help system administrators configure policies that do not conflict in how they route traffic. Policy checking also assists system administrators in configuring policies as they are intended by highlighting any potentially conflicting configuration in policies with a higher priority than the configured policy.

TABLE 1-2. New Features in Deep Edge 2.5 Service Pack 1

FEATURE	DESCRIPTION
Advanced anti-malware protection	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks. For more information about ATSE, see About Advanced Threat Scan Engine on page 4-39.
Integration with Deep Discovery Advisor	Trend Micro™ Deep Discovery Advisor is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. Deep Edge integrates with the Virtual Analyzer in Deep Discovery Advisor. For more information about Deep Discovery Advisor, see About Deep Discovery Advisor on page 4-42.
Streamlined network configuration	To simplify network configurations, Deep Edge streamlines the settings for interfaces, DNS, DHCP and DNS forwarding, and bridged interfaces.

TABLE 1-3. New Features in Deep Edge 2.5

FEATURE	DESCRIPTION
Dual ISP and WAN support	Deep Edge can now support dual WAN or ISP connections. - In routing mode, Deep Edge 2.5 extends static and dynamic routing with policy-based routing using the destination or source IP address, the service type, or the egress interface of multiple ISPs or WANs. For details, see About Policy-based Route Management on page 3-28. - In bridge mode, Deep Edge 2.5 supports multiple bridged interfaces. For details, see Bridging Interfaces on page 3-20.
Enhanced IPS performance	Deep Edge Intrusion Prevention Systems (IPS) performs deep content inspection on all traffic to stop harmful activities. Deep Edge 2.5 now has the capabilities to scan traffic with over 7000 easily-configured predefined IPS rules by setting filtering criteria about the severity level, affected operating systems, release date, or traffic categories. For details, see IPS Security on page 4-36.
Granular application control	Application control objects now include specific behaviors within the application, such as only limiting video calls or uploading files, to set granular policy rules.
New custom URL category objects	Deep Edge 2.5 supports customized URL category objects. For details, see Adding a Custom URL Category on page 4-27.

FEATURE	DESCRIPTION
Command & Control (C&C) Contact Alert Services	Command & Control (C&C) Contact Alert Services provides Deep Edge with enhanced detection capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks by blocking traffic from high-risk sources. A new C&C Callback Attempts widget tracks advanced persistent threat activity in your network by providing actionable intelligence about the user, the compromised host, and how Deep Edge enforced policy actions. For details, see C&C Contact Alert Widget on page 5-16.
Improved widget framework	Several improvements to the widget framework have increased performance, reliability and speed of the dashboard widgets.
Increased configuration visibility	A new <i>Getting Started</i> guide is available to simplify the setup process. Access help content by going to Administration > Getting Started from the web console.
Improved NAT rules	Each Deep Edge 2.5 NAT rule now has a description parameter to easily differentiate between multiple SNAT and DNAT configurations.
More robust log analysis	Deep Edge 2.5 enhances log presentation in the dashboard, log query results, and reports.

TABLE 1-4. New Features in Deep Edge 2.1

FEATURE	DESCRIPTION
Bandwidth Control	Peer-to-peer downloading, video streaming and instant message applications consume network bandwidth and can impact productivity. Deep Edge 2.1 supports using bandwidth control to reduce network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation. For more information, see About Bandwidth Control on page 4-60. In addition to policy settings, a new Bandwidth Control widget illustrates affected traffic. For more information, see Bandwidth Control Widget on page 5-23.
VPN enhancements	Deep Edge 2.1 enhances VPN compatibility: • Total connected clients are now listed in the Clients tab • PPTP VPN now allows for a larger address pool • Address objects are now listed in the Local Networks drop-down list For details, see Virtual Private Network on page 3-58.
Mobile VPN compatibility	Deep Edge 2.1 Mobile VPN supports multiple local domains. For more information, see Configuring Advanced Mobile VPN Settings on page 3-81.
Local users and groups	Local user and group management allows for authentication when an organization does not use Active Directory or LDAP authentication. Additional Deep Edge 2.1 enhancements include: • Only authenticated local users can access the external network • Policy rules support local user and group selection • Local user management improvements • VPN support For more information, see Local User and Group Management on page 6-14.

TABLE 1-5. New Features in Deep Edge 2.0

FEATURE	DESCRIPTION
HTTPS Inspection	The HTTPS Inspection feature in Deep Edge allows you to enable or disable HTTPS inspections, configure client certificate requests, and exclude specific websites, URLs, and IP addresses from inspection. For more information, see About HTTPS Inspection on page 4-54 .
Mobile VPN Support	Deep Edge, a gateway device, provides VPN services not only to laptops or desktops but also mobile devices. Mobile VPN offers support for mobile devices in the “closed” environment of Apple iOS or the “open source” environment of Android. For more information, see Mobile VPN on page 3-79 .
Anti-DoS Capability (and Report)	Deep Edge prevents Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attacks, which attempt to make a machine or network resource unavailable to users, and is intended to temporarily or indefinitely interrupt or suspend services to a host connected to the Internet. Typical attacks involve saturating the target machine with external communication requests, such that the machine can no longer respond to legitimate traffic or responds so slowly it is rendered unavailable. Such attacks usually lead to server overload. For more information, see About Anti-DoS on page 4-69.
End-user Notifications	Deep Edge provides end-user notifications for violations of the following policies: Web Reputation Services (WRS), URL Filtering, anti-malware, blacklisted URLs, file extensions detections, IPS and certificate failure (server and client). For more information, see About User Notifications on page 4-76 .
Email Security Solution	Deep Edge processes SMTP or POP3 email messages, scans them, and either cleans infected email messages and delivers them or performs the user-selected action set in the policy on email messages in violation. Email messages can be quarantined and delivered later. For more information, see Anti-Spam Profiles on page 4-48 .

FEATURE	DESCRIPTION
SSL VPN Enhancements	Deep Edge supports Secure Sockets Layer Virtual Private Network (SSL VPN), a form of VPN that can be used with a standard Web browser. The Deep Edge SSL VPN solution requires the installation of client software, and is ideal for applications including web-based email, business and government directories, file sharing, remote backup, remote system management, and consumer-level electronic commerce. For more information, see Secure Socket Layer Virtual Private Network on page 3-62 .

Main Features

The tables below describe key parts of the Deep Edge solution. All technology components are designed to integrate and optimized performance, which allows all security features to be turned on while providing excellent product performance.

Security Protection

FEATURE	DESCRIPTION
Advanced Firewall	Easily deploy and manage next-generation firewall capabilities. The Advanced Firewall blocks attacks while allowing good application traffic to pass.
IPS/IDS	Identify and stop many active threats, exploits, back-door programs, and other attacks, including DoS and DDoS attacks, passing through the device. The Intrusion Prevention System and Intrusion Detection System (IPS/IDS) bolsters a firewall's security policy by ensuring that traffic allowed by the firewall is further inspected to make sure it does not contain unwanted threats.
Web Protection	Use Trend Micro Web Reputation technology to control the level of protection against malicious websites.
Antivirus	Leverage multiple security components and antivirus protection based on high-speed application content scanning to protect the customer with lower latency and improved user experience.

FEATURE	DESCRIPTION
Anti-spam	Use Trend Micro Email Reputation Services (ERS) and an integrated high speed anti-spam engine to detect, block, or quarantine spam email messages based on the reputation of the mail sender and the email content .
ActiveUpdate	Enable on-demand and real-time updates from the Smart Protection Network to the local virus, protocol, spyware, IPS, IntelliTrap, and anti-spam pattern files.

Operations Control

FEATURE	DESCRIPTION
Application Control	Automatically discover popular Internet applications and control access to them using policies.
URL Filtering	Create and configure unique URL filtering procedures for different profiles. URL filtering, along with WRS, is part of the multi-layered, multi-threat protection solution.
LDAP Integration	Integrate with Lightweight Directory Access Protocol (LDAP) including Active Directory and OpenLDAP, to create policies specific to users or groups. Event logs and reports use LDAP user names and groups for user identification.

Visibility and Monitoring

FEATURE	DESCRIPTION
Summary Dashboard	Customize the dashboard to select, drill down, and display security and traffic information using widgets.
Application Bandwidth Monitoring	Record and monitor top bandwidth users on the network with Application Control and LDAP integration. Notify managers about abuse by identifying users and the applications used that burden the network.

FEATURE	DESCRIPTION
System Notifications and Alerts	Send security-related event email notifications (alerts) for: • Firewall • Web Reputation Service (WRS) • Malware • Intrusion Protection Services (IPS) • Hardware monitoring • URL filtering • Application control violations Notifications are sent directly to end-users, allowing them to take corrective action without impacting IT administrators.
Reports	Generate reports about detected malware and malicious code, blocked files, and accessed URLs to optimize program settings and fine tune security policies.
Logs	Detect and act upon security risks according to the settings specified for each risk type. These events are recorded in the logs.

Network Connectivity

FEATURE	DESCRIPTION
Network Configuration	View and edit detected network interfaces, or modify physical L2 and L3 port configurations. The following configurations are support for L3 ports: • Dynamic Host Configuration Protocol (DHCP) • Static route configurations by IP address and netmask • Point-to-point Protocol over Ethernet (PPPoE)

FEATURE	DESCRIPTION
Bridging	Transparently bridge two interfaces and filter network traffic to protect endpoints and servers with minimal impact to the existing network environment. Spanning Tree Protocol (STP) ensures a loop-free topology for any bridged Ethernet local area network.
Routing	Configure static and dynamic routes, including Routing Information protocol (RIP) and Open Path Shortest First (OSPF).
NAT	Configure Network Address Translation (NAT) policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports.
Services	Configure the following services: • Domain Name server (DNS) forwarding • Dynamic Host Configuration Protocol (DHCP) servers • Dynamic DNS (DDNS) settings
User VPN	Configure Virtual Private Network (VPN) with the Point-to-Point Tunneling Protocol (PPTP), Secure Sockets Layer Virtual Private Network (SSL VPN).
Site-to-Site VPN	Create encrypted L3 tunnels by using the Internet Key Exchange (IKE) and IP Security (IPsec) protocols.
Mobile VPN	Allow iPhone and Android mobile device users to easily and securely connect back to the corporate environment by utilizing the built-in IPsec VPN clients. No agent installation is required for the mobile devices.

Chapter 2

Getting Started

Getting Started explains how to start using Deep Edge for the first time. Make sure to review the *Deep Edge Deployment Guide* before proceeding with reading the *Deep Edge Administrator's Guide*. If you are upgrading from a previous Deep Edge version or updating components of your existing configuration, see [Keeping Updated on page 7-1](#).

Topics include:

- [Logging on to the Web Console on page 2-2](#)
- [Accessing the Setup Wizard on page 2-2](#)
- [Changing the Deep Edge System Password on page 2-3](#)
- [Configuration Overview on page 2-4](#)
- [Summary of Operations on page 2-5](#)

Logging on to the Web Console

Log on to Deep Edge to set the deployment mode.

Procedure

1. Use the address `https://<appliance_IP_address>:8443`.

Specify the IP address provided during the installation.



Important

Remember to include the “s” in `https://`

2. Specify the administrator credentials.

Default credentials:

User name: `admin`

Password: `adminDeepEdge`

3. Press ENTER or click **Log On**.
-

Accessing the Setup Wizard

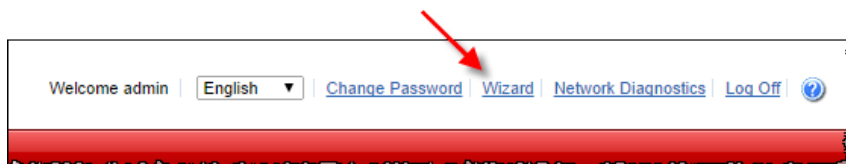
The **Setup Wizard** screen is available to make the setup process more visible. For more information about deploying Deep Edge, see the *Deep Edge Deployment Guide*.

Procedure

1. Log on to the web console.

See [Logging on to the Web Console on page 2-2](#).

2. Click **Wizard** at the top menu.



The **Setup Wizard** appears.

Changing the Deep Edge System Password

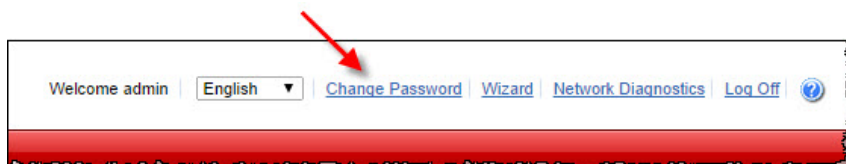
Change the Deep Edge system password after installing Deep Edge or if there is a possibility the system security has been compromised.

Procedure

1. Log on the Deep Edge web console.

See *Logging on to the Web Console on page 2-2*.

2. Click **Change Password** at the top menu.



The **Change Password** screen appears.

3. Specify the old and new passwords.
4. Click **Apply**.

Configuration Overview

The following tables explain the required, recommended, and optional settings to get started using Deep Edge. After reviewing the configuration overview, see [Summary of Operations on page 2-5](#) to begin configuring your Deep Edge appliance.

TABLE 2-1. Required Configurations

CONFIGURATION	REFERENCE
Configure DNS	Configuring DNS Settings on page 3-8
Activate license	Product License on page 8-3
Set default gateway	Adding a Static Route on page 3-25.

TABLE 2-2. Recommended Configurations

CONFIGURATION	REFERENCE
Change web console password	Changing the Deep Edge System Password on page 2-3
Set location and time	Configuring Time and Date Settings on page 6-3
Enable experience improvement	Experience Improvement on page 6-5
Configure anti-spam and approved lists	About Approved/Blocked URLs on page 4-67

TABLE 2-3. Optional Configurations

CONFIGURATION	REFERENCE
Switch language settings	Switching the Language Settings on page 6-2
Configure proxy settings	Configuring Proxy Settings on page 6-5
Add address objects for internal addresses	About Addresses and Address Objects on page 3-9
Configure bandwidth settings	About Bandwidth Control on page 4-60

CONFIGURATION	REFERENCE
Endpoint user	End User Management on page 6-9

Summary of Operations

The following procedure explains the basic configurations required to use Deep Edge for the first time. For more information about deploying Deep Edge, see the *Deep Edge Deployment Guide*.

Procedure

1. Set the default route.
[See Adding a Static Route on page 3-25.](#)
2. Configure the system settings.
 - For the host name setting, see [General System Settings on page 6-3.](#)
 - For DNS settings, see [Configuring DNS Settings on page 3-8.](#)
 - For location and time settings, see [Configuring Time and Date Settings on page 6-3.](#)
3. Select the deployment mode and configure the settings.
 - For bridge mode, see [Bridging Interfaces on page 3-20.](#)
 - For routing mode, see [Routing Traffic on page 3-25.](#)



Note

For additional requirements about deployment modes and required settings, review the *Deployment Mode Configuration* chapter of the *Deep Edge Deployment Guide*.

4. Optional: Set the management interface IP address.

[See Editing Network Interfaces on page 3-2.](#)

5. Optional: Configure proxy settings.

See [Configuring Proxy Settings on page 6-5](#).

6. Configure policies and security.

See [Policies, Objects, and Security on page 4-1](#).



Note

For recommended policy configurations, including configurations in DMZ networks, review the *Security Policy Configuration* chapter of the *Deep Edge Deployment Guide*.

7. Configure bandwidth control.

See [About Bandwidth Control on page 4-60](#).

8. Configure VPN access.

See [Virtual Private Network on page 3-58](#)

9. Configure user authentication.

See [About Authentication on page 4-72](#).

Chapter 3

Processing and Identifying Traffic

Topics include:

- *Network Traffic Overview on page 3-2*
- *Interfaces on page 3-2*
- *Deployment Settings on page 3-12*
- *Bridging Interfaces on page 3-20*
- *Routing Traffic on page 3-25*
- *About Static Routes on page 3-25*
- *About Dynamic Route Management on page 3-31*
- *Network Address Translation (NAT) on page 3-45*
- *Services on page 3-50*
- *Virtual Private Network on page 3-58*
- *Site-to-Site VPN on page 3-104*

Network Traffic Overview

This section describes how to configure Deep Edge to operate in the network. Basic network settings include configuring Deep Edge interfaces. More advanced configuration includes router, bridge, VLAN, network address translation (NAT), wide area network (WAN), services, and Virtual Private Network (VPN) settings for the Deep Edge network.

Interfaces

View and edit the auto-detected Deep Edge network interfaces in the web console at **Network > Interfaces**. Deep Edge supports modifying the configurations of physical L2 and L3 ports. For L3 configurations, Deep Edge offers Dynamic Host Configuration Protocol (DHCP) configuration as well as static route configurations by IP address and netmask. Point-to-point Protocol over Ethernet (PPPoE) is another option for the L3 port.

Editing Network Interfaces

Deep Edge auto-detects L2 and L3 interfaces.

Procedure

1. Go to **Network > Interfaces** to view all Deep Edge network interfaces.
2. Click an interface in the **Name** column.
3. Configure the interface settings based on the interface mode.
 - For a static address, configure the following parameters.

OPTION	DESCRIPTION
Type	Select L3 .
Mode	Select Static .

OPTION	DESCRIPTION
IPv4 address	Specify the IPv4 address. Example: 123.123.123.123
IPv4 netmask	Specify the IPv4 subnet mask. Example: 255.255.254.0
IPv4 default gateway	Specify the IPv4 default gateway. This settings is only required for WAN configurations. Example: 123.123.123.123
IPv6 address / prefix length	Specify the IPv6 settings. Example: 2001:db8:10ff::ae:44f2/8
IPv6 default gateway	Specify the IPv6 default gateway. This settings is only required for WAN configurations. Example: 2001:db8:10ff::ae:44f2/64 Example: 2001:db8:10ff::ae:44f2/64
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.  Note For information about controlling administrative access, see Administrative Access on page 6-5.

- For DHCP, configure the following parameters.

OPTION	DESCRIPTION
Type	Select L3 .
Mode	Select DHCP .
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.

OPTION	DESCRIPTION
	 Note For information about controlling administrative access, see Administrative Access on page 6-5 .

- For PPPoE, configure the following parameters.

OPTION	DESCRIPTION
Type	Select L3 .
Mode	Select PPPoE .
User name	Specify the user name provided by the Internet Service Provider.
Password	Specify the password provided by the Internet Service Provider.
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.  Note For information about controlling administrative access, see Administrative Access on page 6-5 .
PPPoE Advanced Settings	Specify the on-demand, idle time, and connection timeout settings.

- Under **Monitoring Settings**, configure the monitoring hosts.

See [Monitoring Hosts on page 3-5](#).

- Under **Bandwidth Settings**, specify the maximum allowed upstream and downstream bandwidth.

See [Interface Bandwidth Settings on page 3-5](#).

- Click **Apply**.

7. Verify the updates in the interface list at **Network > Interfaces**.
-

Monitoring Hosts

Deep Edge checks whether a WAN works by pinging the corresponding monitor IP address or host name from each egress interface. If the monitoring hosts are unreachable, any static routes or policy-based routes associated with the interface are disabled. If the traffic matches another route, the traffic routes to other static routes or policy-based routes. If the traffic does not match another route, it is routed via the default gateway or discarded.

To configure the monitoring hosts, see [Editing Network Interfaces on page 3-2](#).

To configure the default gateway, see [Adding a Static Route on page 3-25](#).

To configure a policy-based route, see [Adding a Policy-based Route on page 3-30](#).

For information about automatic failover, see [Automatic Failover for Multiple ISP/WAN Environments on page 3-29](#).

Interface Bandwidth Settings

Configure interface bandwidth settings to set the maximum thresholds for downstream and upstream traffic. Bandwidth control policies cannot exceed the interface bandwidth threshold. By default, Deep Edge does not limit the bandwidth. Each interface can be configured with different thresholds.

Network congestion may occur when interface bandwidth settings are incorrectly allocated. Trend Micro recommends setting the interface bandwidth to the maximum thresholds allowed by that interface, and to then set bandwidth control policies that determine which traffic has higher priority. For details about bandwidth control policies, see [About Bandwidth Control on page 4-60](#).

To configure interface bandwidth settings, see [Editing Network Interfaces on page 3-2](#).

About VLANs

A Virtual Local Area Network (VLAN) is a group of endpoints, servers, and other network devices that communicate as if they are on the same LAN segment, regardless

of their location. Endpoints and servers can belong to the same VLAN even though they are geographically scattered and connected to numerous network segments.

A VLAN segregates devices logically, not physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. Communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding 802.1Q VLAN tags to all packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

Adding VLAN Subinterfaces



Important

Each VLAN subinterface VLAN ID must match the VLAN ID added by the IEEE 802.1Q-compliant router. The VLAN ID can be any number between 1 and 4094 (0 and 4095 are reserved). Configure each L3 VLAN subinterface with a unique IP address and netmask.

Add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

Procedure

1. To view all Deep Edge network interfaces, go to **Network > Interfaces**
2. Click the VLAN add configuration icon () in the **Action** column.
3. Specify the following information:

OPTION	DESCRIPTION
Name	Name the VLAN subinterface.
Type	L2 VLAN or L3 VLAN displays automatically, depending upon the parent interface.

OPTION	DESCRIPTION
Mode	For L3 interfaces, use the Mode drop-down list to set whether the subinterface uses a dynamic or static address.
VLAN ID	Specify the VLAN ID that matches the VLAN ID of the packets received by this VLAN subinterface. You cannot change the VLAN ID of an existing VLAN subinterface. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface.

4. Click **Apply**.

DNS

View and edit the Domain Name Server (DNS) settings for Deep Edge at **Network > DNS**. Environments utilizing DHCP or PPPoE to access the Internet may not be required to configure DNS settings or the default static route.

DNS Best Practice Suggestions

Smart Protection Network (SPN) uses cloud-based services and relies on DNS queries for lookups. To ensure fast response and minimum latency, the Deep Edge device must be configured with a DNS server. You can set up to three DNS servers.

The DNS servers must be able to support the volume of DNS requests made by Deep Edge. In general, before Deep Edge builds up its local DNS cache, two DNS requests will be made for each URL accessed. Make sure your DNS server is installed on a server with enough resources and performance to handle the extra DNS volume.

To reduce latency, each DNS server should have a fast network card and be installed on a fast network switch.

Trend Micro recommends on-site DNS servers versus ISP-provided DNS servers that are housed outside of the company's network. In general, ISP DNS servers have higher latency and do not support large numbers of DNS queries from a single IP address. Many ISP DNS servers have throttling mechanisms that limit the number of DNS

requests per second and can affect Deep Edge's Web Reputation Services (WRS) performance.

To improve network response time and performance, try to place the DNS server as close to the Deep Edge unit(s) as possible to eliminate unnecessary network hops between the devices.

WRS and URL Filtering requests are made over HTTP port 80. Do not block the Deep Edge management IP address for these ports on the firewall.

Configuring DNS Settings

Procedure

1. Log on to the Deep Edge web console.
2. Go to **Network > DNS**.
3. For either or both the **IPv4** and **IPv6** tabs, configure the DNS server IP addresses.



Note

If Deep Edge dynamically acquires the DNS from an Internet Service Provider, the **Inherit DNS Information** section appears with read-only DNS information.

4. Click **Apply**.
-

Addresses

Addresses determine the internal network IP address ranges. By default, Deep Edge allows all internal IP address ranges. Configure settings according to the internal network requirements. Deep Edge supports single IP addresses, '-' as a range marker, and IP address/netmask (192.168.1.1/24).

About Addresses and Address Objects

Address objects affect both policy and network settings. Address objects determine allowed IP address ranges in the internal network. By default, Deep Edge includes all internal IP address ranges. To set security policies for specific source or destination addresses, first define the addresses and address ranges in your network settings.

Go to **Network > Addresses**.

Address Object Parameters

Use the following information to define configure address object parameter to simplify the creation of security policies.

To create address objects, specify the following information.

TABLE 3-1. Address Object Parameters

PARAMETER	DESCRIPTION
Name	Specify a name that describes the addresses to be defined. This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Protocol	Specify if using an IPv4 or IPv6 address.

PARAMETER	DESCRIPTION
IP Address	IPv4 Address: Specify the address or network using the following notation: <code>ip_address</code> <code>ip_address/bitmask</code>  Note The bitmask is the number of significant binary digits used for the network portion of the address. - IP address range such as: <code>192.168.1.1-192.168.1.10</code> Example: <code>192.168.80.150/32</code> indicates one address, and <code>192.168.80.0/24</code> indicates all addresses from 192.168.80.0 through 192.168.80.255 IPv6 address Specify the IPv6 address or IPv6 address with prefix. Example: <code>2001:db8:123:1::1</code> or <code>2001:db8:123:1::/64</code>

Adding Address Objects

Procedure

1. Go to **Network > Addresses**.
 2. Click **Add**.
 3. Specify the IP address, IP address range, or IP address and netmask for the network.
 4. Click **Apply**.
-

Configuring Address Objects

Procedure

1. Go to **Network > Addresses**.
 2. Click **Add New**.
 3. Specify a name for the address object.
 4. Select the appropriate protocol version from the drop-down list box.
 5. Specify the IP address or CIDR network (single or comma delimited).
Example: 192.168.0.1 or 10.0.0.1-10.0.0.4 or 10.0.0.8
 6. Click **OK**.
 7. Verify the new address object displays in the list at **Network > Addresses**.
-

Viewing Address Objects

Procedure

- Go to **Network > Addresses**.
-

Deleting Address Objects

Procedure

1. Go to **Network > Addresses**.
2. Select the check box in the row of the object to delete.
3. Click the **Delete** icon ()

4. Click **Delete** in the confirmation dialog box.
 5. Verify the deleted address object is not in the list at **Network > Addresses**.
-

Deployment Settings

Deep Edge offers two deployment modes: Monitoring Mode and Inline Mode. Deep Edge also supports adding internal addresses.

About Deployment Modes

This section provides an overview of the working modes of Deep Edge, and how to configure Deep Edge for each mode.

Deep Edge runs in two different inline modes, depending on the network infrastructure and requirements. Use Routing mode and Bridge mode for traffic inspection and to take action based on policies. They support the same network security features. Use Monitoring mode to evaluate what effect security policies might have if deployed in Routing mode or Bridge mode.

TABLE 3-2. Deployment Modes

MODE	PURPOSE
Bridge	The Deep Edge unit is invisible to the network. All of its interfaces are on the same subnet. You only have to configure a management IP address so that you can make configuration changes. You would typically use Bridge mode on a private network behind an existing firewall or behind a router. For details, see Overview of Bridge Mode on page 3-13 .
Routing	The Deep Edge unit is visible to the network. All of its interfaces are on different subnets. Each interface connected to a network must be configured with an IP address valid for that network. You would typically use Routing mode when the Deep Edge unit is deployed as a gateway between private and public networks. For details, see Overview of Routing Mode on page 3-15 .

MODE	PURPOSE
Monitoring	Monitoring mode is designed for evaluating Deep Edge on a production network without blocking any traffic or making Deep Edge a point of failure in the network flow. In Monitoring mode, Deep Edge only applies policies to mirrored traffic to produce logs and reports; no blocking actions are enforced on the traffic. For details, see Overview of Monitoring Mode on page 3-17 .

About Inline Mode

Inline Mode allows Deep Edge to actively inspect traffic passing through the network.

Overview of Bridge Mode

In bridge mode, Deep Edge is invisible on the network and acts as a layer 2 bridge between network devices (switch, router, or firewall), transparently scanning network traffic in both directions. Bridge mode is the simplest way to deploy Deep Edge into an existing network topology and does not require client, router, or switch modifications.

Deep Edge acts as a “bump in the wire” and scans for malware. *Figure 3-1: Deep Edge in Bridge mode on page 3-14* illustrates Deep Edge in Bridge mode:

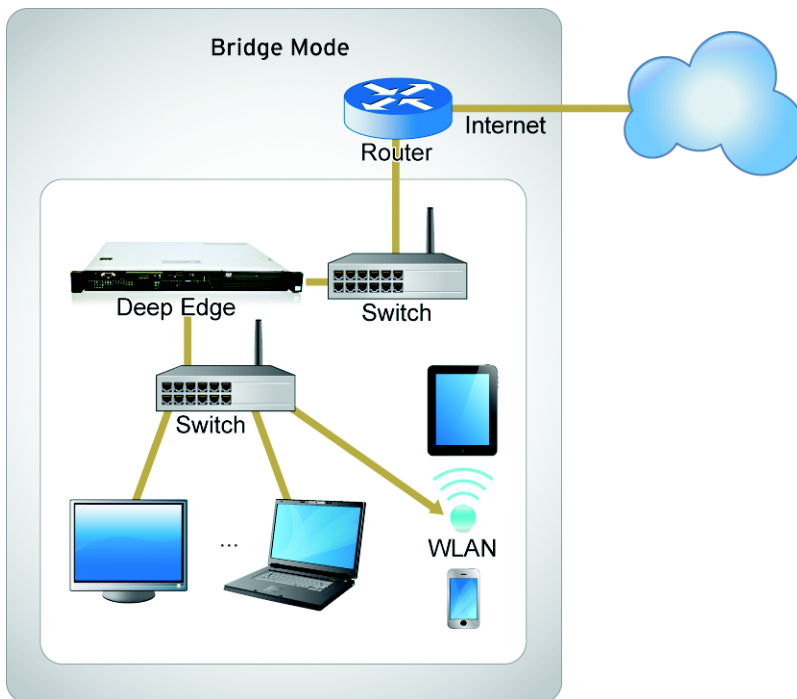


FIGURE 3-1. Deep Edge in Bridge mode

Similar to using a network bridge, all Deep Edge interfaces must be on the same subnet. To configure bridge mode, two network cards are required; one for internal use, and one for external use. You can also configure an IP address on the bridge to manage Deep Edge for scheduled pattern updates and to leverage the real-time security information power of the Trend Micro Smart Protection Network™ in the Cloud.

Configure bridge mode when Deep Edge operates on a private network behind an existing firewall or router so that Deep Edge can perform all scanning functions transparently.

For details about configuring bridge mode, see [*Bridging Interfaces on page 3-20*](#).

Overview of Routing Mode

In routing mode, Deep Edge is visible on the network and acts as a layer 3 routing device with traffic stream scanning capabilities. Deploying in routing mode requires configuring two network interfaces: one for internal use and one for external use. All the interfaces are on different subnets, enabling you to have a single IP address available to the public Internet. Deep Edge can perform network address translation before it sends and receives packets to the destination network and works as a router.

Deep Edge also provides Point-to-Point Protocol over Ethernet (PPPoE) functionality to support dialing to the ISP through asymmetric digital subscriber line (ADSL). See the

following figure for the typical deployment. *Figure 3-2: Deep Edge in Routing Mode on page 3-16* illustrates Deep Edge in routing mode:

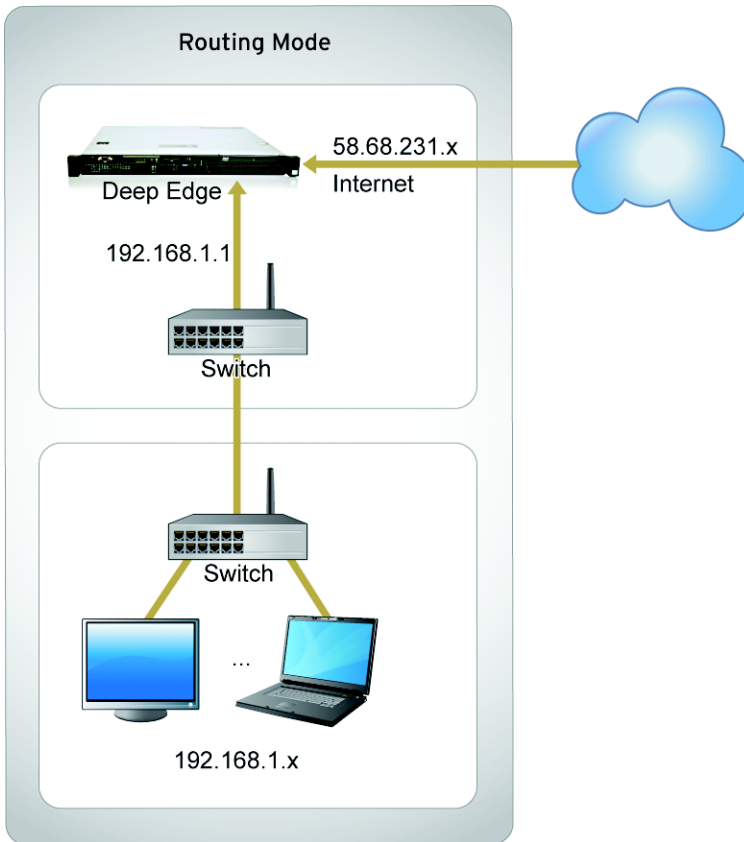


FIGURE 3-2. Deep Edge in Routing Mode

Configure routing mode when Deep Edge operates as a gateway between private and public networks. In this configuration, you must create NAT mode firewall policies to control traffic flow between the internal, private network and the external, public network, usually the Internet.

About Monitoring Mode

Monitoring Mode provides a way to access data flowing across a network. Deployed in Monitoring Mode, Deep Edge passively monitors traffic through a switch SPAN or mirror port.

The SPAN or mirror port permits copying traffic from other ports on the switch. By dedicating an interface on the firewall as the "Monitoring Mode" interface and connecting that interface with a switch SPAN port, the switch SPAN port provides the firewall with the mirrored traffic. This provides application visibility within the network without being in the flow of network traffic.



Note

When deployed in Monitoring Mode, the firewall is not able to take action, such as blocking traffic.

Overview of Monitoring Mode

Monitoring mode is designed for evaluating Deep Edge on a production network without blocking any traffic or making Deep Edge a point of failure in the network flow. In monitoring mode, Deep Edge is invisible to the network. Establish the correct monitoring settings on the network switch to mirror traffic to the port that connects to Deep Edge. Deep Edge will apply policies to the mirrored traffic, but only logs violation-related information. Network traffic is never blocked by policies in this mode.

Figure 3-3: Deep Edge in Monitoring mode on page 3-18 illustrates Deep Edge in monitoring mode:

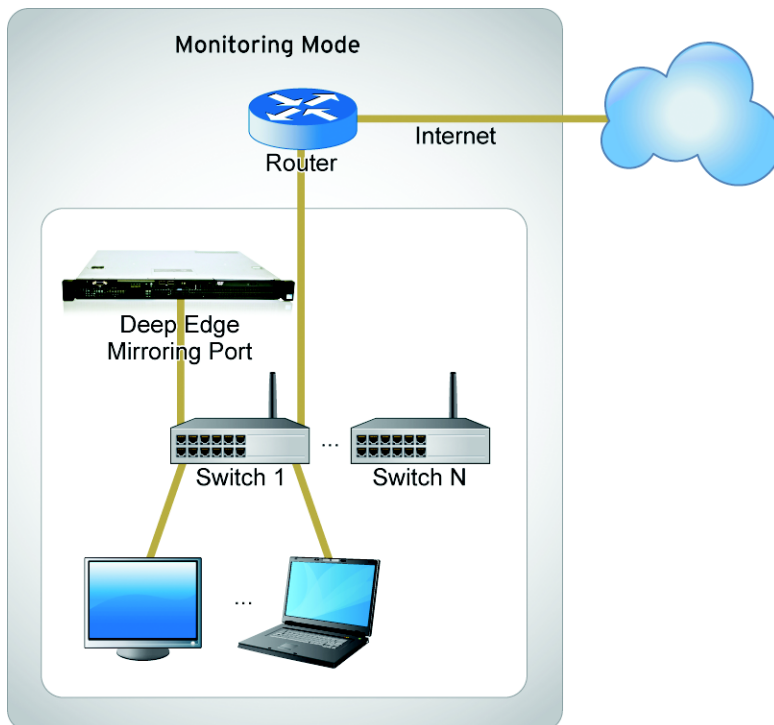


FIGURE 3-3. Deep Edge in Monitoring mode

In monitoring mode, network traffic does not pass directly through Deep Edge. Deep Edge runs independently outside the network (logically) aided by the switches of the network which mirror the specified traffic to interface(s) on which Deep Edge listens. Deep Edge monitors the status of the traffic and presents the information to the Deep Edge user.

Trend Micro suggests Deep Edge be deployed at the core Internet switch in order to see a copy of all Internet traffic leaving and entering the network. Deep Edge requires at least two network interfaces to function correctly in Monitoring mode. In addition to the interface that Deep Edge uses to listen for traffic, there should be another

connection for Deep Edge to access the Internet to connect to the ActiveUpdate and WRS query servers, as well as other cloud protection sources that Deep Edge offers.

Monitoring mode is typically used when:

- The network already has related devices (firewall, IDS/IPS) deployed, but there is a lack of visibility into the overall network posture. In this case, Deep Edge provides visibility without dramatically changing the network topology.
- Before deploying Deep Edge inline, Monitoring mode could help with the evaluation of the Deep Edge device. After learning the security benefits provided by Deep Edge, you could change from Monitoring mode to either Bridge mode or Router mode for true inline protection.

Configuring Deployment Mode Settings

Procedure

1. Go to **Network > Deployment**.
2. Click the **Deployment Mode** tab.
3. Select the radio button for the appropriate mode:

OPTION	DESCRIPTION
Inline Mode	For details, see About Inline Mode on page 3-13 .
Monitoring Mode	For details, see About Monitoring Mode on page 3-17 .

- a. For Monitoring mode, click the (+) sign to the right of the name of the interface to use in offline mode. It moves to the left column of the table. Click the (-) sign to move it back if needed. Use the **Add All** link to move all interfaces to the left side to use all in Monitoring mode.
4. Click **Apply**.

Bridging Interfaces

A bridge connects two interfaces using the same protocol to pass traffic transparently across the bridged interfaces. While in bridge mode, Deep Edge is invisible on the network and acts as a layer 2 bridge between network devices (switch, router, or firewall), transparently scanning network traffic in both directions.



Note

To receive security updates from Trend Micro, make sure that the management interface can access the Internet.

Deep Edge supports dual links to configure multiple WAN/ISPs connected to the appliance. Deep Edge has two inbound and two outbound links. Add multiple bridges to support multiple ISPs or WANs. Deep Edge is transparent between the two ISPs while an L3 router manages traffic.

Deep Edge supports Spanning Tree Protocol (STP) to ensure a loop-free topology for any bridged Ethernet local area network.

Important Notes About Bridging Interfaces

Select two different interfaces to form a bridge. Although all L2 and L3 interfaces can be selected, different combinations result in different behaviors:

- If Interface 1 and Interface 2 are both L2 interfaces, the two interfaces are added to a bridge.
- The IP address, netmask, and default gateway for the bridge are optional.
- Any L3 interfaces used in creating a bridge are degraded to L2 interface types.
- If the L3 interface is referenced by services like NAT, DHCP, Dynamic DNS, the interface can be added into the bridge until the reference relationship is removed.

**Note**

The IP address and netmask of the bridge are optional when there are other configured L3 interfaces with access rights to the web console. Otherwise, the web console access may not have access to Deep Edge. Users must access the CLI to repair this condition.

Adding a Bridge

For a bridge mode overview, see [Overview of Bridge Mode on page 3-13](#).

Procedure

1. Go to **Network > Deployment** and verify that the **Inline Mode** radio button is selected.
2. Go to **Network > Bridge**.
3. Click **Add New**.

The **Add/Edit Bridge** screen appears.

4. Specify a name for the network bridge.
5. From the **Interface 1** and **Interface 2** drop-down list boxes, select the interfaces to bridge.

**Note**

These bridged interfaces should correspond to the trusted and untrusted sides of the network so that data can pass between the Internet and internal systems.

6. Under **Bridge Binding IP Configuration**, specify the network settings.

**Note**

The bridge IP address, netmask, and default gateway are optional when other L3 interfaces are configured with access rights to the web console.

OPTION	DESCRIPTION
IPv4 address	Specify the IPv4 address. Example: 123.123.123.123
IPv4 netmask	Specify the IPv4 subnet mask. Example: 255.255.254.0
IPv4 default gateway	Specify the IPv4 default gateway. This settings is only required for WAN configurations. Example: 123.123.123.123
IPv6 address / prefix length	Specify the IPv6 settings. Example: 2001:db8:10ff::ae:44f2/8
IPv6 default gateway	Specify the IPv6 default gateway. This settings is only required for WAN configurations. Example: 2001:db8:10ff::ae:44f2/64 Example: 2001:db8:10ff::ae:44f2/64
Administrative access	Select which management services and traffic to allow (web console, ping, SSH, SNMP). These services originate from devices behind the Deep Edge appliance.  Note For information about controlling administrative access, see Administrative Access on page 6-5.

7. Configure **Advanced Settings**.

- Ensure a loop-free topology for the bridged network by selecting **Enable Spanning Tree Protocol**.
- Ensure that attached devices are aware of the link status in high availability networks by selecting **Enable Link Loss Forwarding**. For information about Link Loss Forwarding, see [Link Loss Forwarding on page 3-23](#).

8. Click **Apply**.

Link Loss Forwarding

Link Loss Forwarding ensures high availability by disabling both bridged interfaces if one interface fails. Any failure along the signal link is passed through and can be seen by attached devices. When Link Loss Forwarding is disabled, a failure in one bridged interface does not disable the other interface and connected devices are unaware that the link is lost.

Deep Edge monitors and enables the interface once the bridged interface signal link restores.

Configuring the Management Service

Configuring the management service allows remote access to Deep Edge. Any configured bridge with an IP address appear in the table under **Management Settings**. The interface will not appear if a network bridge has not been configured. For more details about management interface settings, see [Device Management on page 6-5](#).

Procedure

1. Go to **Administration > Device Management**.
 2. Under **Management Settings**, locate the network bridge interface and select one or more of the following:
 - Web console
 - Ping
 - SSH
 - SNMP
 3. Click **Apply**.
-

Removing a Network Bridge

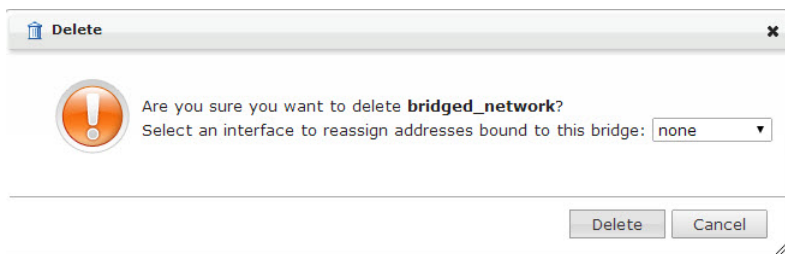
Removing a bridge removes the ACL setting of the bridge. The bridge IP address settings are also dropped. If there are other L3 interfaces with access rights to the web

console, then the IP address and netmask of the bridge is optional. If not, it may result in the loss of web console access for Deep Edge. Users can access the CLI to repair this condition.

Procedure

1. Go to **Network > Bridge**.
2. Select the check box next to the network bridge.
3. Click  **Delete**.

A delete confirmation message appears.



4. (Optional) Select an interface to reassign addresses bound to the selected interface.



Important

Deep Edge overwrites the original interface settings when bridging the interfaces. If you configured administrative access on the bridged pair, removing the bridge without reassigning the addresses bound to the bridge may affect access to the Deep Edge appliance. If another interface handles administrative access, removing the bridge pair will not affect access to the appliance.

-
5. Click **Delete** to remove the network bridge.
-

Routing Traffic

Deep Edge works as a security device on a network and packets must pass through it. You must understand certain basic routing concepts to configure the Deep Edge unit appropriately.

Deep Edge supports configuring static, dynamic, or policy-based routes at **Network > Routing**. Deep Edge supports these dynamic protocols for IPv4 and IPv6:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Deep Edge selects routes and updates its routing table dynamically based on the specified rules. Given a set of rules, the unit can determine the best route or path for sending packets to a destination. For details about routing traffic, see [Overview of Routing Mode on page 3-15](#)

About Static Routes

Static routes control how traffic moves between endpoints connected to the network. Defining a static route provides Deep Edge with the information to forward a packet to a particular destination. Configure static routes by defining the destination IP address and netmask of packets that the Deep Edge appliance is intended to intercept, and by specifying a gateway IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.

You can specify through which interface packets leave and to which device to route packets. The Static Route list at **Network > Routing > Static Routes** displays information that the Deep Edge appliance compares to packet headers in order to route packets.

Adding a Static Route

When new static routes are added, Deep Edge checks whether a matching route and destination already exist in the Deep Edge routing table. If no match is found, Deep Edge adds the route to the routing table.

To configure IPv6 static routes, select **IPv6 from the Protocol** drop-down list box.

Procedure

1. Go to **Network > Routing > Static Routes**.

2. Click **Add New** to add a default route.

The **Add/Edit Static Route** window appears.

3. Select **Enable static route**.

4. In **Network**, specify the network address.

Any of the following options are valid:

- **IP address**
- **Default gateway** (Example: 0.0.0.0/0)

**Note**

If multiple default gateways are configured, outgoing traffic is routed from these gateways using round-robin selection.

- **Bitmask**

**Note**

The bitmask is the decimal equivalent of the netmask.

- **Class InterDomain Routing (CIDR) notation** (Example: 255.255.255.0/24)

5. In **Nexthop**, specify the next-hop IP address.

6. Click **Apply**.
-

Enabling/Disabling Static Routes

Procedure

1. Go to **Network > Routing > Static Routes**.
 2. In the list of static routes, do one of the following:
 - Select the **Enable** icon () to enable the static route.
 - Deselect the **Enable** icon () to disable the static route.
-

Modifying a Static Route

Procedure

1. Go to **Network > Routing > Static Routes**.
2. Do one of the following:
 - In the **Route ID** column, click the route name.
 - In the **Action** column, click the edit icon ()

The **Add/Edit Static Route** screen appears.

3. Use the check box to enable or disable the static route.
 4. View the network IP address/bitmask. This field is read-only.
 5. Specify the next hop parameters.
 6. Click **Apply**.
-

Deleting a Static Route

Procedure

1. Go to **Network > Routing > Static Routes**.
 2. In the **Action** column, click the delete icon .
 3. Click **Delete** to verify the deletion.
-

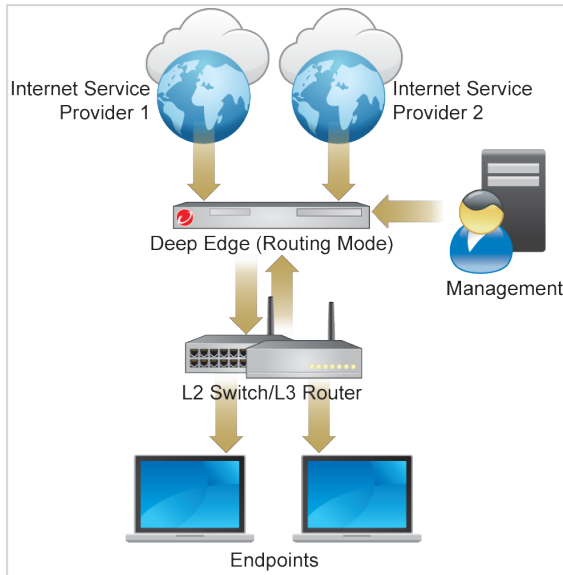
About Policy-based Route Management

In today's high performance networks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. While static and dynamic routing focus on the traffic destination for routing, policy-based routing provides a mechanism to mark packets so that certain kinds of traffic receive differentiated routing. Destination-based routing techniques make it difficult to change the routing behavior of specific traffic. Also known as “intelligent routing”, policy-based routing allows you to dictate the routing behavior based on a number of different criteria other than destination network, including source interface, source or destination address, or service type.

Consider a company that has two links between locations, one a high bandwidth, low delay expensive link and the other a low bandwidth, higher delay lower expense link. Using traditional routing protocols, the higher bandwidth link would get most if not all of the traffic sent across it based on the metric savings obtained by the bandwidth and/or delay (using EIGRP or OSPF) characteristics of the link. Policy-based routing can route higher priority traffic over the high bandwidth/low delay link while sending all other traffic over the low bandwidth/high delay link.

With policy-based routing, Deep Edge can route traffic from multiple ISPs and WANs. The following illustration shows how to configure Deep Edge for two ISPs using an L2 switch.

FIGURE 3-4. Policy-based Routing Example



If the monitoring IP addresses of one interface are unavailable, all policy-based routes associated with that interface are disabled. All traffic matching the policy-based routing rules is routed via the default gateway. To configure the monitoring IP addresses, go to [Monitoring Hosts on page 3-5](#). If multiple default gateways are configured, then outgoing traffic is routed from these gateways using round-robin selection.

Automatic Failover for Multiple ISP/WAN Environments

Deep Edge supports automatic failover among multiple WAN/ISP links when an ISP or WAN connection fails. Deep Edge checks the connection every ten (10) seconds. If Deep Edge cannot detect a connection, Deep Edge continues to check every two (2) seconds. After four (4) consecutive unsuccessful connection attempts, automatic failover initiates. The link automatically recovers if a connection is established later.

When a failover occurs, do the following:

- View the system event log
- Check the routing table to verify the actual traffic routing

**Note**

For more information about monitoring hosts, see [Monitoring Hosts on page 3-5](#).

Adding a Policy-based Route

When the network traffic does not match any policy-based routing rule, the default gateway (static route to 0.0.0.0/0) applies to all traffic. To configure a default gateway, go to [Adding a Static Route on page 3-25](#).

**Tip**

Trend Micro recommends configuring at least one default gateway.

Procedure

1. Go to **Network > Routing > Policy Routing**.
2. Click **Add New**.
3. Optionally enable the rule.
4. Specify a policy name between 1 and 32 characters, consisting of letters, numbers, or underlines.
5. Type an optional **Description**.
6. Under **Source Addresses**, select one of the following parameters:
 - **Any**: Includes all source addresses. (Default)
 - **Selected addresses**: Displays a list of previously configured source addresses available or to add a new IP address.

**Note**

To add new address objects, see [Configuring Address Objects on page 3-11](#).

7. Select the appropriate source interface from the drop-down box.
8. Under **Destination Addresses**, select one of the following parameters:

- **Any:** Includes all destination addresses
- **Selected addresses:** Displays a selectable list of previously configured destination addresses to use. Use this option to add address objects, if needed.

**Note**

To add destination addresses, see [Configuring Address Objects on page 3-11](#)

9. Under **Service type**, select one of the following parameters:

- **Any:** Include all services
- **Selected:** Include only selected services

10. Select the egress interface.

11. For interfaces with static IP addresses, specify the next hop.

12. Optionally enable network masquerading.

**Note**

Enable network masquerade if internal IP address must be translated to the IP address of the egress interface.

13. Click **OK**.

About Dynamic Route Management

This section explains how to configure dynamic protocols to route traffic through large or complex networks. Dynamic routing protocols enable Deep Edge to automatically share information about routes with neighboring routers and learn about routes and networks advertised by them. Deep Edge supports the following dynamic routing protocols:

- Routing Information Protocol (RIP) and RIP for IPv6
- Open Shortest Path First (OSPF) and OSPF for IPv6

Deep Edge selects routes and dynamically updates its routing table based on the specified rules. Given a set of rules, Deep Edge can determine the best route or path for sending packets to a destination. You can also define rules to suppress routes advertising to neighboring routers and change Deep Edge routing information before it is advertised.

About Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance-vector routing protocol. The Deep Edge implementation of RIP supports RIP version 2 (see RFC 2453) and RIPng (see RFC 2080).

RIP was designed for small IP networks and relies on hop count to determine routes; the best routes have the fewest number of hops. RIP is based on UDP and uses port 520 for route updates. By limiting routes to a maximum of 15 hops, the protocol helps prevent routing loops, but also limits the supported network size. If more than 15 hops are required, traffic is not routed. RIP also can take longer to converge than OSPF and other routing protocols.

When RIP is enabled, Deep Edge multicast requests for RIP updates from each of its RIP-enabled interfaces. Neighboring routers respond with information from their routing tables. Deep Edge adds routes from neighbors to its own routing table only if those routes are not already recorded in the routing table. When a route already exists in the routing table, Deep Edge compares the advertised route to the recorded route and chooses the shortest route for the routing table.

RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the unit, while a hop count of 16 represents a network that Deep Edge cannot reach. Each network that a packet travels through to reach its destination usually counts as one hop. When Deep Edge compares two routes to the same destination, it adds the route having the lowest hop count to the routing table.

Similarly, when RIP is enabled on an interface, Deep Edge sends RIP responses to neighboring routers on a regular basis. The updates provide information about the routes in the Deep Edge routing table, subject to the rules that you specify for advertising those routes. You can specify how often Deep Edge sends updates, how long a route can be kept in the routing table without being updated, and, for routes that

are not updated regularly, how long the unit advertises the route as unreachable before it is removed from the routing table.

When configuring RIP settings, make sure to specify the networks running RIP and any additional settings needed to adjust RIP operation on the Deep Edge interfaces connected to the RIP-enabled network.

About Global RIP Settings

When configuring global RIP settings, you must specify the networks running RIP and any additional settings needed to adjust RIP operation on the Deep Edge interfaces connected to the RIP-enabled network.

Enabling RIP Global Settings

Procedure

1. Go to **Network > Routing > RIP**.
 2. Open the **Global** tab.
 3. Select the **Enable RIP Service** check box.
 4. Click **Apply**.
-

Configuring RIP IP Settings

Procedure

1. Go to **Network > Routing > RIP**
2. On the upper right side of the tabs, select the **Protocol**.
 - IPv4
 - IPv6

3. Click **Apply**.
-

Configuring Advanced RIP Settings

Procedure

1. Go to **Network > Routing > RIP > Global**.
2. Expand **Advanced Settings**.
3. Select **Distribute default route** to enable distribution of default routes.



Note

Distributing the default route is not enabled until the change is applied.

4. Set the timers as needed.

See [Advanced RIP Timer Descriptions on page 3-34](#).

5. Click **Apply**.
-

Advanced RIP Timer Descriptions

TABLE 3-3. Advanced RIP timer settings

TIMER	DESCRIPTION
Timeout	Amount of time (seconds) that Deep Edge waits between sending RIP updates. Default: 30 seconds
Garbage	Maximum amount of time (seconds) that a route is reachable while no updates are received for the route. This is the maximum time Deep Edge keeps a reachable route in the routing table while no updates for that route are received. If Deep Edge receives an update for the route before the timeout period expires, the timer restarts. The Timeout period should be at least three times longer than the Update period set for the Upgrade timer. Default: 180 seconds

TIMER	DESCRIPTION
Garbage	Amount of time (seconds) that Deep Edge advertises a route as unreachable before deleting the route from the routing table. The value determines how long an unreachable route remains in the routing table. Default: 120 seconds

About Network RIP Settings

The network settings of IP addresses and netmasks apply to the major networks connected through Deep Edge that run RIP. When adding a network to the Networks list, the Deep Edge interfaces that are part of the network are advertised in RIP updates. You can enable RIP on all Deep Edge interfaces whose IP addresses match the RIP network address space.

Adding a New RIP Network

Procedure

1. Go to **Network > Routing > RIP**.
 2. Open the **Network** tab.
 3. Click **Add New**.
 4. Specify the IP address/netmask for the new RIP network.
 5. Click **Apply**.
 6. Verify the new RIP network appears in the list at **Network > Routing > RIP > Network**.
-

Modifying a RIP Network

Context for the current task

Procedure

1. Go to **Network > Routing > RIP**.

2. Open the **Network** tab.
 3. In the **Action** column, click the edit icon () of the RIP network to modify.
 4. Click **OK** to confirm.
-

Deleting a RIP Network

Procedure

1. Go to **Network > Routing > RIP**.
 2. Open the **Network** tab.
 3. In the **Action** column, click the delete icon () of the RIP network to delete.
 4. Click **OK** to confirm.
-

About the Redistribute RIP Settings

Select one or more options to redistribute RIP updates about routes that were not learned through RIP. Deep Edge can use RIP to redistribute routes learned from directly connected networks, kernels, static routes, and OSPF.

Configuring the Redistribution Options

Procedure

1. Go to **Network > Routing > RIP**.
2. Open the **Redistribute** tab.
3. Select the redistribution options:

OPTION	DESCRIPTION
Redistribute kernel	Select to redistribute routes that were installed in the kernel routing table
Redistribute connected	Select to redistribute routes learned from directly connected networks
Redistribute static	Select to redistribute routes learned from static routes
Redistribute OSPF	Select to redistribute routes learned through OSPF

4. Click **Apply**.

About Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a link-state routing protocol that is most often used in large heterogeneous networks to share routing information among routers in the same Autonomous System (AS). Deep Edge supports OSPF version 2 (see RFC 2328) and OSPF version 3 (see RFC 2740).

The main benefit of OSPF is that routing overhead is reduced by only advertising routes when neighbors change state instead of at timed intervals.

OSPF dynamically determines routes by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The router keeps information about the links between it and the destination to make highly efficient routing decisions. A cost is assigned to each router interface, and the best routes are determined to be those with the lowest costs, when summed over all the encountered outbound router interfaces and the interface receiving the LSA.

Deep Edge uses hierarchical techniques to limit the number of routes that must be advertised and the associated LSAs.



Note

Due to dynamically processing a considerable amount of route information, OSPF has greater processor and memory requirements than RIP.

About Global OSPF

The global settings for OSPF allow you to enable OSPF, specify the Route ID, and enable the default route distribution.

Router ID

Specify a unique router ID to identify Deep Edge to other OSPF routers. By convention, the router ID is the numerically highest IP address assigned to any of the Deep Edge interfaces.

If you change the router ID while OSPF is configured on an interface, all connections to OSPF neighbors will be broken temporarily. The connections will re-establish themselves.

Enabling Global OSPF Settings

Procedure

1. Go to **Network > Routing > OSPF > Global**.
 2. Select the **Enable OSPF Service** check box.
 3. Specify the **Router ID**.
 4. Click **Apply**.
-

Enabling the OSPF Distribute Default Route

Procedure

1. Go to **Network > Routing > OSPF > Global**.
 2. Select the **Distribute default route** check box.
 3. Click **Apply**.
-

About Area OSPF

The **Area OSPF** information refers to the areas making up an **OSPF** in Deep Edge. The header of an **OSPF** packet contains an area ID, which helps to identify the origination of a packet.

Access the list of OSPF areas at **Network > Routing > OSPF > Area**.

To add a new **OSPF** area, configure the following:

- **Area ID**—The unique identifier of an area.
- **Area type**—The options for area types include:

TABLE 3-4. Area Type

AREA TYPE	DESCRIPTION
Normal	A regular OSPF area containing more than one router, each having at least one OSPF-enabled interface to the area.
Stub	To reach the OSPF backbone, the routers in a stub area must send packets to an area border router. Routes leading to non-OSPF domains are not advertised to the routers in stub areas. The area border router advertises a single default route into the stub area, which ensures that any OSPF packet that cannot be matched to a specific route will match the default route. Any router connected to a stub area is considered part of the stub area.
NSSA	In a Not-So-Stubby Area (NSSA), routes that lead out of the area into a non-OSPF domain are made known to OSPF. However, the area itself continues to be treated like a stub area
Stub, no summary	Same as a stub area without Link-State Advertisement (LSA) or external destination information.
NSSA, no summary	Same as an NSSA, without Link-State Advertisement (LSA) or external destination information.
Area network	Define an interface on which OSPF runs for the Area ID

AREA TYPE	DESCRIPTION
(Optional) Area virtual link	Configure the virtual link settings to maintain or enhance backbone area connectivity. The settings must be defined for area border routers, and must be defined within the backbone area (0.0.0.0). Specify the IP address/bitmask for each virtual link to be included in the backbone area. The IP address/bitmask describes the router ID of the router (neighbor) on the other side of the virtual link.

Adding a New OSPF Area

Procedure

1. Go to **Network > Routing > OSPF > Area**.
 2. Specify the **Area ID**.
 3. For **Area type**, specify the following:
 - Normal
 - Stub
 - NSSA
 - Stub, no summary
 - NSSA, no summary
 4. To add a network, expand **Network Settings** and specify a valid IP address/netmask.
 5. If needed, expand **Vlink Settings** and add a router IP address..
 6. Click **Apply**.
 7. Verify that the new area displays in the list at **Network > Routing > OSPF > Area**.
-

Modifying an OSPF Area

Procedure

1. Go to **Network > Routing > OSPF > Area**.
2. Do one of the following:
 - In the **Area ID** column, click IP address.
 - In the **Action** column, click the edit icon .The **Add/Edit OSPF Area** screen appears.
3. Modify the OSPF area settings.
4. Click **Apply**.
5. Verify that the new area changes display in the list at **Network > Routing > OSPF > Area**.

Deleting an OSPF Area

Procedure

1. Go to **Network > Routing > OSPF > Area**.
2. In the **Action** column, click the delete icon .
3. To confirm, click **Delete**.
4. Verify that the OSPF area was removed from the list at **Network > Routing > OSPF > Area**.

About OSPF Interfaces

An OSPF interface definition contains specific operating parameters for a Deep Edge OSPF-enabled interface. The definition includes the interface name (for example,

external or VLAN_1), priority, and timer settings for sending and receiving OSPF Hello and dead-interval packets.

You can enable OSPF on all Deep Edge interfaces with an IP addresses that matches the OSPF-enabled network space. For example, define an area of 0.0.0.0 and the OSPF network as 10.0.0.0/16. Then define vlan1 as 10.0.1.1/24, vlan2 as 10.0.2.1/24 and vlan3 as 10.0.3.1/24. All three VLANs can run OSPF in area 0.0.0.0. To enable all interfaces, create an OSPF network 0.0.0.0/0

It is possible to configure different OSPF parameters for the same Deep Edge interface when more than one IP address has been assigned to the interface. For example, the same Deep Edge interface could connect to two neighbors through different subnets. You can configure an OSPF interface definition containing one set of Hello and dead-interval parameters for compatibility with one neighbor's settings, and a second OSPF interface definition for the same interface to ensure compatibility with the second neighbor's settings.

To view OSPF operating parameters for a Deep Edge interface, go to **Network > Routing > OSPF > Interface**.

Modifying an OSPF Interface

Procedure

1. Go to **Network > Routing > OSPF > Interface**.
2. Click the name of the OSPF interface to change.
3. Change one or more of the following options as needed:

OPTION	DESCRIPTION
Passive option	Select check box to restrict the OSPF interface from sending or receiving OSPF packets.
Interface	Select the Deep Edge interface name to associate with this OSPF interface definition (for example, port1, external, or VLAN_1). The Deep Edge unit can have physical, VLAN, virtual IPsec or GRE interfaces connected to the OSPF-enabled network.

OPTION	DESCRIPTION
Priority	Specify the OSPF priority for this interface (0-255). It is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR.
Hello Interval	Optionally, set the Hello Interval to be compatible with Hello Interval settings on all OSPF neighbors. This setting defines the period of time (in seconds) that Deep Edge waits between sending Hello packets through this interface.
Dead Intervals	Optionally, set the Dead Interval to be compatible with Dead Interval settings on all OSPF neighbors. This setting defines the period of time (in seconds) that Deep Edge waits to receive a Hello packet from an OSPF neighbor through the interface. If Deep Edge does not receive a Hello packet within the specified amount of time, Deep Edge declares the neighbor inaccessible. By convention, the Dead Interval value is usually four times greater than the Hello Interval value.

- Click **Apply**.
- Verify the changes in the list at **Network > Routing > OSPF > Interface**.

About Redistribute OSPF

Distribute routing information from the kernel, connected, static, or RIP.

Select one or more of the options (kernel, connected, static, and/or RIP) to redistribute OSPF link-state advertisements about routes that were not learned through OSPF. Deep Edge can use OSPF to redistribute routes learned from directly connected networks, static routes, and RIP.

Redistributing OSPF

Redistribute link-state advertisements not learned through OSPF.

Procedure

- Go to **Network > Routing > OSPF > Redistribute**.

2. Check one or more of the following options:

OPTION	DESCRIPTION
Redistribute kernel	Redistribute routes installed in the kernel routing table.
Redistribute connected	Redistribute routes learned from directly connected networks.
Redistribute static	Redistribute routes learned from static routes.
Redistribute RIP	Redistribute routes learned from directly RIP networks.

3. Click **Apply**.
-

About Routing Table

In the factory default configuration, the Deep Edge routing table contains a single static default route. Add routing information to the routing table by defining additional static routes. The table may include several different routes to the same destination—the IP addresses of the next-hop router specified in those routes or the Deep Edge interfaces associated with those routes may vary.

Deep Edge evaluates the information in the routing table and selects the best route to a destination, typically the shortest distance between the Deep Edge unit and the closest next-hop router. In some cases, a longer route is selected if the best route is unavailable. Deep Edge installs the best available routes in the unit's forwarding table, which is a subset of the unit's routing table. Packets are forwarded according to the information in the forwarding table.

Viewing the Routing Table

Procedure

1. Go to **Network > Routing > Routing Table**.
2. On the upper right side of the tabs, select the **Protocol**.
 - IPv4

- IPv6

Routing Table Indicators

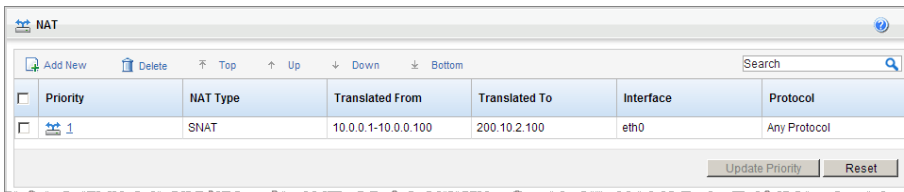
The following table explains routing table indicators.

CODE	DEFINITION
K	Kernel route
C	Connected
S	Static
R	RIPng
O	OSPFv3

Network Address Translation (NAT)

Use Network Address Translation (NAT) policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports on Layer 3 interfaces. For example, private source addresses can be translated to public addresses on traffic sent from an internal (trusted) zone to a public (untrusted) zone.

The following NAT policy rule translates a range of private source addresses (10.0.0.1 to 10.0.0.100) to a single public IP address (200.10.2.100) and a unique source port number (dynamic source translation). The rule applies only to traffic received on a Layer 3 interface in the internal (trusted) zone that is destined for an interface in the public (untrusted) zone. Because the private addresses are hidden, network sessions initiate from the public network. If the public address is not a Deep Edge interface address (or on the same subnet), the local router requires a static route to direct return traffic to Deep Edge.

**FIGURE 3-5. Simple NAT Rule**

NAT Rules

NAT address translation rules are based on the source and destination addresses and ports. Similar to security policies, NAT policy rules are compared against the incoming traffic in sequence, and the first rule matching the traffic is applied.

As needed, add static routes to the local router so that traffic to all public addresses is routed to Deep Edge. You can also add static routes to the receiving interface on Deep Edge to route traffic back to the private address.

Adding a Source NAT Rule

Source NAT (SNAT) changes the source address in the IP header of a packet. The primary purpose is to change the private (RFC 1918) address/port into a public address/port for packets leaving the network. The following table explains the required configurations if using SNAT.

Procedure

1. Go to **Network > NAT > Add New**.
2. Configure the NAT settings based on the NAT type, then click **Apply**.

OPTION	DESCRIPTION
NAT type	Select Source NAT to specify settings when IP packets are received.

OPTION	DESCRIPTION
Egress Interface	Select ANY or any L3 interface from the drop-down box list to act as an interface for egress traffic, which is traffic that originates from inside the network.
Source IP translation	Select from the following options: • Egress interface IP address—Egress interface IP address is used for translation. When not using the egress interface IP address, users must explicitly specify an interface with one of the next three options. • Single IP address—IP address specified will be used for translation. • IP address range—IP address range specified will be used for translation. • Subnet—Subnet specified will be used for translation.
Description	Specify an identifying characteristic about use or configuration for the NAT rule.
Advanced options for SNAT	Allow users to specify more detailed information or matching conditions, including: • Protocol—Any, TCP, or UDP. Any means all protocols. • Source IP address range—Specified by the network. • Source Port range—Specified by administrator. • Destination IP address range—Specified by administrator. • Destination Port range—Specified by administrator.

3. Verify that the new rule is added to the list at **Network > NAT**.

Adding a Destination NAT Rule

Destination NAT (DNAT) changes the destination address in IP header of a packet. The primary purpose of this is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside the network. The following table explains the required configurations if using DNAT.

Procedure

1. Go to **Network > NAT > Add New**.
2. Configure the NAT settings based on the NAT type, then click **Apply**.

NAT type	Select Destination NAT to specify setting when IP packets are forwarded.
Ingress interface	Select ANY or any L3 interface from the drop-down list to act as the interface for network traffic that originates from outside of the network's routers and proceeds toward a destination inside of the network.
Destination IP translation	Select from the following options: • Use Ingress Interface IP—Ingress Interface IP address range specified will be used for translation. When not using the ingress interface IP address, users must explicitly specify an interface with the next option, Use Virtual IP address. • Use a Virtual IP address—When users specify an external IP address range, the translated IP address range is automatically generated according to the beginning IP address. The mapping is one-to-one mapping. • Port Forward—Check the Port Forward check box for static one-to-one NAT mapping with port forwarding: an external IP address is always translated to the same mapped IP address, and an external port number is always translated to the same mapped port number. Select the protocol from Any, TCP, or UDP. (Any means all protocols.) When users specify the External Service Port range, the Map to Port will be generated automatically according to the beginning port. The mapping is one-to-one mapping.
Description	Specify an identifying characteristic about use or configuration for the NAT rule.

Advanced options for DNAT	Allow users to specify more detailed information or matching conditions, including: • Source IP address range: Specified by administrator. • Source Port range: Specified by administrator.

3. Verify that the new rule is added to the list at **Network > NAT**.

Modifying NAT Rules

Procedure

1. Go to **Network > NAT**.
2. In the **Priority** column, click the number of the NAT rules to change.
3. Edit the parameters as needed.
4. Click **Apply**.
5. Verify the changes at **Network > NAT**.

Changing NAT Rule Priorities

Procedure

1. Go to **Network > NAT**.
2. Select the check box of the NAT rule to be given a higher priority.
3. To rearrange the order, use the operators (Top, Up, Down, Bottom) above the NAT rules list.
4. Click **Update Priority** to save changes.

Deleting NAT Rules

Procedure

1. Go to **Network > NAT**.
 2. Select the row of the NAT rule to delete.
 3. Click  **Delete**.
The **Delete** confirmation message appears.
 4. To confirm, click **Delete**.
 5. Verify that the NAT rule is no longer listed at **Network > NAT**.
-

Services

Deep Edge services support allows for Domain Name Server (DNS) Forwarding, Dynamic Host Configuration Protocol (DHCP) server, and Dynamic DNS (DDNS) configuration settings.

About DNS Forwarding

Several Deep Edge functions use DNS, including alert email messages and URL filtering. Specify the IP addresses of the DNS servers to which Deep Edge connects. DNS server IP addresses are usually supplied by your ISP.

You can configure Deep Edge to obtain DNS server addresses automatically. To obtain these addresses automatically, at least one Deep Edge interface must use the DHCP (or PPPoE) addressing mode. For configuration details, see [About DHCP on page 3-51](#).

Deep Edge can provide DNS Forwarding on their interfaces. Hosts on the attached network use the interface IP address as their DNS server. DNS requests sent to the interface are forwarded to the configured DNS server addresses or that Deep Edge automatically obtained.

Users can enable and disable DNS forwarding in Deep Edge or specify a name server to use local DNS or customized DNS.

Configuring DNS Forwarding Settings

Procedure

1. Go to **Network > Services > DNS Forwarding**.
 2. Select a DNS forwarding settings.
For option details, see [DNS Forwarding Settings on page 3-51](#).
 3. Click **Apply**.
-

DNS Forwarding Settings

The following table describes Deep Edge DNS forwarding settings.

SETTING	DESCRIPTION
Disable DNS forwarding	No DNS forwarding is available.
Use system DNS settings	This option applies only to the Deep Edge appliances operating in NAT / route mode. Deep Edge forwards DNS requests to the configured DNS server IP addresses.
Use specified DNS servers	Specify the IP addresses of the primary and secondary Domain Name Service (DNS) servers that will be used on the clients in IPv4 or IPv6 format.

About DHCP

Deep Edge supports multiple Dynamic Host Configuration Protocol (DHCP) services for the network interface. It supports multiple pools and one DHCP pool supports one physical pool. Specify the IPv4 or IPv6 DHCP services and configure the IPv4 or IPv6 DHCP settings at **Network > Services > DHCP**.

Deep Edge automatically responds with a DHCP request to interfaces configured with DHCP. Configure DHCP to use the Deep Edge appliance, interface, or specified DNS IP addresses and then configure the IP address pool and default gateway address that the DHCP server provides.

DHCP Advanced Settings: Static Mapping and Lease Time

SETTING	DESCRIPTION
Static Mapping	Enables assignment of static IP addresses with manual bindings.
Lease time	Denotes any limitations on the DHCP lease interval. Specify days, hours, or minutes. For example, if you specify only hours, then the lease is restricted to that number of hours.

Viewing DHCP Services and Settings

Procedure

1. Go to **Network > Services > DHCP**.
2. In the table, view the parameters associated with any DHCP service:

OPTION	DESCRIPTION
Name	Name of the DHCP service (examples: eth0, eth1).
IP Address/ Netmask	The IP address/bitmask leased from the DHCP server.
Enable	The icon indicates the state of the service: enable (green/on) or disable (red/off).
IP Pools	Range of applicable IP addresses for the DHCP service.

OPTION	DESCRIPTION
Options	The DNS server IP address, the gateway IP address, and the lease time. The DNS IP address shows only when the DHCP server uses a specified DNS.
Action	Click the icon to edit the DHCP service settings.

Modifying DHCP Service Settings

Procedure

1. Go to **Network > Services > DHCP**.
2. Do one of the following:
 - In the **Name** column, click the name of the DHCP server to modify.
 - In the **Action** column, click the edit icon  in the row of the DHCP service to modify.
3. Modify the parameters associated with the DHCP service:

OPTION	DESCRIPTION
Enable DHCP	Select to enable the service.
IP address / Netmask	View the IP address and subnet mask leased from the DHCP server.
Preferred DNS	Select the preferred DNS method. • Select Use system DNS settings to use the appliance system DNS configured at Network > DNS. • Select Use the interface IP address to use the interface IP address as the DNS. If the DHCP server is enabled and DNS forwarding is disabled, Deep Edge automatically enables DNS forwarding through the system DNS settings. If DNS forwarding is already enabled, Deep Edge maintains the existing DNS forwarding configuration.

OPTION	DESCRIPTION
	• Select Use specified DNS servers to manually configure the DNS settings. If the specified IP addresses match the interface DNS addresses, make sure to check that the DNS forwarding settings also match.
Gateway	The DHCP server gateway automatically populates based on interface IP address and netmask settings. Optionally change the IP address.
IP address range from and to	Specify the range of IP addresses to create the IP Pool to which the DHCP configuration applies .

4. Change the **Advanced Settings**, if needed.
 - For **Lease time**, adjust the time and date when the leased IP address and netmask is no longer valid.
 - For **Static mapping**, specify MAC address and IP addresses to add to the service.
 5. Click **Apply**.
 6. Verify the settings changed at **Network > Services > DHCP**.
-

About Dynamic DNS

A Dynamic Domain Name System (DDNS) refers to the updating of Internet DNS name servers in real-time to keep the active DNS configuration of host names, addresses, and other information up to date. It is typically used when businesses have frequent changes to the public host-name-to-IP-address mappings, usually when companies use PPPoE or DHCP to obtain Internet access. Using a DDNS service provides an automated way to deal with the propagation of new hostname-to-IP address mapping across the Internet. DDNS service providers act as a broker to manage this process. Deep Edge is designed to be the first Internet-facing device an external client would connect to when trying to reach the business, it needs to make sure that all Internet users route their traffic to it for each host name / domain that they are trying to

reach on the business side. With the DDNS client, Deep Edge can communicate host-name-to-IP address changes to the DDNS service provider.

With the Deep Edge Dynamic DNS support, register their domains on the website of DDNS service vendors, and then configure information such as their account, password, and domain to have it maintained by Deep Edge. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software (implementing RFC 2136 or other protocols) running on an endpoint or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS queries. The Deep Edge DDNS client monitors the public IP address changes and auto-synchronizes the IP address-domain mapping.

**Note**

Some abnormal events will be logged, such as unexpected return status from the service vendor. All updating events are logged.

Supported DDNS Service Providers

The four supported DDNS service providers are:

PROVIDER	USER SCOPE
Dyn DNS	Global
Free DNS	
Oray	China
DNSPod	

**Note**

IPv6 is not supported.

Configuring the DDNS Client

Configure basic settings according to the service vendor. The information needed varies between different services. Basically, each service requires the domain name, account, and password information.

Some vendors (such as Oray and Dyn DNS) provide HTTPS connections as an option. Others (such as FreeDNS) do not expose the HTTPS interface, while DNSPod requires mandatory HTTPS connections.

Procedure

1. Go to **Network > Services > Dynamic DNS > General**.
2. In the Dynamic DNS dialog box, do the following information:
 - a. Select the **Enable Dynamic DNS** check box.
 - b. Select a **Vendor**.
 - c. Type the **User name, Password**, and **Domain**.
 - d. Select the WAN interface:

Auto:	(Default) Deep Edge auto-discovers an interface with non-private IP address according to RFC 1597
Other:	Deep Edge will always try to get public IP address from the interface.

3. For Oray only, select the **Service level**. All non-Free services are paid services required for HTTPS connections.
 - Free
 - Professional
 - Enterprise
 - Ultimate
4. If **Professional** was selected in **Service level**, select **Enable HTTPS**.

5. Click **Apply**.

DDNS Status

The **Network > Services > Dynamic DNS > Status tab** shows the current DDNS running status, including current interface (auto-discovered or specified), WAN IP address, and status message.

Possible status messages include:

- SUCCESS
- ERROR: Authentication failed
- ERROR: Account hasn't been activated
- ERROR: Invalid or unregistered domain info
- ERROR: Internet access unavailable or can't connect to service vendor
- ERROR: Used some paying user only features, such as HTTPS connection service, related settings has been reset
- ERROR: Service unavailable Message from Service Vendor
- ERROR: No Available WAN IP detected
- ERROR: No suitable IP on specified interface
- ERROR: Service Interface may have changed, please contact Trend Micro for updating
- ERROR: Too many authentication failures, the account was banned temporarily
- ERROR: Invalid or unregistered sub domain info
- ERROR: Update host in a round robin way is not allowed.
- ERROR: Unknown error, please check your internet access.

- Not Enabled

Virtual Private Network

Virtual Private Network (VPN) technology is generally used to ensure that employees working off-site can remotely access their corporate network with appropriate security measures in place. In general terms, authentication is the process of attempting to verify the (digital) identity for both accessing network resources and logging on the VPN network. VPN leverages existing infrastructure (the Internet) to securely build and enhance existing connectivity. Based on standard secure Internet protocols, VPN implementation enables secure links between special types of network nodes, secure gateways. Site-to-site VPN ensures secure links between gateways. User VPN ensures secure links between gateways and remote access clients.

A typical Deep Edge deployment allows users to remotely connect to the corporate network resources using VPN. Other remote sites are guarded by Deep Edge and strict security policies regulate communication between all network resources and the remote endpoint.

Deep Edge supports IPV4-to-IPV4 VPN access.

User VPN

Whenever users access the organization from remote locations, it is essential that the usual requirements of secure connectivity be met but also the special demands of remote clients. User Virtual Private Networking (VPN) extends VPN functionality to remote users, enabling users to securely communicate sensitive information to networks and servers over the VPN tunnel, using both dial-up (including broadband connections), and LAN (and wireless LAN) connections.

For details about configuring LDAP or Local User accounts for VPN access, see [End User Management on page 6-9](#).

Point-to-Point Tunneling Protocol (PPTP) VPN

This section explains how to specify a range of IP addresses for PPTP clients or configure the PPTP client-side IP address to be used in the tunnel setup.

Deep Edge supports Point-to-Point Tunneling Protocol (PPTP) to tunnel PPTP traffic between two VPN peers. Windows or Linux PPTP clients can establish a PPTP tunnel with a Deep Edge that has been configured to act as a PPTP server. As an alternative, configure Deep Edge to forward PPTP packets to a PPTP server on the network behind the Deep Edge. PPTP VPN is available only in NAT/Route mode. The current maximum number of PPTP sessions is 254.

When using Deep Edge as a PPTP gateway, select a PPTP client IP from a local address range or use the server defined in the PPTP user group. Select which method to use for IP address retrieval and, in the case of the user group server, provide the IP address and the user group.

You must select the local user or LDAP for authentication at **Administration > End User Management > General Settings** tab.

Enabling PPTP VPN

Procedure

1. Go to **Network > User VPN > PPTP VPN**.
 2. Select the **Enable PPTP** check box.
 3. Click **Apply**.
-

Configuring General PPTP VPN Settings



Note

If LDAP is configured to authenticate PPTP VPN users, Deep Edge can only support unencrypted password(PAP) authentication protocol.

Procedure

1. Go to **Network > User VPN > PPTP VPN > General**.
2. Select how the IP address is assigned:

OPTION	DESCRIPTION
IP address pool	Specify the IP address (192.168.0.0) of the clients gaining remote access through PPTP.
DHCP server	Specify the IP address/bitmask of the DHCP server (sample 10.10.1.1./24) and select the valid interface (eth1-eth3) from the drop-down list box.

3. Configure **Advanced Settings**, if needed.

See [Advanced Settings: Enabling Debug Mode and Encryption Level on page 3-60](#).

4. Click **Apply**.
-

Advanced Settings: Enabling Debug Mode and Encryption Level

Deep Edge PPTP VPN uses Microsoft Point-to-Point Encryption (MPPE). MPPE is a protocol for encrypting data across Point-to-Point Protocol (PPP) and Virtual Private Network (VPN) links. It uses the RSA RC4 encryption algorithm. MPPE supports 40-bit and 128-bit session keys, which are changed frequently to improve security.

Procedure

1. Go to **Network > User VPN > PPTP VPN > General**.
 2. Click the **Advanced Settings** link.
 3. Specify the **Encryption** strength:
 - 40 bits (Weak)
 - 128 bits (Strong)
 4. To show additional debugging information in PPTP logs, elect the **Enable Debug Mode** check box.
 5. Click **Apply**.
-

Viewing PPTP VPN Clients

The **Clients** tab shows all clients currently connecting through VPN. The table displays the user name, when the session started, the client public IP address, and the virtual IP address. The total number of connected clients is displayed above the table.

Procedure

1. Go to **Network > User VPN > PPTP VPN**.
 2. Click the **Clients** tab.
-

Viewing PPTP VPN Logs for Troubleshooting

Procedure

1. Go to **Network > User VPN > PPTP VPN**.
 2. Click the **Troubleshooting** tab.
-

PPTP VPN Troubleshooting

If there are problems setting up the PPTP VPN, you may receive the following errors.

TABLE 3-5. Understanding PPTP VPN Error Messages

ERROR MESSAGE	EXPLANATION	RECOMMENDED ACTION
VPN Error 800 - Unable to establish the VPN connection.	PPTP packets from the VPN client cannot reach the Deep Edge server.	- Ping the Deep Edge appliance, assuming pinging is allowed (that is, not blocked) between the PPTP client and the Deep Edge appliance. Confirm that you have network connectivity between the PPTP client and the Deep Edge appliance. - To allow PPTP traffic, configure the network firewall to open TCP port 1723 and to forward IP protocol 47 for Generic Routing Encapsulation (GRE) traffic to the Deep Edgeserver. Some firewalls refer to IP protocol 47 as VPN or PPTP pass-through.
VPN Error 734 - The PPP link control protocol terminated.	The protocol between the PPTP client and Deep Edge server is mismatched.	For security considerations, Deep Edge appliance only supports MS-CHAP Version 2 and Point-to-Point Encryption. Make sure the PPTP client supports these two protocols.
VPN Error 691 - Access denied because user name and/or password is invalid on the domain	User name and/or password is invalid.	Input the correct user name and/or password or ask your System Administrator to reset the password.

Secure Socket Layer Virtual Private Network

A Secure Sockets Layer Virtual Private Network (SSL VPN) is a form of VPN that can be used with a standard web browsers. The Deep Edge SSL VPN solution requires client software installation, and is ideal for applications including web-based email, business and government directories, file sharing, remote backup, remote system management, and consumer-level electronic commerce.

When users have complete administrative rights over their endpoints and use a variety of applications, tunnel mode allows remote clients to access the local internal network as if they were connected to the network directly.

This section provides information about the features of SSL VPN available for configuration in the web-based manager. Only Deep Edge appliances that run in NAT/Route mode support the SSL VPN feature.

Enabling SSL VPN

Procedure

1. Go to **Network > User VPN > SSL VPN > General**.
 2. Select the **Enable SSL VPN** check box.
-

Configuring General SSL VPN Server Settings

SSL VPN must be enabled to perform this procedure. To configure the general SSL VPN settings, select the interface, protocol (TCP/UDP), port, and authentication method associated with the VPN server. All SSL VPN clients use the override host name option when accessing the corporate network.

Procedure

1. Go to **Network > User VPN > SSL VPN > General**.
2. Use the **Protocol** drop-down list to select the protocol or SSL VPN.
 - TCP
 - UDP
3. In **Port**, specify the SSL port number.
4. Configure **Local Networks**.

See *Configuring Local Networks for SSL VPN* on page 3-64.

5. Configure **Virtual IP Pool Settings**.

See *Configuring Virtual IP Address Pools for SSL VPN on page 3-64*.

6. Configure **Advanced Settings**.

See *Configuring Advanced Settings for SSL VPN on page 3-65*.

7. Click **Apply**.
-

Configuring Local Networks for SSL VPN

Procedure

1. Go to **Network > User VPN > SSL VPN > General**.
 2. Click the **Local Networks**.
 3. Click **Add New**.
 4. Specify the IP address/bitmask for the local network.
 5. Click **OK**.
 6. Verify that the local network was added at **Network > User VPN > SSL VPN > General > Local Networks**.
-

Configuring Virtual IP Address Pools for SSL VPN

Procedure

1. Go to **Network > User VPN > SSL VPN > General**.
2. Click **Virtual IP Pool Settings**.
3. Specify the **Network pool** (default: 10.252.1.0).
4. Select the bitmask value from the drop-down list box.

5. Click **Apply**.

Configuring Advanced Settings for SSL VPN

Procedure

1. Go to **Network > User VPN > SSL VPN > General**.
2. Click **Advanced Settings**.
3. Select the **Encryption algorithm**:

OPTION	DESCRIPTION
AES 128 CBC	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
AES 192 CBC	A 192-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
AES 256 CBC	A 256-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.
3DES	Triple-DES, in which plain text is encrypted three times by three keys.
BF-CBC	A 64-bit block keyed, symmetric Cipher Block Chaining (CBC) algorithm by Blowfish.



Note

The Digital Encryption Standard (DES) is a 64-bit block algorithm that uses a 56-bit key. The Advanced Encryption Standard (AES) is a private key algorithm supporting key lengths from 128 to 256 bits and variable-length blocks of data.

4. Select the **Authentication algorithm**:

OPTION	DESCRIPTION
MD5	Message Digest (version 5) hash algorithm (on one-way hash function) developed by RSA Data Security, which is intended for digital signature

OPTION	DESCRIPTION
	applications, where a large file must be compressed in a secure manner before being encrypted with a private key/public key algorithm.
SHA1	Secure Hash Algorithm 1, which produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.

5. Select the **Key size**:
 - 1024-bit
 - 2048-bit
 6. Set the **Key lifetime** options in hours (1-24). Maximum allowable hours is 24.
 7. Specify the **Local DNS** settings.
 8. Add or remove **Local Domains**:
 - Use the >> option to add a new local domain
 - Use the << option to remove an existing local domain
 9. Select **Enable compress traffic** to allow SSL VPN traffic to be transparently compressed and uncompressed.
 10. Select **Enable debug mode** to show additional debugging information SSL VPN logs.
 11. Select **Enable simultaneous logon** to allow multiple client to use a single account.
 12. Select **Enable network masquerade** to automatically add the NAT rule.
 13. Click **Apply**.
-

Viewing SSL VPN Clients

The **Clients** tab shows all clients currently connecting through VPN. The table displays the user name, when the session started, the client public IP address, and the virtual IP address. The total number of connected clients is displayed above the table.

Procedure

1. Go to **Network** > **User VPN** > **SSL VPN**.
 2. Select the **Clients** tab
-

Viewing SSL VPN Logs

Procedure

1. Go to **Network** > **User VPN** > **SSL VPN**.
 2. Select the **Troubleshooting** tab.
-

Client Installation

Deep Edge supports several SSL VPN client installation types.

For Windows users, the SSL VPN client installation package automatically installs when logging on using the SSL VPN portal at:

`https://<appliance_server_IP_address>/`

For Linux or Mac users, download the latest installation package from <http://openvpn.net>. Obtain the SSL VPN configuration files from `https://<appliance_server_IP_address>/`.

SSL VPN Windows Client Supported Browsers

OPERATING SYSTEM	BROWSER
Windows XP	• Internet Explorer 7, 8, 9 • Firefox 21+ (with JRE installed) • Chrome 27+ (with JRE installed)

OPERATING SYSTEM	BROWSER
Windows 7	• Internet Explorer 8, 9, 10 • Firefox 21+ (with JRE installed) • Chrome 27+ (with JRE installed)

Installing the SSL VPN Client on Linux or MAC OS

Procedure

1. Access `https://<appliance_server_IP_address>/` with a browser.
2. Click the **Configuration package** for Linux and MacOS to download the `sslvpnlinuxconfig.tgz` file.
3. Extract the `sslvpnlinuxconfig.tgz` file to a local folder, and then copy the `ca.crt` and `openvpn.ovpn` files to the **OpenVPN** configuration folder.

The the client machine dials into Deep Edge. For problems, check [SSL and VPN Troubleshooting on page 3-77](#).

Installing the SSL VPN Client on iOS

Procedure

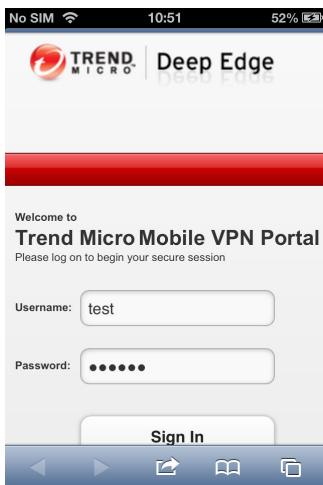
1. Install **OpenVPN Connect** from the App Store.



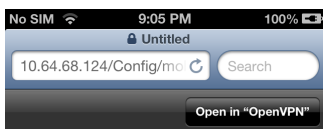
2. Open the **OpenVPN Connect** application.



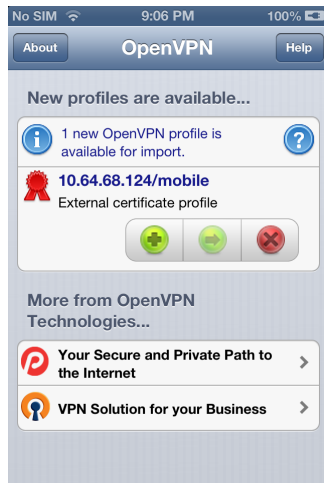
3. Access the Deep Edge VPN portal ([https://<appliance_server IP_address>/](https://<appliance_server_IP_address>/)) from Safari and log on.



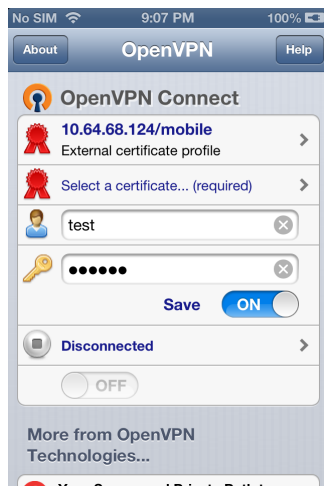
4. Download the OVPN file from https://<appliance_server_IP_address>/Config/mobile.ovpn.



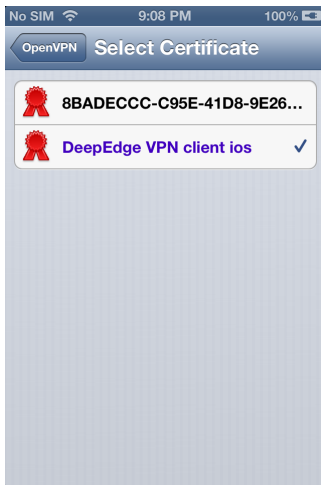
5. Tap **Open in “OpenVPN”** to load the configuration file with OpenVPN Connect.



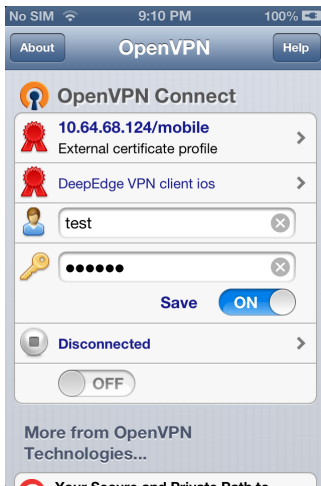
6. Tap “+” to configure the profile.



7. Tap **Select a certificate... (required)** and then tap **DeepEdge VPN client iOS** to select the certificate.



8. Tap **OpenVPN** to return to the main menu.



9. Specify the account user name and password and then switch **OFF** button under **Disconnected** to access the Deep Edge SSLVPN server.

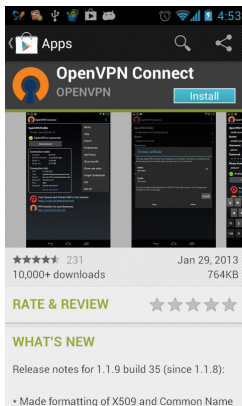


SSLVPN tunnel is established and the user can access internal resources via the secure VPN tunnel.

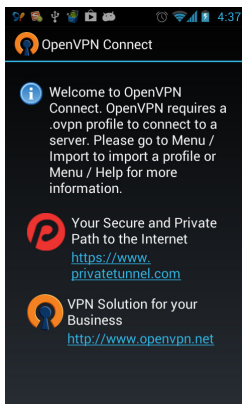
Installing the SSL VPN Client on Android OS (4.0+)

Procedure

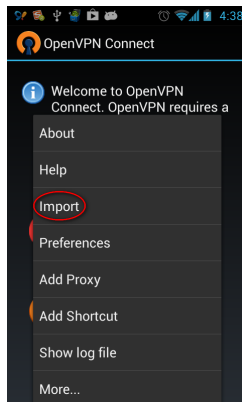
1. Download the SSLVPN mobile configuration file from [https://<appliance_server_IP address>/Config/mobile.ovpn](https://<appliance_server_IP_address>/Config/mobile.ovpn) and then copy configuration file to the Android device's SD card.
2. Install **OpenVPN Connect** from Google Play.



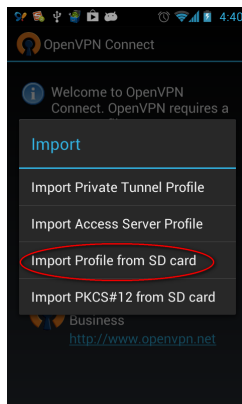
3. Open the **OpenVPN Connect** application.



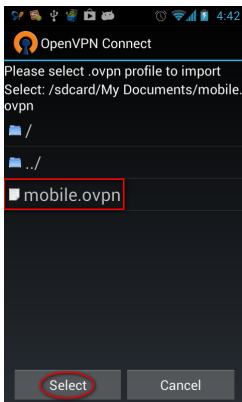
4. Press the **Action Overflow** button and then select **Import**.



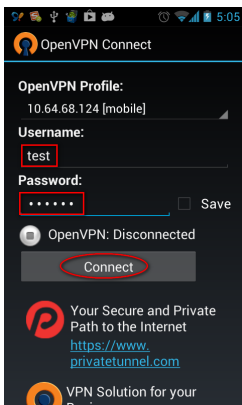
5. Select **Import Profile from SD card**.



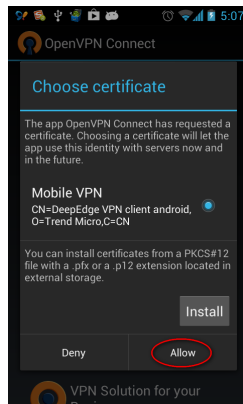
6. Select **mobile.ovpn** and then tap **Select**.



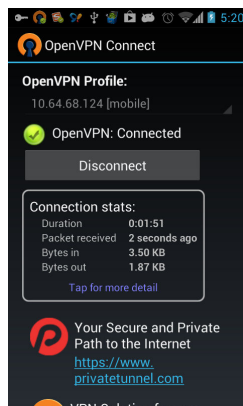
7. Specify the user name and password, and then tap **Connect**.



8. Tap **Allow**.



The **OpenVPN Connect** screen appears.



SSLVPN tunnel is established and the user can access internal resources via the secure VPN tunnel.

SSL and VPN Troubleshooting

If there are problems setting up SSL VPN, the following list explains some general troubleshooting guidelines:

Procedure

- Verify that the client can ping the Deep Edge appliance successfully.
 - Verify that the client can access the SSL VPN-configured TCP or UDP port.
 - Verify that the Windows client configuration file `openvpn.ovpn` is configured the same as the `https://<appliance_server_IP_address>/Config/openvpn.ovpn` file.
 - Verify that the mobile client configuration file **mobile.ovpn** is configured the same as the `https://<appliance_server_IP_address>/Config/mobile.ovpn`.
-

Understanding SSL VPN Error Messages

ERROR MESSAGE	EXPLANATION	RECOMMENDED ACTION
TCP: connect to X.X.X.X:8445 failed, will try again in 5 seconds: Connection refused	SSL VPN client cannot reach the Deep Edge appliance.	1. Ping the Deep Edge appliance, assuming ping is allowed (that is, not blocked) between the SSL VPN client and the Deep Edge appliance. Confirm that you have network connectivity between the SSL VPN client and the Deep Edge appliance. 2. To allow SSL VPN traffic, configure the network firewall to open the SSL VPN-configured TCP or UDP port to the Deep Edge appliance.
SIGTERM[soft,auth-failure] received, process exiting	User name and/or password is invalid.	Specify the correct user name and/or password or ask an Administrator to reset the password.

Mobile VPN

Deep Edge provides VPN services not only to laptops or desktops but also mobile devices. Mobile VPN offers support for mobile devices in the “closed” environment of Apple iOS or the “open sourced” Android.

Deep Edge provides VPN support on iOS and Android devices by utilizing the built-in IPsec VPN clients. No agent installation is required for the mobile devices.

Deep Edge supports the creation of policy profiles that support the “VPN on Demand” feature of iOS. This support offers the ability to push iOS policy profiles to the iOS devices. This enables the iOS device to automatically trigger and establish a VPN connection whenever a corporate resource is accessed.

**Note**

Android devices do not support VPN on demand..

Mobile VPN supports the following functions:

- User authentication with the corporate LDAP server
- DHCP Server integration of the corporate environments to vend out IP addresses to the remote clients
- Split Tunneling occurs when only corporate traffic is routed via the VPN tunnel and non-corporate traffic is routed via the provider’s network
- Split DNS occurs when corporate resources are sent to the DNS server residing in the corporate environment via the VPN tunnel. Lookups for non-corporate resources are sent to the provider’s DNS Server
- Usage of multiple devices by a single user
- Revocation of VPN access for any devices. Revocation is made possible by removing the user credentials from the corporate LDAP Server or local user database
- Management interface for creating and managing policies and monitoring all the activity related to VPN connections including:

Mobile VPN supports the following functions: Local users added at **Administration > End User Management > Local User** are accepted by mobile VPN, SSL VPN, and PPTP VPN.

Configuring Mobile VPN General Settings

The IPSec remote access VPN connection is disabled by default. Make sure to configure required settings to enable it. The options in the following task define:

- the interface to use
- the user authentication method to use
- the network pool and local network to use
- VPN On Demand (for iOS) configurations

Procedure

1. Go to **Network > User VPN > Mobile VPN > General** tab.
2. Select the **Enable Mobile VPN connection** check box.
3. Select an interface from the **Interface** drop-down list box to use for mobile VPN client connections.
4. Specify the IP address and netmask for the pool network for the virtual IP addresses that can be assigned to connecting clients.
5. Specify the IP address of the **Local Network**.
6. For Apple devices, configure **VPN on Demand (for iOS)** settings.
 - a. Select the **VPN On Demand** check box to allow certificate-based VPN configurations, which automatically triggers VPN connections when accessing certain domains.



Note

Enabling VPN On Demand (for iOS) adds this information to the profile file.

- b. Specify the **Domain or Host** information.

c. Select the condition under for establishing connection:

- Always establish
- Never establish
- Establish if needed

7. Click **Apply**.

Viewing Mobile VPN Clients

The **Clients** tab shows all clients currently connecting through VPN. The table displays the user name, when the session started, the client public IP address, and the virtual IP address. The total number of connected clients is displayed above the table.

Procedure

1. Go to **Network > User VPN > Mobile VPN**.
 2. Click the **Clients** tab.
-

Configuring Advanced Mobile VPN Settings

The **Advanced** tab provides some settings for advanced feature such as split DNS and split tunneling.

Procedure

1. Go to **Network > User VPN > Mobile VPN**.
2. Click the **Advanced** tab.
3. Select **Dead peer detection** to enable the system to detect dead (offline) remote systems.
4. Select the appropriate IKE debug level:
 - **Control**

- **Emitting**
 - **Parsing**
 - **Raw**
 - **Crypt**
5. Select **Enable Network Masquerade** to automatically add the NAT rule.
 6. Select **Enable Split Tunneling** to split the local networks specified on the **General** tab.

Only corporate traffic is routed via the VPN tunnel; non-corporate traffic is routed via the provider's network. For details about setting the local network, see [*Configuring Mobile VPN General Settings on page 3-80*](#)

7. Select **Enable Split DNS** to send corporate resources via the VPN tunnel to the DNS server residing in the corporate environment.

**Note**

Non-corporate lookups are sent to the provider's DNS server.

- a. In **DNS Server**, specify the DNS server IP address of the DNS server residing inside the corporate environment.
- b. In **Local Domains**, specify all relevant local domains that correspond to the DNS server.

**Note**

If no local domains are specified, the mobile VPN clients cannot resolve FQDN.

8. Click **Apply**.
-

Troubleshooting Mobile VPN

The **Troubleshooting** tab shows live logs of IPSec daemons useful for debugging.

Procedure

1. Go to **Network > User VPN > Mobile VPN > Troubleshooting** tab.
 2. View the live logs readout.
-

Mobile Device VPN Configuration

Virtual Private Networks (VPN) are often used within organizations to allow you to communicate private information securely over a public network. You must configure VPN, for example, to access your work email account on an iOS device. VPN works over both Wi-Fi and cellular data network connections. Deep Edge uses an IPsec connection solution, and no agent is needed on the mobile device.

Mobile VPN establishes an authenticated, encrypted tunnel, enabling mobile users to securely access applications and network resources residing on the corporate network via a public network. Deep Edge provides mobile VPN applications for both Apple iOS and Android devices.

Accessing Mobile VPN for Apple Devices

Procedure

1. Access the Deep Edge VPN portal using Safari by going to `https://<appliance__IP_address>`.

The **Welcome to Trend Micro Mobile VPN Portal** page appears.

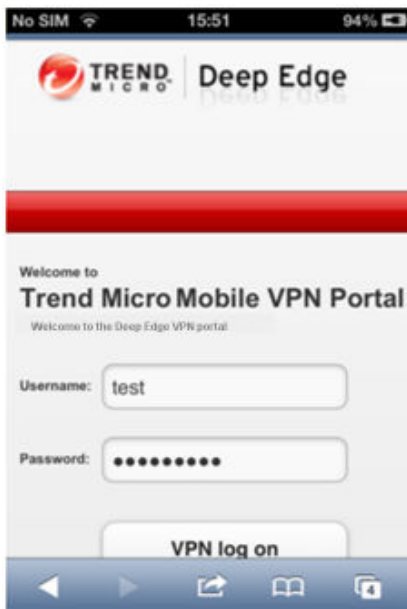


FIGURE 3-6. Mobile VPN Login

2. Specify a valid user name and password, then press **VPN log on**.

The **Download profile file from here** link displays.

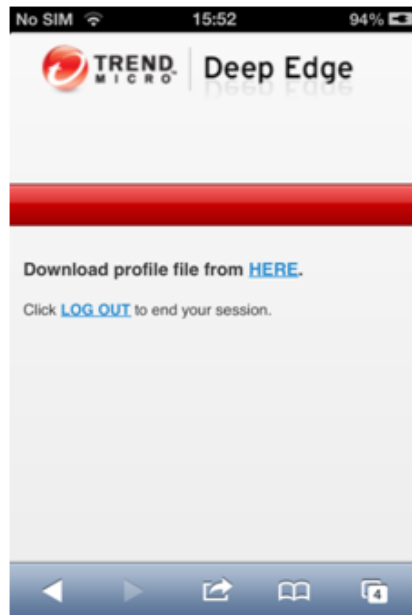


FIGURE 3-7. Mobile VPN Profile Download

3. Press the **HERE** link to install the VPN profile.
4. Press the **Install** button.



FIGURE 3-8. Install Profile

5. Press **Install Now** in the **Unsigned Profile** warning.



FIGURE 3-9. Acknowledge Unsigned Profile



FIGURE 3-10. Mobile VPN Profile Summary

6. Press **Done** and return to the **Login** page.
7. Press **LOGOUT** link to log out.

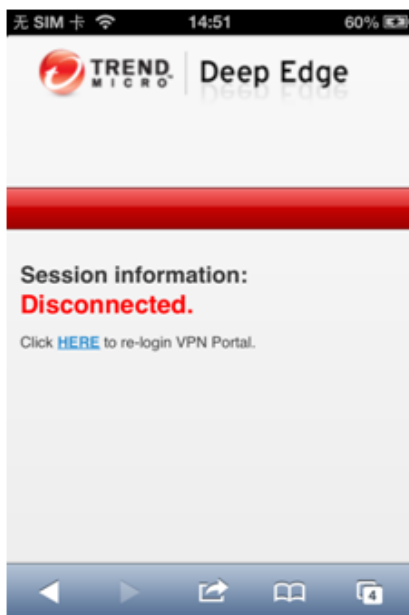


FIGURE 3-11. Logged Out Confirmation

Changing Mobile VPN Settings for Apple Devices

Change the Mobile VPN settings to access internal company resources from iOS devices.



Note

If the you enable VPN On Demand from the Deep Edge web console, then the mobile VPN tunnel establishes automatically, providing the mobile user accesses a pre-defined domain or host.

Procedure

1. Log on the Mobile VPN portal. For details see: *Accessing Mobile VPN for Apple Devices on page 3-83*

2. Go to **Settings > VPN**.



FIGURE 3-12. Changing your Mobile VPN settings

3. Press **Mobile VPN Trend Micro** to continue.



4. Type valid account and password credentials, then press **Save** to return to the previous screen.
5. Switch to on.

The VPN connection will be established.



FIGURE 3-13. Mobile VPN Connected Status displays

Accessing Mobile VPN for Android Devices

Procedure

1. Access the Deep Edge VPN portal pointing your browser to: `https://<appliance_IP address>`.

A security warning appears.

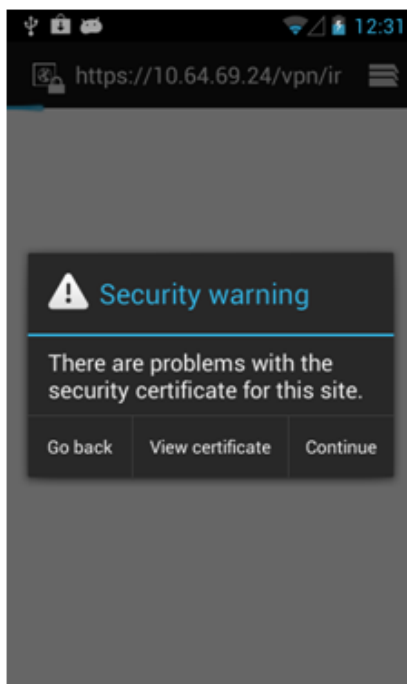


FIGURE 3-14. Accessing the Mobile VPN Portal

2. Acknowledge the warning and click **Continue**.

The **Welcome to Trend Micro Mobile VPN Portal** page appears.



FIGURE 3-15. Trend Micro Mobile VPN Login

3. Specify a valid user name and password, and then press **VPN log on**.



FIGURE 3-16. Setup Options

4. Tap the **HERE** link to download certificates.
An **Extract certificate** window appears.

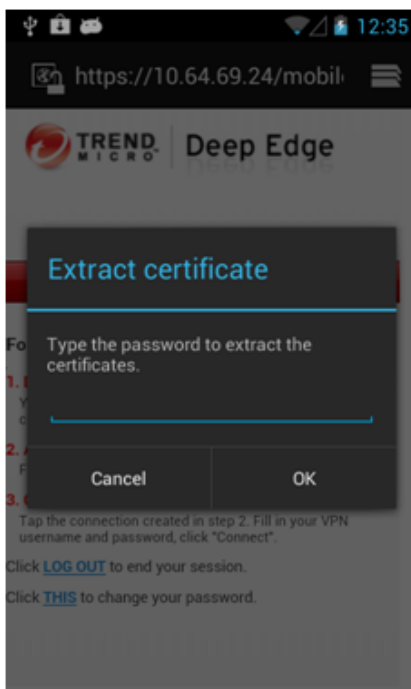


FIGURE 3-17. Certificate download

5. Type **111111** to extract the certificates, then tap **OK**.

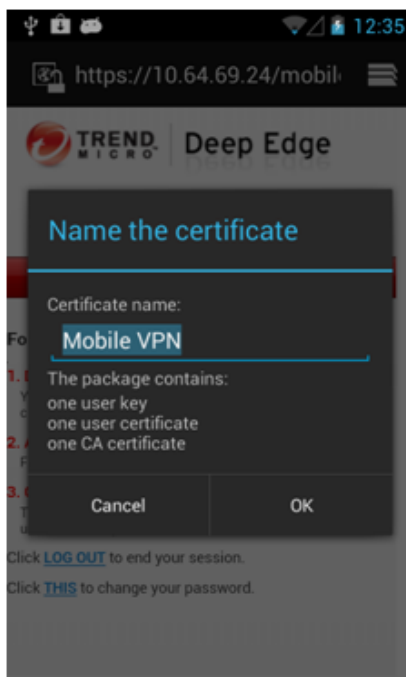


FIGURE 3-18. Add Certificate Name

6. Specify the default certificate name or rename it, and press **OK**.
The certificate file downloads.
7. Return to the **Setup Options** screen.

What to do next

Tap **LOG OUT** to log out or tap **THIS** to add a VPN connection. For more information, see [Adding a Mobile VPN Connection for Android Devices on page 3-97](#)

Adding a Mobile VPN Connection for Android Devices

You must add a mobile VPN connection before the Android device can establish a VPN tunnel and access internal company resources.

**Note**

Unlike Apple devices, Android devices do not support VPN On Demand.

Procedure

1. Log on the Mobile VPN portal. For more information, see [Accessing Mobile VPN for Android Devices on page 3-92](#)
2. To add a new connection, tap **THIS** under the **2. Add a new VPN connection** option of the **Setup Options** screen.

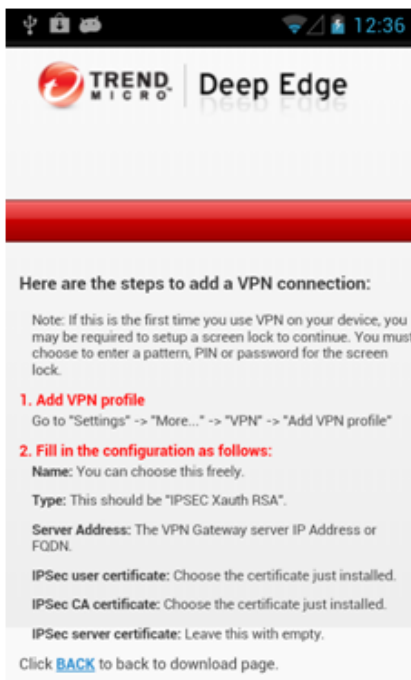


FIGURE 3-19. Configuring a new VPN connection

3. Follow the steps for adding a VPN connection:
 - a. Go to **Settings > More > VPN > Add VPN profile**.

b. Add the following information:

Name	Specify a name.
Type	Type IPSEC Xauth RSA
Server Address	specify the VPN gateway server IP address or FQDN
IPsec User Certificate	Select the previously installed certificate. For more information, see: Accessing Mobile VPN for Android Devices on page 3-92
IPsec CA Certificate	Select the previously installed certificate.
IPsec Server Certificate	Leave blank.

4. Log out after reviewing how to add a VPN connection.
5. Log in and go to **Settings > More > VPN > Add VPN profile**.

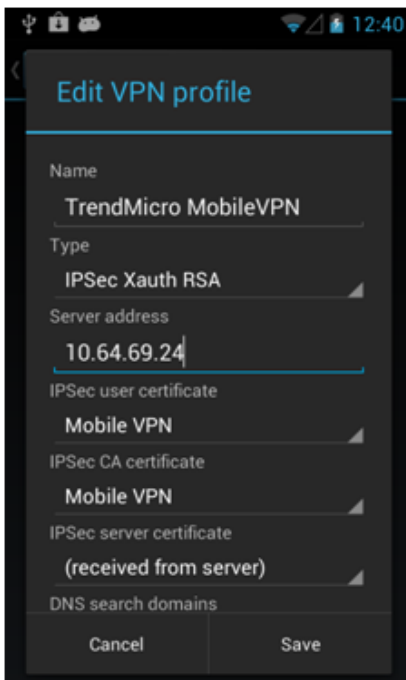


FIGURE 3-20. Editing your VPN profile

6. Press **Save**.

The new profile displays.

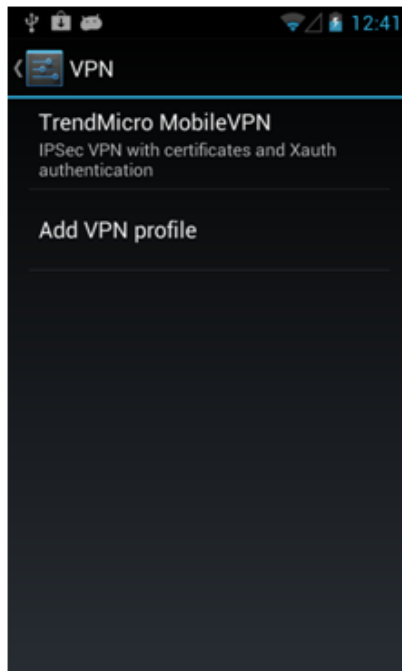


FIGURE 3-21. New Mobile VPN profile

7. Press the new created VPN profile to connect to Deep Edge.

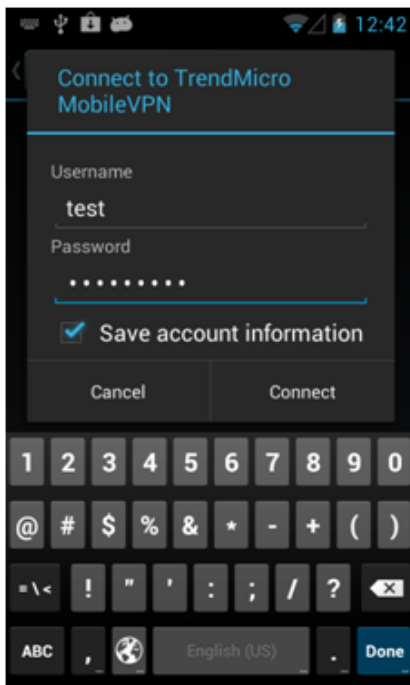


FIGURE 3-22. Connect to the new Mobile VPN profile

8. Type a valid user name and password, then press **Connect**.

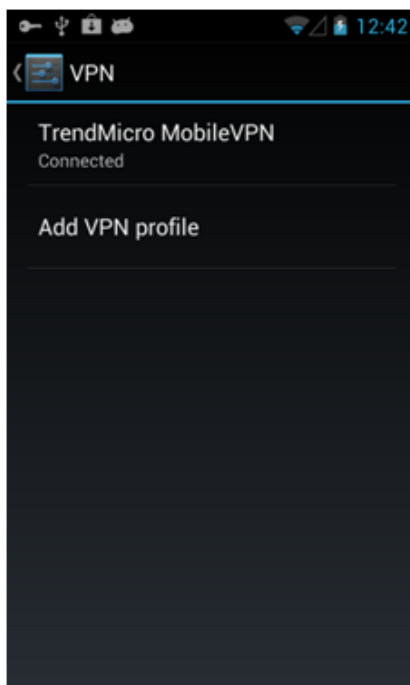


FIGURE 3-23. Connected Status

Customizing the VPN Portal

The VPN portal login page is customizable to include a company logo, company name, and welcome message

Procedure

1. Go to **Network > User VPN > Portal Customization**.
2. Click **Browse** to locate the logo file.

**Note**

Use a .PNG or .GIF file format. Do not exceed 700 x 60 pixels or 1MB in size.

3. Click **Upload** to upload the file.
 4. Type a value in the **Company Name** field.
 5. Update the welcome message in the **Welcome Message** field.
 6. Click **Apply**.
-

Site-to-Site VPN

A Virtual Private Network (VPN) is a network that employs encrypted tunnels to exchange securely protected data. Deep Edge creates encrypted tunnels by using the Internet Key Exchange (IKE) and IP Security (IPsec) protocols. IKE creates the VPN tunnel, and this tunnel is used to transfer IPSec encoded data.

Think of IKE as the process that builds a tunnel, and IPSec packets as trucks that carry the encrypted data along the tunnel.

Deep Edge units implement the Encapsulated Security Payload (ESP) protocol. The encrypted packets look like ordinary packets that can be routed through any IP network.

IKE is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode, supported in NAT/Route mode only, creates a virtual interface for the local end of a VPN tunnel.

IPsec Connections

A dynamic routing protocol daemon running on the security gateway can exchange routing information with a neighboring routing daemon running on the other end of an **IPSec** tunnel/connection.

An IPsec (or VPN) tunnel is a virtual interface on a security gateway associated with an existing VPN connection, and is used by IP routing as a point-to-point interface directly connected to a VPN peer gateway.

Outbound packets use the following routing process:

- An IP packet with destination address X is matched against the routing table
- The routing table indicates that IP address X should be routed through a point-to-point link which is the VPN tunnel interface that is associated with peer gateway Y
- The VPN kernel intercepts the packet as it specifies the virtual tunnel interface
- The packet is encrypted using the proper IPsec authentication type parameters with peer gateway Y, and the new packet receives the peer gateway Y's IP address as the destination IP
- Based on the new destination IP, the packet is rerouted to the physical interface according to the appropriate routing table entry for Y's address

Inbound packets use the following routing process:

- An IPsec packet specifies the machine coming from gateway Y
- The VPN kernel intercepts the packet on the physical interface
- The VPN kernel identifies the originating VPN peer gateway
- The VPN kernel decapsulates the packet, and extracts the original IP packet
- The VPN kernel detects that a VPN tunnel interface exists for the peer VPN gateway, and reroutes the packet from the physical interface to the associated VPN tunnel interface
- The packet specifies the IP stack through the VPN tunnel interface

Adding a New IPsec Connection

Use **Site-to-Site VPN** to establish IPsec VPN tunnels between Deep Edges.



Note

Make sure that Ethernet interfaces and routers are configured properly.

Procedure

1. Go to **Network > Site-to-site VPN > Connections**.
2. Click **Add New Connections**.

The **Add/Edit IPsec Connections** dialog box appears.

3. Specify the IPsec connection parameters.

Enable IPsec connect	Select the check box to enable the tunnel.
Name	Type a name to identify the IPsec tunnel.
Gateway type	Select Initiate (active) or Response (passive) role of the IPsec tunnel.
Gateway	Specify the gateway IP address.
Interface name	Select the interface name from the drop-down list box (eth0, eth1).
Policy name	Select the policy name from the drop-down list box, either Default or a specific policy, that applies to the IPsec tunnel.  Note Configure non-default IPsec policies at Network > Site-to-site VPN > Policies.
Authentication type	Select Pre-shared key or RSA key from the drop-down list box.
For Pre-shared Key	Specify the key and confirm it. If Pre-shared Key is selected, specify the pre-shared key that Deep Edge uses to authenticate itself to the remote peer or dial-up client. Make sure to define the same value at the remote peer or client. The key must contain at least six printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

For RSA key	Specify the public key. If RSA key is selected, select the name of the server certificate that Deep Edge uses to authenticate to the remote peer.
VPN ID	Input the local IP address if the IPsec gateway is behind a NAT device.
Add Local Networks	Select the local network, or add a new address object.
Add Remote Networks	Select the remote network, or add a new address object.

4. Click **Apply**.
5. Verify the new IPsec connection at **Network > Site-to-site VPN > Connections**.

Site-to-site VPN Policies

Deep Edge allows you to configure the IKE encryption and authentication algorithms used for VPN policies.

Adding VPN Site-to-site Policies

Procedure

1. Go to **Network > Site-to-site VPN > Policies**.
2. Click **Add New**.
3. Specify a name for the new IPsec policy.
4. Select **IKE encryption algorithm** from the drop-down list box:

**Note**

The Digital Encryption Standard (DES) is a 64-bit block algorithm that uses a 56-bit key. The Advanced Encryption Standard (AES) is a private key algorithm supporting key lengths from 128 to 256 bits and variable-length blocks of data.

OPTION	DESCRIPTION
3DES	Triple-DES, in which plain text is encrypted three times by three keys.
AES 128	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
AES 192	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
AES 256	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

5. Select the **IKE authentication algorithm** value from the drop-down list box.
 - MD5—Message Digest (version 5) hash algorithm (on one-way hash function) developed by RSA Data Security, which is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private key/public key algorithm.
 - SHA1—Secure Hash Algorithm 1, which produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
6. Select the **IKE SA lifetime** value (in hours, maximum 24) from the drop-down list box (1-24). It specifies the length of time that the negotiated key will stay effective.
7. Select the **IKE DH group** value from the drop-down list box that are supported by secure gateways.
 - Group2: MODP—1024 bits (default)
 - Group5: MODP—1536 bits
 - Group14: MODP—2048 bits

The above groups refer to the Diffie-Hellman key computation (also known as exponential key agreement) that is based on the Diffie-Hellman (DH) mathematical groups supported by a security gateway for IKE and IPsec Security Association (SA).

8. Select the `IPsec encryption` value from the drop-down list box.
 - No encryption—Do not use an encryption algorithm.
 - 3DES
 - AES 128
 - AES 192
 - AES 256
 9. Select the `IPsec authentication algorithm` value from the drop-down list box.
 - MD5
 - SHA1
 10. Select the `IPsec lifetime` value (in hours, maximum 24) from the drop-down list box (1-24).
 11. Select the `IPsec PFS group` value from the drop-down list.
 - None
 - Group2: MODP
 - Group5: MODP
 - Group14:MODP
 12. Click **Apply**.
 13. Verify the new policy is listed at **Network > Site-to-site VPN > Policies**.
-

Advanced IPsec Configuration

Advanced configuration options for site-to-site VPN at **Network > Site-to-site VPN > Advanced Options** include:

CONFIGURATION	DESCRIPTION
Use dead peer detection	Dead peer detection identifies inactive or unavailable IKE peers through ICMP ping and can help restore resources that are lost when a peer is unavailable. Selecting Use dead peer detection reestablishes VPN tunnels on idle connections and cleans up dead IKE peers if required. Use this option to receive notifications whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dynamic DNS peer connects from an IP address that changes periodically, traffic may suspend while the IP address changes.
IKE Debugging	Select the check boxes of the following IKE debug options: • Control—Shows IKE decision making • Emitting—Shows the structure of output messages • Parsing—Shows the structure of input messages • Raw—Shows the raw bytes of messages • Crypt—Shows the encryption and decryption status of messages
Current local public RSA key	Displays the current public portion of the local RSA key in a format that can be copied and specified into remote devices that use IPsec RSA authentication.
Regenerate local RSA Key	Regenerates the local RSA key with a different key length and overwrites the currently installed RSA key.

IPSec Status

To view the live IPSec connection status, go to **Network > Site-to-site VPN > Status** tab.

IPsec Troubleshooting

Network > Site-to-site VPN > Troubleshooting displays the live IPSec log. Use the IPSEC logs to view activity on IPSec VPN tunnels.

IPsec Troubleshooting: Branch Office Configuration Example

In the first example, two branch offices are connected to a headquarters office.

Headquarters:	Public IP 1.1.1.1, on interface eth0. Local networks are 10.0.0.0/8
Branch Office #1:	Public IP 2.2.2.1, on interface eth0. Local networks are 192.168.10.0/8
Branch Office #2:	Public IP 3.3.3.1, on interface eth0. Local networks are 192.168.20.0/8

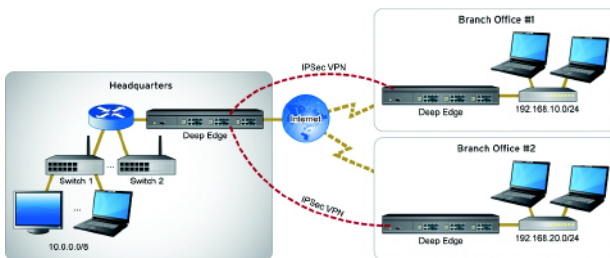


FIGURE 3-24. Deep Edge connecting two branch offices by IPSec VPN

TABLE 3-6. VPN Connection Configuration

LOCATION	CONFIGURATION
Headquarters	Name: HQ Enable: Yes Gateway type: Response Interface name: Eth0 Policy name: default Authentication type: Pre-shared key Key: ***** Local Network: 10.0.0.0/24 Remote Network: 192.168.10.0/24 and 192.168.20.0/24
Branch Office #1	Name: toHQ1 Enable: Yes Gateway type: Initiate Gateway: 1.1.1.1 Interface name: Eth0 Policy name: default Authentication type: Pre-shared key Key: ***** Local Network: 192.168.10.0/24 Remote Network: 10.0.0.0/24

LOCATION	CONFIGURATION
Branch Office #2	Name: toHQ1 Enable: Yes Gateway type: Initiate Gateway: 1.1.1.1 Interface name: Eth0 Policy name: default Authentication type: Pre-shared key Key: ***** Local Network: 192.168.10.0/24 Remote Network: 10.0.0.0/24

IPsec Troubleshooting: Configuration Behind a NAT Device

In the second example, the Deep Edge is located behind a NAT device.

NAT-A:	Public IP 202.101.1.1, NAT translates 192.168.1.2 to 202.101.1.3
Appliance-A:	Internal IP 192.168.1.2, on interface eth0. Local networks are 172.16.1.0/24
NAT-B:	Public IP 202.101.2.1, NAT translates 202.101.2.3 to 192.168.2.2
Appliance-B:	Internal IP 192.168.2.2, on interface eth0. Local networks are 172.16.2.0/24



FIGURE 3-25. Deep Edge VPN behind a NAT device

TABLE 3-7. VPN Connection Configuration

LOCATION	CONFIGURATION
Appliance-A	Name: toB Enable: Yes Gateway type: Initiate Gateway: 202.101.2.3 Interface name: Eth0 Policy name: default Authentication type: Pre-shared key Key: ***** Local Networks: 172.16.1.0/24 Remote Networks: 172.16.2.0/24 VPN ID: 192.168.1.2
Appliance-B	Name: toA Enable: Yes Gateway type: Response Interface name: Eth0 Policy name: default Authentication type: Pre-shared key Key: ***** Local Networks: 172.16.1.0/24 Remote Networks: 172.16.2.0/24

Chapter 4

Policies, Objects, and Security

Deep Edge uses policies, policy objects, and security settings to provide a modern firewall capability that is easy to deploy and manage on day-to-day basis. Deep Edge stops costly events that lead to data loss or theft, infected endpoints, and other productivity-adverse incidents, such as scanners, bots, denial of service attacks, and other threats. Protection includes bi-directional stateful inspection, centralized, targeted policies with configurable objects, IPv4 and IPv6 support, user and groups support, logs and reports.

Topics include:

- *About Policies on page 4-2*
- *About Policy Objects on page 4-10*
- *About Security Settings on page 4-34*
- *About HTTPS Inspection on page 4-54*
- *About Bandwidth Control on page 4-60*
- *About Approved/Blocked URLs on page 4-67*
- *About Anti-DoS on page 4-69*
- *About Authentication on page 4-72*
- *About User Notifications on page 4-76*

About Policies

Policies control firewall operations by enforcing rules and automatically taking action. Configure security policies to block or allow a network session based on the application, the source and destination zones and addresses, source users, and, optionally, the service (port and protocol).

How Firewall Policies Work

Firewall policies control all traffic attempting to pass through the Deep Edge unit, between Deep Edge interfaces, zones, and VLAN subinterfaces.

Firewall policies are instructions the Deep Edge unit uses to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.

Firewall policies can contain many instructions for Deep Edge to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

Policy instructions may include protection profiles, which can specify application-layer inspection and other protocol-specific protection and logging.

Firewall policies integrate with the other Deep Edge functions to provide a centralized policy configuration and management architecture for:

- Antivirus, spyware, and email policies
- Network intrusion protection policies (see [Network Intrusion Protection on page 4-35](#))
- URL category objects (see [About URL Category Objects on page 4-17](#))

About Policy Rules

Security policies can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and because the first rule that matches the

traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic is blocked.

To create policy rules, first create some policy objects, which are used to define the parameters of the policy rules. For more information, see [About Policy Rules on page 4-2](#).

The **Policies** page at **Policies > Rules** allows users to:

- View the list of existing rules
- Add, copy, and delete rules
- Enable or disable rules

Adding Policy Rules

Policy rules determine whether to allow or block a network session based on specified traffic attributes. After creating a new rule, configure the rule by using the tabs to specify the appropriate information.

Procedure

1. Go to **Policies > Rules**.
2. Click **Add New**.
3. Optionally enable the rule.
4. Specify a policy name between 1 and 32 characters, consisting of letters, numbers, or underlines.
5. Type an optional **Description**.
6. Optionally select **Enable Internet access log**.



Important

To capture traffic logs, enable the Internet access log and filtering criteria at **Analysis & Reports > Log Settings**. For details, see [Log Settings on page 5-39](#).

7. Configure source address and user rules.

See [Configuring Sources and Users Policy Rules on page 4-4](#).

8. Configure destination address rules.

See [Configuring Destination Policy Rules on page 4-5](#).

9. Configure traffic type rules.

See [Configuring Traffic Type Policy Rules on page 4-7](#).

10. Configure schedule and bandwidth rules.

See [Configuring Schedule and Action Profile Policy Rules on page 4-8](#).

11. Click **OK**.
-

Configuring Sources and Users Policy Rules

Before you begin

Add a new policy at **Policies > Rules > Add New**. For details, see [Adding Policy Rules on page 4-3](#).

Use the **Sources and Users** tab to define rules enforced on traffic coming from the designated source IP addresses, source users and groups, and/or source zones.

Procedure

1. Click the **Sources and Users** tab.
2. Under **Source Addresses**, select one of the following parameters:
 - **Any**: Includes all source addresses. (Default)
 - **Selected addresses**: Displays a list of previously configured source addresses available or to add a new IP address.



Note

To add new address objects, see [Configuring Address Objects on page 3-11](#).

3. Select from the following under **Users and groups**

OPTION	DESCRIPTION
Anyone	Rule affects all known and unknown users.
Known users	Rule affects authenticated users via captive portal or identified users via transparent authentication. For details about user identification, see About Authentication on page 4-72 .
Unknown users	Rule affects users that transparent authentication cannot identify. For details about user identification, see About Authentication on page 4-72
Selected users	Rule affects specified users and groups (local user or LDAP). For details about user management, see End User Management on page 6-9 .

4. Select **Enable source zone rules** to enable using source zones.

- **Any:** Includes all source zones
- **Selected zones:** Provides the **Add New** zone option. For details about adding zones, see [Configuring Zone Objects on page 4-11](#)

What to do next

Continue to configure the following:

- To configure destination addresses, see [Configuring Destination Policy Rules on page 4-5](#)
- To configure traffic type, see [Configuring Traffic Type Policy Rules on page 4-7](#)
- To configure schedules and actions, see [Configuring Schedule and Action Profile Policy Rules on page 4-8](#)

Configuring Destination Policy Rules

Before you begin

- Add a new policy at **Policies > Rules > Add New**. For details, see [Adding Policy Rules on page 4-3](#).

- Optionally configure the sources and users as shown in [Configuring Sources and Users Policy Rules on page 4-4](#).

Use the **Destinations** tab to define rules for traffic ending at the specified destination IP addresses and destination zones.

Procedure

1. Click the **Destinations** tab.
2. Under **Destination Addresses**, select one of the following parameters:
 - **Any:** Includes all destination addresses
 - **Selected addresses:** Displays a selectable list of previously configured destination addresses to use. Use this option to add address objects, if needed.



Note

To add destination addresses, see [Configuring Address Objects on page 3-11](#)

3. Select the **Enable destination zone rules** check box to enable using destination zones.
 - **Any:** Includes all source zones
 - **Selected zones:** Provides the **Add New** zone option. For details about adding zones, see [Configuring Zone Objects on page 4-11](#)

What to do next

Continue to configure the following:

- To configure traffic type, see [Configuring Traffic Type Policy Rules on page 4-7](#)
- To configure schedules and actions, see [Configuring Schedule and Action Profile Policy Rules on page 4-8](#)

Configuring Traffic Type Policy Rules

Before you begin

- Add a new policy at **Policies > Rules > Add New**. For details, see [Adding Policy Rules on page 4-3](#).
- Optionally configure source addresses and users as shown in [Configuring Sources and Users Policy Rules on page 4-4](#)
- Optionally configure destination addresses as shown in [Configuring Destination Policy Rules on page 4-5](#).

Use the **Traffic Type** tab to define rules for traffic matching any specified applications, URL categories, or services.

Procedure

1. Click the **Traffic Type** tab.
2. Under **Applications and URL categories**, select one of the following parameters:
 - **Any:** Include all application groups and URL categories (Default)
 - **Selected:** Include only selected applications and URL categories



Note

For more information about adding new applications, URL category groups, or custom URL categories, see:

- [Adding a New Application Object on page 4-15](#)
 - [Adding a New URL Category Object on page 4-25](#)
 - [Adding a Custom URL Category on page 4-27](#)
-

3. Select **Enable service rules** to enforce rules on specific services.
 - **Any:** Include all services
 - **Selected:** Include only selected services

For details about adding service objects, see [Adding a Custom Service Object on page 4-13](#)

What to do next

Continue to configure schedules and actions, as shown in [Configuring Schedule and Action Profile Policy Rules on page 4-8](#).

Configuring Schedule and Action Profile Policy Rules

Before you begin

- Add a new policy at **Policies > Rules > Add New**. For details, see [Adding Policy Rules on page 4-3](#).
- Configure source addresses and users as shown in [Configuring Sources and Users Policy Rules on page 4-4](#)
- Configure destination addresses as shown in [Configuring Destination Policy Rules on page 4-5](#).
- Configure traffic type as shown in [Configuring Destination Policy Rules on page 4-5](#).

Use the **Schedule and Action Profile** tab to define a schedule and action for the rule when traffic matches the policy.

Procedure

1. Click the **Schedule and Actions Profile** tab.
2. Select one the following from the **Schedule** drop-down list:

OPTION	DESCRIPTION
Always	Includes all schedules. (Default)
Schedule name	Displays names of available schedule objects.
Add new	Access the Add/Edit schedule object creation dialog box.

**Note**

For more information about schedule objects, see [About Schedules and Schedule Objects on page 4-29](#).

3. Select the **Action** from the drop-down list.

**Note**

For information about action profiles, see [About Action Profiles on page 4-30](#).

4. Click **OK**.
-

Enabling/Disabling Policy Rules

Policies can be provisioned disabled. This procedure applies to policy rules already created but not enabled.

Procedure

1. Go to **Policies > Rules**.
 2. Click the name of the policy rule to enable or disable
 3. Do one of the following:
 - Select the check box to enable the policy
 - Deselect the check box to disable policy
 4. Click **OK**.
-

Validating Policy Rules

Validating policy rules highlights potentially conflicting rules across multiple policies. If a higher policy has a configuration that limits a lower policy, the high policy always takes precedence. Validate policy rules to check whether multiple policy rules conflict in how they control traffic. If a conflict exists, reconfigure policies to optimize network performance and security.

Procedure

1. Go to **Policies > Rules**.
2. Click **Validate Policies**.
3. Specify parameters to check.
4. Click **Validate**.

Any matching policy rules appear in the list. Modify matching policies to remove potentially conflicting rules.

About Policy Objects

Policy objects are the elements that enable you to construct, schedule, and search for policies. The following element types are supported:

TABLE 4-1. Policy Objects

OBJECT	DESCRIPTION
Address objects	Determine the scope of the policy. See About Addresses and Address Objects on page 3-9 .
Zone objects	Group interfaces and VLAN subinterfaces into zones to simplify policy creation. See About Zones and Zone Objects on page 4-11 .
Service objects	Limit the protocol (TCP or UDP) and port numbers. See About Services and Service Objects on page 4-13 .
Application objects	Specify how software applications are treated in policies. See About Applications and Application Objects on page 4-15 .
URL category objects	Restrict access to specific websites and website categories. See About URL Category Objects on page 4-17 .
Schedule objects	Specify when policies are active. See About Schedules and Schedule Objects on page 4-29 .

OBJECT	DESCRIPTION
Action profile objects	Control the action to take on traffic types identified by specific security policies. See About Action Profiles on page 4-30 .

About Addresses and Address Objects

Address objects affect both policy and network settings. Address objects determine allowed IP address ranges in the internal network. By default, Deep Edge includes all internal IP address ranges. To set security policies for specific source or destination addresses, first define the addresses and address ranges in your network settings.

Go to **Network > Addresses**.

About Zones and Zone Objects

Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation, allowing faster creation of policy and firewall rules. Configure policies for connections to and from a zone, but not between interfaces in a zone. Add zones, rename and edit zones, and delete zones from the zone list. When adding a zone, select the names of the interfaces and VLAN subinterfaces to add to the zone.

Zones are configured from physical network adapters.

Configuring Zone Objects

Adding zone objects allow for faster and simple policy creation. In order for a firewall interface to be able to process traffic, it must be assigned to a security zone. The zone name appears in the list of zones when defining security policies and configuring interfaces.

Procedure

1. Go to **Policies > Objects > Zones**.
2. Click **Add New**.
3. Specify the following parameters:

- **Object name**
 - **Description**
4. In **Interface**, click the **+** to add any applicable interface from the right pane.
 5. Click **OK**.
 6. Verify the new zone displays in the list at **Policies > Objects > Zones**.
-

Viewing Zones

Zone objects must be configured before they appear in the zone list.

Procedure

- Go to **Policies > Objects > Zones**.
-

Deleting Zone Objects

Zone objects assigned to a policy cannot be deleted.

Procedure

1. Go to **Policies > Objects > Zones**.
 2. Select the check box in the row of the object to delete.
 3. Click the **Delete** icon ()
 4. Click **Delete** in the confirmation dialog box.
-

The object is removed.

About Services and Service Objects

When defining security policies for specific applications, select one or more services to limit the port numbers the application(s) can use. The default service is any, which allows all TCP and UDP ports.

Deep Edge offers over 100 predefined services (DNS, FTP, HTTP, POP3, SMTP, SSL, and TELNET). Custom service definitions can also be added, if necessary.

The following functions are available:

- [Adding a Custom Service Object on page 4-13](#)
- [Viewing Custom Service Objects on page 4-14](#)
- [Deleting Custom Service Objects on page 4-14](#)

Service Object Parameters

Use the parameters in the table below to define services.

TABLE 4-2. Service Object Parameters

PARAMETER	DESCRIPTION
Service object name	This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Protocol	Select any protocol used by the service or create a custom service.
Destination ports	For custom services, specify the port number (0 to 65535) or range of port numbers (port1-port2) used by the service. Multiple ports or ranges must be separated by commas.

Adding a Custom Service Object

Procedure

1. Go to **Policies > Objects > Services > Customized Services**.

2. Click **Add New**.
3. Specify the following information:
 - **Object name**
 - **Protocol**
 - **Destination ports**
 - **Description**



Note

The destination port can be a single port (22), multiple single ports (22, 23), as a range of ports (22-80), or any combination of those options. Up to 15 port segments are allowed.

4. Click **OK**.
 5. Verify the new service object is listed at **Policies > Objects > Services > Customized Services**.
-

Viewing Custom Service Objects

Procedure

- Go to **Policies > Objects > Services > Customized Services**.
-

Deleting Custom Service Objects

Procedure

1. Go to **Policies > Objects > Services > Customized Services**.
2. Select the check box in the row of the object to delete.

3. Click the **Delete** icon (.
4. Click **Delete** in the confirmation dialog box.

The object is removed.

About Applications and Application Objects

Internet-based applications have grown in popularity over the last few years beyond using the browser to surf websites. Even with corporate usage policies, many companies are unable to curb and regulate the use of those applications. Recent findings show that 75% to 80% of corporate users ignore their company's endpoint usage policies. To avoid significant risk, Deep Edge Application Control automatically discovers popular Internet applications and allows you to set policies that limit application access.

Deep Edge provides both visibility and control for almost 1000 application types running across any port, including applications using custom clients (Skype, BitTorrent, P2P) or leveraging Web 2.0 technologies within the browser (social networking, web mail, and streaming media sites). You have the flexibility to control applications or to allow the application but granularly control the activities within the application, such as uploading files, watching video, or playing specific games.

Adding a New Application Object

Add a new application group to consolidate multiple applications from different application categories into a single group. Add specific applications into that group to apply policies to all added applications. For example, group a set of prohibited applications that includes iTunes™, MSN Messenger®, Netflix™, and Facebook™. By default, these application reside in different application categories.

To avoid creating multiple policies blocking a specific application, group applications to allow one policy to block them.

Procedure

1. Go to **Policies > Objects > Applications**.
2. Click **Add New**.

3. Specify a name and description for the new application object.
4. Expand the appropriate application category to include in the application group.
5. Select the check box for any application within the application category to include in the application group.
6. Click **OK**.

The new application object is added to the list.

Viewing/Editing Application Objects

Procedure

1. Go to **Policies > Objects > Applications**.
 2. Click the name of the appropriate application object.
 3. Review the application object and/or modify the selection.
 4. Click **OK**.
-

Deleting Application Objects

Procedure

1. Go to **Policies > Objects > Applications**.
 2. Select the check box in the row of the object to delete.
 3. Click the **Delete** icon (.
 4. Click **Delete** in the confirmation dialog box.
-

The object is removed.

About URL Category Objects

URL filtering profiles restrict access to specific websites and website categories. Each security policy can specify a URL filtering profile that blocks access to specific websites and website categories or generates an alert when the specified websites are accessed. The web categories are predefined by Trend Micro.

The URL filtering module provides procedures for creating and configuring profiles used in URL filtering policies. URL filtering, along with Web Reputation, is part of the multi-layered, multi-threat protection solution provided by Deep Edge.

With the URL Filtering feature in Deep Edge, set policies based on the URL categories (examples: Adult, Gambling, Financial Services). When a user requests a URL, Deep Edge first looks up the category for that URL and then allows or denies access to the URL based on the configured policies. You can also define a list of approved URLs that will not be filtered.

URL Filtering Category Groups

The following table shows the URL Filtering groups and categories.

TABLE 4-3. Grouping Definitions for URL Categories

CATEGORY GROUP	DESCRIPTION
Adult	Websites generally considered inappropriate for children
Business	Websites related to business, employment, or commerce
Communications and Search	Websites that provide tools and services for online communications and searches.
General	Websites that do not fall into or have not been classified into the other categories.
Internet Security	Potentially harmful websites, including those known to distribute malicious software
Lifestyle	Websites about religious, political, or sexual preferences, as well as recreation and entertainment

CATEGORY GROUP	DESCRIPTION
Network Bandwidth	Websites offering services that can significantly impact the speed of the endpoint's Internet connection

URL Filtering Categories

The table below lists definitions of the URL filtering categories and groupings.

TABLE 4-4. URL Filtering Categories Definitions

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Adult	Abortion	Sites that promote, encourage, or discuss abortion, including sites that cover moral or political views on abortion
Adult	Adult/Mature Content	Sites with profane or vulgar content generally considered inappropriate for minors; includes sites that offer erotic content or ads for sexual services, but excludes sites with sexually explicit images
Adult	Alcohol/Tobacco	Sites that promote, sell, or provide information about alcohol or tobacco products
Adult	Gambling	Sites that promote or provide information on gambling, including online gambling sites
Adult	Illegal Drugs	Sites that promote, glamorize, supply, sell, or explain how to use illicit or illegal intoxicants
Adult	Illegal/Questionable	Sites that promote and discuss how to perpetrate nonviolent crimes, including burglary, fraud, intellectual property theft, and plagiarism; includes sites that sell plagiarized or stolen materials

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Adult	Intimate Apparel/ Swimsuit	Sites that sell swimsuits or intimate apparel with models wearing them
Adult	Marijuana	Sites that discuss the cultivation, use, or preparation of marijuana, or sell related paraphernalia
Adult	Nudity	Sites showing nude or partially nude images that are generally considered artistic, not vulgar or pornographic
Adult	Pornography	Sites with sexually explicit imagery designed for sexual arousal, including sites that offer sexual services
Adult	Sex Education	Sites with or without explicit images that discuss reproduction, sexuality, birth control, sexually transmitted disease, safe sex, or coping with sexual trauma
Adult	Tasteless	Sites with content that is gratuitously offensive and shocking; includes sites that show extreme forms of body modification or mutilation and animal cruelty
Adult	Violence/Hate/Racism	Sites that promote hate and violence; includes sites that espouse prejudice against a social group, extremely violent and dangerous activities, mutilation and gore, or the creation of destructive devices
Adult	Weapons	Sites about weapons, including their accessories and use; excludes sites about military institutions or sites that discuss weapons as sporting or recreational equipment
Business	Auctions	Sites that serve as venues for selling or buying goods through bidding, including business sites that are being auctioned

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Business	Brokerage/Trading	Sites about investments in stocks or bonds, including online trading sites; includes sites about vehicle insurance
Business	Business/Economy	Sites about business and the economy, including entrepreneurship and marketing; includes corporate sites that do not fall under other categories
Business	Financial Services	Sites that provide information about or offer basic financial services, including sites owned by businesses in the financial industry
Business	Job Search/Careers	Sites about finding employment or employment services
Business	Real Estate	Sites about real estate, including those that provide assistance selling, leasing, purchasing, or renting property
Business	Shopping	Sites that sell goods or support the sales of goods that do not fall under other categories; excludes online auction or bidding sites
Communications and Search	Blogs/Web Communications	Blog sites or forums on varying topics or topics not covered by other categories; sites that offer multiple types of web-based communication, such as e-mail or instant messaging
Communications and Search	Chat/Instant Messaging	Sites that provide web-based services or downloadable software for text-based instant messaging or chat
Communications and Search	Email	Sites that provide email services, including portals used by companies for web-based email

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Communications and Search	Internet Infrastructure	Content servers, image servers, or sites used to gather, process, and present data and data analysis, including web-based analytic tools and network monitors
Communications and Search	Internet Telephony	Sites that provide web services or downloadable software for Voice over Internet Protocol (VoIP) calls
Communications and Search	Newsgroups	Sites that offer access to Usenet or provide other newsgroup, forum, or bulletin board services
Communications and Search	Search Engines/Portals	Search engine sites or portals that provide directories, indexes, or other retrieval systems for the web
Communications and Search	Social Networking	Sites devoted to personal expression or communication, linking people with similar interests
Communications and Search	Web Hosting	Sites of organizations that provide top-level domains or web hosting services
General	Computers/Internet	Sites about endpoints, the Internet, or related technology, including sites that sell or provide reviews of electronic devices
General	Education	School sites, distance learning sites, and other education-related sites
General	Government/Legal	Sites about the government, including laws or policies; excludes government military or health sites
General	Health	Sites about health, fitness, or well-being
General	Military	Sites about military institutions or armed forces; excludes sites that discuss or sell weapons or military equipment

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
General	News/Media	Sites about the news, current events, contemporary issues, or the weather; includes online magazines whose topics do not fall under other categories
General	Politics	Sites that discuss or are sponsored by political parties, interest groups, or similar organizations involved in public policy issues; includes non-hate sites that discuss conspiracy theories or alternative views on government
General	Reference	General and specialized reference sites, including map, encyclopedia, dictionary, weather, how-to, and conversion sites
General	Translators/Cached Pages	Online page translators or cached Web pages (used by search engines), which can be used to circumvent proxy servers and Web filtering systems
General	Untested	Sites that have not been classified under a category
General	Vehicles	Sites about motorized transport, including customization, procurement of parts and actual vehicles, or repair services; excludes sites about military vehicles
Internet Security	Made for AdSense sites (MFA)	Sites that use scraped or copied content to pollute search engines with redundant and generally unwanted results
Internet Security	Potentially Malicious Software	Sites that contain potentially harmful downloads
Internet Security	Proxy Avoidance	Sites about bypassing proxy servers or web filtering systems, including sites that provide tools for that purpose

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Internet Security	Web Advertisement	Sites dedicated to displaying advertisements, including sites used to display banner or pop-up ads
Lifestyle	Activist Groups	Sites that promote change in public policy, public opinion, social practice, economic activities, or economic relationships; includes sites controlled by service, philanthropic, professional, or labor organizations
Lifestyle	Alternative Journals	Online equivalents of supermarket tabloids and other fringe publications
Lifestyle	Arts	Sites about visual arts, such as painting and sculpture.
Lifestyle	Cult/Occult	Sites about alternative religions, beliefs, and religious practices, including those considered cult or occult
Lifestyle	Cultural Institutions	Sites controlled by organizations that seek to preserve cultural heritage, such as libraries or museums; also covers sites owned by the Boy Scouts, the Girl Scouts, Rotary International, and similar organizations
Lifestyle	Entertainment	Sites that promote or provide information about movies, music, non-news radio and television, books, humor, or magazines
Lifestyle	For Kids	Sites designed for children
Lifestyle	Games	Sites about board games, card games, console games, or endpoint games; includes sites that sell games or related merchandise
Lifestyle	Gay/Lesbian	Sites about gay, lesbian, transgender, or bisexual lifestyles

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Lifestyle	Gun Clubs/Hunting	Sites about gun clubs or similar groups; includes sites about hunting, war gaming, or paintball facilities
Lifestyle	Humor	Sites intended for humor.
Lifestyle	Personal Sites	Sites maintained by individuals about themselves or their interests; excludes personal pages in social networking sites, blog sites, or similar services
Lifestyle	Personals/Dating	Sites that help visitors establish relationships, including sites that provide singles listings, matchmaking, or dating services
Lifestyle	Recreation/Hobbies	Sites about recreational activities and hobbies, such as collecting, gardening, outdoor activities, traditional (non-video) games, and crafts; includes sites about pets, recreational facilities, or recreational organizations
Lifestyle	Religion	Sites about popular religions, their practices, or their places of worship
Lifestyle	Restaurants/Food	Sites that list, review, discuss, advertise, or promote food, catering, dining services, cooking, or recipes
Lifestyle	Society/Lifestyle	Sites that provide information about life or daily matters; excludes sites about entertainment, hobbies, sex, or sports, but includes sites about cosmetics or fashion
Lifestyle	Sports	Sites about sports or other competitive physical activities; includes fan sites or sites that sell sports merchandise
Lifestyle	Travel	Sites about traveling or travel destinations; includes travel booking and planning sites

CATEGORY GROUP	CATEGORY TYPE	CATEGORY DEFINITION
Network Bandwidth	Internet Radio and TV	Sites that primarily provide streaming radio or TV programming; excludes sites that provide other kinds of streaming content
Network Bandwidth	Pay to Surf	Sites that compensate users who view certain websites, email messages, or advertisements or users who click links or respond to surveys
Network Bandwidth	Peer-to-Peer	Sites that provide information about or software for sharing and transferring files within a peer-to-peer (P2P) network
Network Bandwidth	Personal Network Storage/File Download Servers	Sites that provide personal online storage, backup, or hosting space, including those that provide encryption or other security services
Network Bandwidth	Photo Searches	Sites that primarily host images, allowing users to share, organize, store, or search for photos or other images
Network Bandwidth	Ringtones/Mobile Phone Downloads	Sites that provide content for mobile devices, including ringtones, games, or videos
Network Bandwidth	Software Downloads	Sites dedicated to providing free, trial, or paid software downloads
Network Bandwidth	Streaming Media/MP3	Sites that offer streaming video or audio content without radio or TV programming; sites that provide music or video downloads, such as MP3 or AVI files

Adding a New URL Category Object

Procedure

1. Go to **Policies > Objects > URL Categories**.

2. Click **Add New**.

The **Add/Edit URL Category Group** screen appears.

3. Specify a name and optional description for the new URL category group.
4. Expand the appropriate category to include.
5. Select applicable check boxes for the content to include.

Add/Edit URL Category Group

Name:

Description:

Selected URL Categories: 1

Name	
	Network Bandwidth(All , None)
	Internet Security(All , None)
	Communications and Search(All , None)
	Adult(All , None)
☐	Abortion
☐	Adult/Mature Content
☐	Alcohol/Tobacco
☒	Gambling
☐	Illegal Drugs
☐	Illegal/Questionable
☐	Intimate Apparel/Swimsuit
☐	Marijuana
☐	Nudity

OK Cancel

FIGURE 4-1. URL category group restricting gambling websites

6. Click **OK**.

The new URL category group is added to the list.

Modifying URL Filtering Category Objects

Procedure

1. Go to **Policies > Objects > URL Categories**.
 2. Click the name of the URL category object to modify.
 3. Make the changes in the **Edit URL Category Group** dialog box.
 4. Click **OK**.
-

Deleting URL Category Objects

Procedure

1. Go to **Policies > Objects > URL Categories**.
 2. Select the check box in the row of the object to delete.
 3. Click the **Delete** icon ()
 4. Click **Delete** in the confirmation dialog box.
-

The object is removed.

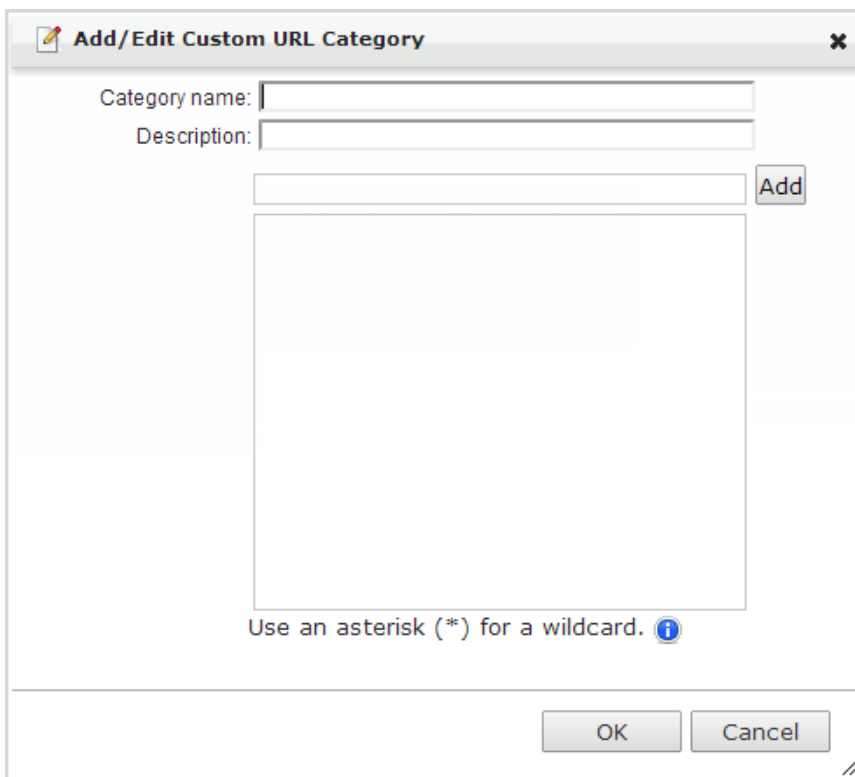
Adding a Custom URL Category

Procedure

1. Go to **Policies > Objects > URL Categories**.
2. Open the **Custom URL Categories** tab.

3. Click **Add New**.

The **Add/Edit Custom URL Category** screen appears.



The screenshot shows a dialog box titled "Add/Edit Custom URL Category" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields: "Category name:" and "Description:". Below the "Description:" field is a large text area. To the right of the text area is an "Add" button. At the bottom of the dialog, there is a note: "Use an asterisk (*) for a wildcard." followed by an information icon (i). At the very bottom of the dialog are "OK" and "Cancel" buttons.

4. Specify the custom URL category name.
5. Specify the URL category description.
6. Specify a URL, and then click **Add**.

**Note**

Insert a wildcard (*) at the beginning or end of a URL to match zero or more characters. Examples: *.example.com, www.example.com/*.

7. Click **OK**.
-

About Schedules and Schedule Objects

By default, each security policy applies to all dates and times. To limit a security policy to specific times, define schedules, and then apply them to the appropriate policies. A schedule object may contain multiple fixed dates and time ranges.

To apply schedules to security policies, refer to [About Security Settings on page 4-34](#).

Adding a Schedule Object

Procedure

1. Go to **Policies > Objects > Schedules**.
 2. Click **Add New**.
The **Add/Edit Schedule Object** screen appears.
 3. Specify a **Name**.
 4. Specify a **Description**.
 5. Click and drag to select the applicable time period.
 6. Click **OK**.
 7. Verify the new schedule object has been added to the list at **Policies > Objects > Schedules**.
-

Editing Schedule Objects

Procedure

1. Go to **Policies > Objects > Schedules**.

2. Click the name of the schedule object to be changed.
 3. Change as needed in the **Add/Edit Schedule Object** dialog box.
 4. Click **OK**.
-

Deleting Schedule Objects

Procedure

1. Go to **Policies > Objects > Schedules**.
 2. Select the check box in the row of the object to delete.
 3. Click the **Delete** icon ()
 4. Click **Delete** in the confirmation dialog box.
-

The object is removed.

About Action Profiles

Action profiles contain the details of the action to be taken on traffic types identified by specific security policies. By default, each security policy allows an action to be taken. To specify the actions for a security policy, use the default action profiles provided for specific traffic, or define the action profiles for specific traffic, and then apply them to the appropriate policies.

To view action profiles, go to **Policies > Objects > Action Profiles**.

Predefined Action Profiles

To view predefined action profiles, go to **Policies > Objects > Action Profiles > Predefined Profiles**.

Deep Edge default action profiles include:

TABLE 4-5. Predefined Action Profiles

ACTION	DESCRIPTION
Deep Scan	The Deep Scan predefined action profile does the following: - Scans traffic for malicious content, blocking viruses, Trojans, worms, and botnets - Enables Web Reputation scanning, blocking sites with low reputation scores - Enables intrusion prevention, blocking malicious behavior
General Scan	The General Scan predefined action profile does the following: - Scans traffic for malicious content, blocking viruses, Trojans, worms, and botnets - Enables Web Reputation scanning, blocking sites with low reputation scores - Enables intrusion prevention, logging malicious behavior
Malware Scan	The Malware Scan predefined action profile does the following: - Scans traffic for malicious content, logging any virus, Trojan, worm, or botnet activity - Enables Web Reputation scanning, blocking sites with low reputation scores - Enables intrusion prevention scanning, logging malicious behavior
Scan for Log	The Scan for Log predefined action profile does the following: - Scans traffic for malicious content, logging any virus, Trojan, worm, or botnet activity - Enables Web Reputation scanning, logging sites accessed with low reputation scores - Enables intrusion prevention scanning, logging malicious behavior

ACTION	DESCRIPTION
Message Scan	The Message Scan predefined action profile does the following: • Enables anti-malware scanning, blocking email messages that contain malicious content • Enables anti-spam scanning, tagging email message containing spam To configure the message tag settings, go to Policies > Security Settings > Anti-Spam and specify Other Settings. For details, see Configuring Anti-Spam Settings on page 4-49.

Viewing Predefined Action Profiles

Procedure

1. Go to **Policies > Objects > Action Profiles > Predefined Profiles**.
2. Click the name of the security function (**IPS**, **Anti-malware**, **Anti-spam**, or **WRS**) to see the settings.



Note

Predefined profiles cannot be modified.

3. Cancel the displayed settings to view additional setting for other security functions.
-

Adding an Action Profile Object

Add an action object if the organization needs to treat actions taken on specific traffic differently than the default actions provided.

Procedure

1. Go to **Policies > Objects > Action Profiles > Customized Profiles**.
2. Click **Add New**.

3. Specify a name and (optional) description.
 4. Select the check box of the security function to be configured: IPS, Anti-malware, Anti-spam, and/or WRS.
 5. Set the action as needed from the corresponding drop-down list box:
 - For **IPS**, **WRS**, or **Anti-malware**, select:
 - **Block**: To block the traffic
 - **Monitor**: To allow the traffic to pass, but record it in the violation logs
 - For **Anti-spam**, select:
 - **Tag**: Allows the email message to be delivered with a tag in the subject line, such as [Spam]
 - **Quarantine**: Do not allow the email message to be delivered, but instead have it saved in a secure location.
 - **Block**: Do not allow the email content to be delivered.
 - **Monitor**: Allow the email message to be delivered and logged in a violation log.
 6. Click **OK**.
-

Editing Action Profile Objects

Existing action profiles can be edited to fit enterprise needs. Predefined action profiles cannot be modified.

Procedure

1. Go to **Policies > Objects > Action Profiles > Customized Profiles**.
2. Click the name of the action profile to be changed.
3. Change the name, description, or action settings as needed.

4. Click **OK**.
-

Deleting Action Profile Objects

Existing action profiles can be deleted, if necessary. Predefined action profiles cannot be deleted.

Procedure

1. Go to **Policies > Objects > Action Profiles > Customized Profiles**.
 2. Select the check box in the row of the object to delete.
 3. Click the **Delete** icon ()
 4. Click **Delete** in the confirmation dialog box.
-

The object is removed.

About Security Settings

Choose from the following actions when defining security profiles:

Intrusion Prevention System (IPS)

Integrates a high-performance Deep Packet Inspection architecture and a dynamically updated signature database to deliver complete network protection from application exploits, worms, and malicious traffic. For details, see [IPS Security on page 4-36](#).

Anti-Malware

Default Global global Anti-Malware security profile. Used by all policies to provide malware protection and against other threats to your networks. It includes virus, spyware, Trojan, worm, and botnet. Once the Global Anti-Malware security profile is enabled, network connection scans are carried out to ensure content is malware free. For details, see [Anti-Malware Security on page 4-38](#).

Anti-Spam

Anti-Spam uses Email Reputation, which is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge. For details, see [Anti-Spam Security on page 4-47](#).

Web Reputation Services (WRS)

Web Reputation Services (WRS) scrutinizes URLs before users access potentially dangerous websites, especially sites known to be phishing or pharming sites. By utilizing WRS, the appliance provides real-time protection, conserves system scanning resources, and saves network bandwidth by preventing the infection chain or breaking it early. For details, see [WRS Profiles on page 4-53](#).

Network Intrusion Protection

Network Intrusion Prevention capabilities are part of the Deep Edge base functionality. An Intrusion Prevention System (IPS) identifies and stops many threats, exploits, back-door programs, and other attacks as they pass through the device. An IPS can bolster a firewalls security policy by ensuring that traffic allowed by the firewall rule policy is further inspected to make sure it does not contain unwanted threats.

Patterns used to detect threats are released before official updates or patches become available—protecting businesses during this crucial period. Deep Edge IPS is a deep-packet-inspection system which peers inside the traffic packets and removes certain packets which contain undesired contents that are compared against a deployable rules list of several hundred patterns. This signature list of patterns is live-updated every few minutes and constantly adapts and evolves to keep you protected from threats as soon as they emerge or spread.

IPS provides support for the common attack types such as:

- DoS/DDoS attacks
- Protocol attacks
- OS attacks

- Application attacks
- Malformed traffic/Invalid header attacks
- Malware and blended attacks
- TCP Segmentation and IP Fragmentation attacks
- Port Scans

The IPS solution has pre-defined policy templates for common applications and protocols to make the IPS function easy to use. Trend Micro provides pre-defined rules but also allows you to create custom IPS rules.

IPS Security

Each security policy can specify an intrusion protection profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default profile protects clients and servers from all known critical-, high-, and medium-severity threats.

Intrusion prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.

Use customized profiles to minimize vulnerability checking for traffic between trusted security zones and to maximize protection for traffic received from untrusted zones (Internet) as well as the traffic sent to highly sensitive destinations (server farms).

In Deep Edge, you can define the filtering rule criteria and then select which IPS rules apply to traffic.

Categories for block or monitor actions:

- **Miscellaneous**—SIP Foundry sipiXtapi Buffer Overflow
- **File transfer server**—NetTerm NetFTPF User Buffer Command or 3Com 3CDaemon FTP server overflow
- **Web server**—Microsoft Windows Explorer Drag and Drop Remote Code Execution, Microsoft IIS WebDAV Long Request Buffer Overflow, and others

- **General server**—Microsoft SSL PCT Buffer Overflow Vulnerability, Solaris Telnetd User Authentication Bypass Vulnerability, and others
- **Client**—Microsoft Visual Studio WMI Object Broker Unspecified Code Execution, Microsoft Internet Explorer XMLHTTP ActiveX Control setRequestHeader Code Execution, and others
- **IM**—IBM Lotus Sametime Multiplexer Buffer Overflow, MSN MSNP2P Message Integer Overflow, and others
- **Message server**—Sendmail Signal Race Vulnerability, Microsoft Exchange SMTP Service Extended Verb Request Buffer Overflow, and others

Modifying IPS Rules

Procedure

1. Go to **Policies > Security Settings > IPS**.
2. Select the **Enable IPS security** check box.
3. Under **IPS Filtering Criteria**, select the minimum IPS severity level to filter. All traffic that has an equal to or greater selected severity level are filtered.

OPTION	DESCRIPTION
1—Information	Port-based traffic (examples: HTTP, SMTP).
2—Low	Policy-related signatures (examples: IM, P2P, Games)
3—Medium	Tunneling and scanning activity.
4—High	Most intrusion-related signatures.
5—Critical	Same as high severity plus very high impact to servers and end users (examples: CVE-2008-4250, Conficker).

4. Select the date that the threat was released.
5. Select affected operating systems.
6. Select the IPS categories.

7. Click **Apply Filter** to set the filtering criteria.

All predefined IPS filtering rules matching the specified criteria populate in the table under **Filtering Rules**.

8. Under **IPS Rules**, all matching criteria are automatically selected. To remove an IPS rule, deselect the check box next to the rule ID.

9. Click **OK**.

The changes are saved.

Anti-Malware Security

Anti-malware profiles protect against emerging security threats. You can enable or disable logging for this profile, but the profile cannot be deleted. This profile can be used by all policies to provide protection from malware and to stop other threats to your networks. Once the Global Anti-Malware security profile is enabled in a policy, network-connection scans ensure content is malware free.

Each security policy can specify whether or not to use the global anti-malware profile. That identifies which applications are inspected for malware and the action taken when malware is detected. The default profile inspects all of the listed protocol decoders for malware and takes the action determined by the policy (block or monitor), depending on the type of malware detected.

Anti-Malware Scan Hierarchy

Configure anti-malware security to provide varying levels of security. Enabling the Advanced Threat Scan Engine in conjunction with Deep Discovery Advisor assists in discovering and preventing targeted attacks by suspected malware threats.

The following table provides an overview of the anti-malware scan engine hierarchy in Deep Edge.

TABLE 4-6. Scan Engine Hierarchy

SCAN ENGINE	DESCRIPTION
Virus Scan Engine scanning	The Virus Scan Engine provides pattern-based and heuristic scanning for traditional malware threats.
ATSE scanning	ATSE enhances the traditional malware threat protection offered by the Virus Scan Engine. ATSE performs an aggressive scan using heuristic algorithms to identify possible targeted attacks, such as document exploits. For scan configurations that enable ATSE without sending files to Deep Discovery Advisor, Deep Edge performs the action configured for Advanced threat files detected as an advanced threat by ATSE.  Note Some detected files may be safe. Perform an evaluation on files not sent to Deep Discovery Advisor to determine the actual threat of the quarantined files.
ATSE and Deep Discovery Advisor	After ATSE detects a suspected malware threat, Deep Edge sends the file to Deep Discovery Advisor for further analysis. Deep Discovery Advisor Virtual Analyzer assesses the risk level of the file in an isolated virtual environment and returns the threat rating to the Deep Edge server. Deep Edge performs the anti-malware policy action based on the configured security for the suspected threats without waiting for the analysis results. Deep Edge regularly synchronizes malicious IP addresses with Deep Discovery Advisor to match and record IP addresses as C&C contact alerts.

About Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
- Enhanced parsers for handling file deformities

**Important**

Because ATSE identifies both known and unknown advanced threats, enabling ATSE may increase the possibility of legitimate files being flagged as malicious.

Understanding Advanced Threats

Advanced threats use less conventional means to attack or infect a system. Heuristic scanning can detect advanced threats to mitigate damage to company systems. Enabling ATSE adds another layer of protection to systems against threats that are typically used in targeted attacks.

Some types of advanced threats that ATSE detects include:

- **Exploits:** Exploits are pieces of code purposely created by attackers to take advantage of software vulnerabilities. Such code is typically incorporated into malware.
- **Targeted attacks:** Targeted attacks refer to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. These attacks seek to maintain a persistent presence within the target's network so that the attackers can move laterally and extract sensitive information.
- **Zero-day threats:** Zero-day threats exploit previously unknown vulnerabilities in software.

**Tip**

Trend Micro recommends enabling ATSE.

Advanced Threat Scan Engine Security Levels

The following table explains the security levels and the corresponding risk levels that trigger the anti-malware security action profile.



Tip

Trend Micro recommends setting the security level to **Low**. This is the default setting.

SECURITY LEVEL	DESCRIPTION	RISK LEVEL
High	Apply action on all files exhibiting any suspicious behavior	• High risk • Medium risk • Low risk
Medium	Apply action on files with a moderate to high probability of being malicious	• High risk • Medium risk
Low	Apply action only on files with a high probability of being malicious	• High risk

Enabling Advanced Threat Scan Engine

Procedure

1. Go to **Policies > Security Settings > Anti-Malware**.
2. Select **Enable anti-malware security**.
3. Select **Enable Advanced Threat Scan Engine**.
4. Click **OK**.
5. To implement the new security settings, click **Apply** in the banner message that appears.

About Deep Discovery Advisor

Trend Micro™ Deep Discovery Advisor is designed to be the next generation in Trend Micro's security visibility and central management products. Deep Discovery Advisor is designed to:

- Collect, aggregate, manage, and analyze logs into a centralized storage space
- Provide advanced visualization and investigation tools that monitor, explore, and diagnose security events within the corporate network

Deep Discovery Advisor provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines.



Note

Deep Discovery Advisor is a separately licensed product. Deep Edge integrates with the Virtual Analyzer in Deep Discovery Advisor.

For more information about Deep Discovery Advisor, view the documentation at:

<http://docs.trendmicro.com/en-us/enterprise/deep-discovery-advisor.aspx>

Sending Samples to Deep Discovery Advisor

Advanced Threat Scan Engine (ATSE) performs the aggressive scanning necessary to detect advanced threats, such as document exploits and other threats used in targeted attacks. Deep Edge leverages ATSE to determine which samples to send to Deep Discovery Advisor. Enable ATSE before configuring Deep Discovery Advisor settings.

Procedure

1. Go to **Policies > Security Settings > Anti-Malware**.
2. Select **Enable anti-malware security**.
3. Select **Enable Advanced Threat Scan Engine**.
4. Configure the ATSE **Security Level** settings.

For details, see [Advanced Threat Scan Engine Security Levels on page 4-41](#).

5. Select **Send files to Deep Discovery Advisor for analysis**.
6. Specify the Deep Discovery Advisor registration settings.

**Note**

Contact the Deep Discovery Advisor administrator to obtain the server IP address, port number, and a valid API key .

- **IP address**
 - **Port**
 - **API key**
7. Click one of the following buttons:
 - **Register:** Establishes the connection to Deep Discovery Advisor
 - **Test Connection:** Verifies the connection settings to Deep Discovery Advisor but does not register Deep Edge to the server
 8. Click **OK**.
 9. To implement the new security settings, click **Apply** in the banner message that appears.
-

About Deep Discovery Inspector

Deep Discovery Inspector is a third-generation threat management solution, designed and architected by Trend Micro to deliver breakthrough advanced persistent threat (APT) and targeted attack visibility, insight, and control.

Trend Micro Deep Discovery Inspector is the result of thorough investigations of targeted attacks around the world, interviews with major customers, and the participation of a special product advisory board made up of leading G1000 organizations and government agencies.

Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports.

Deep Discovery Inspector deploys in offline monitoring mode. It monitors network traffic by connecting to the mirror port on a switch for minimal or no network interruption.

For more information about Deep Discovery Inspector, view the documentation at:

<http://docs.trendmicro.com/en-us/enterprise/deep-discovery-inspector.aspx>

APT Attack Sequence

Targeted attacks and advanced persistent threats (APTs) are organized, focused efforts that are custom-created to penetrate enterprises and government agencies for access to internal systems, data, and other valuable assets. Each attack is customized to its target, but follows a consistent lifecycle to infiltrate and operate inside an organization.

In targeted attacks, the APT lifecycle follows a continuous process of six key phases.

TABLE 4-7. APT Attack Sequence

PHASE	DESCRIPTION
Intelligence Gathering	Attackers identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack.
Point of Entry	The initial compromise is typically from zero-day malware delivered via social engineering (email, IM, or drive-by download). A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.
Command & Control (C&C) Communication	C&C communication is typically used throughout the attack, allowing the attacker to instruct and control the malware used, and to exploit compromised machines, move laterally within the network, and exfiltrate data.
Lateral Movement	Once inside the network, an attacker compromises additional machines to harvest credentials, escalate privilege levels, and maintain persistent control.
Asset/Data Discovery	Several techniques (such as port scanning) are used to identify the noteworthy servers and the services that house the data of interest.

PHASE	DESCRIPTION
Data Exfiltration	Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.

Trend Micro Deep Discovery Inspector is purpose-built for detecting APT and targeted attacks. It identifies malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

Integrating Deep Discovery Inspector Deny Lists

Deep Discovery Inspector enables administrators to select, create, configure, import, and export IP addresses, URLs, and domains as lists of denied or allowed objects. Deep Discovery Inspector can also add IP addresses, URLs, and domains from Virtual Analyzer feedback or from behavior or pattern matching scans. Deep Edge uses the Deep Discovery Inspector deny lists to block connections from denied IP addresses, URLs, and domains.

Procedure

1. Configure Deep Discovery Inspector to add the Deep Edge appliance IP address as an authorized Web Services host.



Important

Integrating with Deep Discovery Inspector deny list requires configurations to Deep Discovery Inspector. Contact Trend Micro Support for assistance in configuring Deep Discovery Inspector authorized Web Services hosts.

Go to <http://esupport.trendmicro.com/en-us/business/pages/about-support.aspx>

2. Log on to the Deep Edge web console.
3. Go to **Policies > Security Settings > Anti-Malware**.
4. Select **Enable anti-malware security**.
5. Select **Integrate Deep Discovery Inspector deny lists**.

6. Specify the Deep Discovery Inspector appliance IP address.
 7. Optionally test the connection to verify the Deep Discovery Inspector appliance IP address.
 8. Click **OK**.
 9. To implement the new security settings, click **Apply** in the banner message that appears.
-

About File Extension Verification

Most antivirus solutions today offer two options to determine which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file extensions considered the most vulnerable to infection are scanned.

Selecting File Extensions/Types to Scan

Deep Edge can scan all files that pass through it, or just a subset of those files as determined by the file extension.

Procedure

1. Go to **Policies > Security Settings > Anti-Malware**.
2. In the approved list, blocked list or scan list, specify file extensions in the following format `exe;rar;mp3`. Separate the file extensions with a semi-colon (;).
 - **Approved file extensions**—These file types are allowed without scanning.
 - **Blocked file extension**—These files are blocked without scanning.
 - **Scan list**—These file types are scanned before they are passed on by the Deep Edge server.
3. If needed, under **Scan Optimization**, specify the size of the file to skip when scanning.
4. If needed, select the HTTP MIME types to skip when scanning.

5. If needed, configure the tag to be placed in the email message subject line when and action has been taken on that message. The default is **[Virus Cleaned]**.
 6. Click **OK** to save settings.
 7. Select the **Enable anti-malware security** check box.
-

Anti-Spam Security

This section describes how to configure Deep Edge anti-spam filtering profile for SMTP email. Deep Edge manages unsolicited commercial email by detecting and identifying spam messages from known or suspected spam servers.

About Spam Detection

Deep Edge uses Email Reputation Services (ERS) integration to detect spam email. Trend Micro also offers a separate Software-as-a-Service (SaaS) security component called Hosted Email Security for content-based, spam filtering as well as data leakage filtering and email encryption features.

Email Reputation Technology

Deep Edge uses Email Reputation (ER) technology to maximize protection. ER technology allows Deep Edge to determine spam based on the reputation of the originating Mail Transfer Agent (MTA). With ER enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.



Note

For Email Reputation Services to function properly, all address translation on inbound SMTP traffic must occur after traffic passes through the Deep Edge. If NAT or PAT takes place before the inbound SMTP traffic reaches the Deep Edge, Deep Edge will always see the local address as the originating MTA. ERS only blocks connections from suspect MTA public IP addresses, not private or local addresses. Therefore, customers using Email Reputation Services should not translate inbound SMTP connections before they are scanned by Deep Edge.

- ERS Standard service (formerly known as Realtime Blackhole List or RBL+) is a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed.
- ERS Advanced service (formerly RBL + and Quick IP Lookup or QIL combined) is a DNS, query-based service similar to ERS Standard. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database. This service stops sources of spam while they are in the process of sending millions of messages.

When an IP address is found in either database, ERS “marks” the connection, and the Deep Edge behaves according to your chosen configuration.

Anti-Spam Profiles

Anti-spam profiles are global and cannot be created or deleted, only enabled or disabled. All policies will share the same Anti-Spam settings when applied as a security profile, although the type security action can be modified. When not using anti-spam scanning, the anti-spam profile can be safely disabled.

Anti-spam uses Email Reputation Services (ERS) technology, which is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge. For details, see [Email Reputation Technology on page 4-47](#).

Enabling and Disabling the Anti-Spam Profile

The anti-spam profile must be enabled before using it in a policy.

Procedure

1. Go to **Policies > Security Settings > Anti-Spam**.
2. Do one of the following:

- To enable the use of the anti-spam profile, select the **Enable email reputation** check box.
- To disable the use of the anti-spam profile, deselect the **Enable email reputation** check box.

3. Click **OK**.

Configuring Anti-Spam Settings

Configure Deep Edge anti-spam settings to:

- Use Email Reputation Services to determine spam based on the reputation of the originating MTA. With ERS enabled, all inbound SMTP and POP3 traffic is checked by the IP databases to see whether the originating IP address is clean or it has been blacklisted as a known spam vector.
 - Take default intelligent actions on spam or customize the actions setting for the organization
 - Create approved and blocked senders lists
 - Set the spam "sensitivity" level or catch rate
 - Define the tag used in the subject line of a spam email message
-

Procedure

1. Go to **Policies > Security Settings > Anti-Spam > Anti-Spam** tab.
2. Select **Enable email reputation** to enable ERS.

See *Email Reputation Technology on page 4-47*

3. Select the actions to take on detected spam email messages:
 - a. Leave the **Default intelligent action** radio button selected for the following actions to be in affect:
 - Permanent denial of connection (550) for RBL+ matches
 - Temporary denial of connection (450) for Zombie matches

**Note**

When using the default intelligent action, spam messages are rejected at the MTA with a brief message.

- a. Click the **Take customized action on all matches** radio button to set the actions needed on spam email messages such as:
 - SMTP error code: Set a code between 400 to 599. The default error code is 450
 - SMTP error string: "Service unavailable" is the default string.
4. Under **Approved Senders**, specify an email address and then click **Add** to approve the sender.
5. Under **Blocked Senders**, specify an email address and then click **Add** to block the sender.
6. Set the **Anti-Spam Catch Rate (Sensitivity Level)**.
 - **High:** Catches more spam. Select a high catch rate if too much spam gets through to clients.
 - **Medium:** The standard setting (default)
 - **Low:** Catches less spam. Select a low catch rate if Deep Edge is tagging too many legitimate email messages as spam.

**Note**

If needed, adjust the anti-spam catch rate at a later time. If the threshold is too low, a high incidence of spam occurs. If the threshold is too high, a high incidence of false positives (legitimate messages that are identified as spam) occurs.

7. Under **Other Settings**, change the subject line tag used to identify email messages detected as spam. The default is [Spam].
 8. Click **OK** to save the changes.
-

Modifying Anti-Spam Settings

The default anti-spam profile action can be modified to use the default intelligent action or to specify an SMTP error code, add or delete from the approved and blocked lists, change the catch rate setting or the tag used in the spam email messages subject line.

Procedure

1. Go to **Policies > Security Settings > Anti-Spam**.
2. To change the mail content scanning action, select the appropriate radio button:
 - **Default intelligent action**—Permanent denial of connection (SMTP Error Code 550) for RBL+ matches and temporary denial of connection (SMTP Error Code 450) for Zombie matches. An RBL+ match is a higher degree of confidence that the sender is a known spammer. A Zombie match is when Trend Micro thinks that a previously good sender has gone bad due to a botnet infection. For this reason, the temporary denial of connection code (450) is sent.
 - **Take customized action of all matches**—If this is selected, specify the SMTP error code and message to be viewed when violations of this profile occur.
3. Add or remove entries from the approved and blocked users lists. To delete an entry, select it and click **Remove**.
 - Select an entry and click **Remove** to delete it.
 - Click **Remove All** to remove all entries in the list.
4. Change the **Anti-Spam Catch Rate (Sensitivity Level)**.
 - **High**
 - **Medium**
 - **Low**: (default)

**Note**

The anti-spam catch rate can be adjusted after configuring the anti-spam settings. If the threshold is too low, a high incidence of spam occurs. If the threshold is too high, a high incidence of false positives (legitimate messages that are identified as spam) occurs.

5. Under **Other Settings**, change the subject line tag used to identify email messages detected as spam. The default is **Spam**.
 6. Click **OK**.
-

Configuring Anti-Spam Content Settings

Anti-spam content settings uses various criteria to filter messages.

- Size
 - Header content
 - Body content
 - Attachment content
-

Procedure

1. Go to **Policies > Security Settings > Anti-Spam > Content Filtering** tab.
 2. Under **Filter Message Header**, specify the keywords or regular expressions to filter for the email message footer.
-

**Note**

Use any combination of keywords and regular expressions to define a keyword expression when configuring filtering strings for the header, footer, and attachments. Specify a backslash \ immediately before the following characters:

`. \ | ( ) { } [ ] ^ $ * + or ?`

Separate keywords and regular expressions by a comma.

3. Under **Filter Message Body**, specify the keywords or regular expressions to filter for the email message body.
 4. Under **Filter Message Attachment Name**, specify the keywords or regular expressions to filter for the email message attachment file name.
 5. Click **OK** to apply the changes.
-

WRS Profiles

Web Reputation Services (WRS) scrutinizes URLs before users access potentially dangerous websites, especially sites known to be phishing or pharming sites. Employing WRS, Deep Edge provides real-time protection, conserves system scanning resources, and saves network bandwidth by preventing the infection chain or breaking it early. Web Reputation technology guards end-users against emerging web threats. Because a Web Reputation query returns URL category information (used by URL filtering), Deep Edge does not use a locally-stored, URL database.

Web Reputation technology also assigns reputation scores to URLs. For each accessed URL, Deep Edge queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level. With Trend Micro Web Reputation technology (part of the Smart Protection Network), Deep Edge can perform website scanning at varying protection levels (low, medium, and high).

Deep Edge provides anti-phishing and anti-pharming protection through Web Reputation, if it is enabled.

WRS profiles can be applied to any policy. It is safe to disable any unused WRS profile.

The web reputation database resides on a remote server. When a user attempts to access a URL, Deep Edge retrieves information about this URL from the web reputation database and stores it in the local cache. Having the web reputation database on a remote server and building the local cache with this database information reduces the overhead on Deep Edge and improves performance.

The web reputation database is updated with the latest security information about web pages. If the reputation of a URL seems misclassified or to discover the reputation of a URL, visit: <http://global.sitesafety.trendmicro.com/>

Configuring WRS Profiles

If there are too many false positives or to enhance protection, modify the WRS profile to be stricter or more lenient.

Procedure

1. Go to **Policies > Security Settings > WRS**.
 2. Select the **Enable WRS security** check box.
 3. Click the appropriate radio button (**High**, **Medium**, or **Low**) to set the URL blocking sensitivity level to align with corporate objectives:
 - **High**—Blocks more websites, but risks blocking non-malicious websites.
 - **Medium**—Balances risks between High and Low settings (default).
 - **Low**—Blocks fewer websites, but risks not blocking potentially malicious websites.
 4. Click **OK**.
-

About HTTPS Inspection

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols widely adopted and deployed in network communication today. The traffic over SSL/TLS is encrypted and signed to ensure security, hence HTTPS. Because encrypted HTTP connections can carry the same risks as unencrypted HTTP connections, Deep Edge scans all traffic for potential risks and threats.

Deep Edge can enable or disable HTTPS inspections and exclude specific websites, URL categories, or IP addresses from inspection. After the traffic is identified, Deep Edge determines the appropriate actions for traffic based on specified policy settings. To scan HTTPS traffic, Deep Edge identifies the SSL connection at the first packet of the SSL handshake, acquires the client IP address information from the session, if available, and then gets the server host name from the handshake record. The connection will not be decrypted if this information matches any allowed URL categories, websites, or IP addresses in the Deep Edge exception list.

Information about HTTPS Inspection is shown in corresponding logs and reports. HTTPS Inspection notifications are also available to inform end-users why their actions on the web are being blocked.

General Settings for HTTPS Inspection

Encrypted HTTP connections can carry the same risks as unencrypted HTTP connection. They also must be inspected for potential risks and threats. Deep Edge can enable or disable HTTPS inspection and exclude specific websites, URL categories, or IP addresses from HTTPS inspection

Adding HTTPS Exceptions

Deep Edge closes HTTPS security loopholes by decrypting and inspecting all encrypted traffic. You can allow clients to access all HTTPS traffic for specified URL categories or source IP addresses by adding them to the HTTPS Inspection exception list. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules are applied. Decrypted data remains completely secure in the Deep Edge server's memory. Before leaving the Deep Edge server, data is encrypted for secure passage to the client's browser.

For traffic filtering, Deep Edge first queries URL categories according to the host name from the local pattern or local cache. If the category is not in the local pattern or local cache, then this connection is not decrypted. To determine whether or not to decrypt traffic, another thread will issue a Trend Micro URL Filtering Engine (TMUFE) query at the same time and put the result into local cache. When a user accesses the same site in the future, Deep Edge matches the decryption policy with the category queried to the local cache.

Procedure

1. Go to **Policies > HTTPS Inspection > General Settings**.
2. Select **Enable HTTPS Traffic Inspection**.
3. Under URL Category Exceptions, search or specify specific URL categories to allow. For a full description of available URL categories, see [About URL Category Objects on page 4-17](#).

4. Under **Server Host Name Exceptions**, click **Allow or Block Hosts** to update the approved or block URLs.

The **Approve/Block URLs** screen appears. For details about managing approved and blocked URLs, see [About Approved/Blocked URLs on page 4-67](#).

5. Under **Source Address Exceptions**, click **Add New** to specify an IP address that all clients can access using an HTTPS connection.

The **Add/Edit** window appears.

6. Specify the name, protocol, and all IP addresses to allow, and then click **OK**.

The new source is added to the list.

7. Select the new source address that Deep Edge will not inspect.

8. Click **OK**.

Now, all HTTPS traffic for the specified URL categories, servers, or source addresses will not be inspected.

About Digital Certificates

By default, Deep Edge acts as a private CA and dynamically generates digital certificates that are sent to client browsers to complete a secure passage for HTTPS connections. However, the default CA is not signed by a well-known (trusted) CA on the Internet. Client browsers always display a certificate warning every time users access an HTTPS website. Although users can safely ignore the certificate warning, Trend Micro recommends using a signed CA for Deep Edge.



Note

Deep Edge supports certificates using X509 and PKCS12 formats.

Importing a Certificate Authority

Import the organization's Certificate Authority to secure the communication between the network and Deep Edge.

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Authority** tab.
 2. Do one of the following:
 - For public certificates, click **Browse** next to the **Public Certificate** field, and then select the appropriate certificate to import.
 - For a private key, click **Browse** to the **Private Key** field, and then select the appropriate certificate to import. If the private key is encrypted by a password, type it in the **Passphrase** field. If the private key is not encrypted by a password, leave the **Passphrase** field blank.
 3. Click **Import Certificate**.
-

Exporting a Certificate Authority

Deep Edge will only export public certificates.

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Authority** tab.
 2. Click **Export Certificate**.

The **Opening default.cer** pop-up window appears.
 3. Click **OK** to save the certificate.
-

Digital Certificate Management

For Deep Edge to determine if a web server's signature is trusted, the root Certification Authority (CA) certificate on which the signature is based must be added to the Deep Edge certificate store. There are three types of digital certificates that are involved in producing a digital signature:

- The "end" or "signing" certificate, which contains the public key to be used to validate the actual web server's signature
- One or more "intermediate" CA certificates, which contain the public keys to validate the signing certificate or another intermediate certificate in the chain
- The "root" CA certificate, which contains the public key used to validate the first intermediate CA certificate in the chain (or, rarely, the signing certificate directly).

If Deep Edge encounters an unknown certificate during SSL handshake or signature processing, it saves the certificate in the "not trusted" list. All types of certificates are collected in this way (signing, intermediate, and root). If required later, a CA certificate collected this way can be "trusted" by Deep Edge, allowing the signatures of those web servers that depend on that CA certificate to be processed as valid. Intermediate CA and end certificates might be activated, but this only has an effect if the root certificate is also activated.

To manage the certificates in the Deep Edge certificate store, perform the following operations:

- **Add New**—Add a new certificate that does not exist in the system.
- **Delete**—Remove the selected certificate(s) from the certificate store.
- **Trust Authenticity of Certificate**—Make a CA certificate trusted.
- **Do Not Trust Authenticity of Certificate**—Keep the certificate in the Deep Edge certificate store, but do not trust certificates that use it in their certification path.

Viewing Certificate Details

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Management** tab.
2. Click any listed certificate in the Deep Edge certificate store.

The **Certificate Details** window appears.

3. Review the details and click **Back** to return to the certificate store.
-

Adding a New Certificate

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Management** tab.
2. Click **Add New**.
An **Add a new certificate** window appears.
3. Click **Browse** to select the certificate, and then click **Open**.
4. Click **Add**.
5. At the confirmation window, click **OK**.

The new certificate is added to the Deep Edge certificate store.

Changing a Certificate's Status

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Management** tab.
2. Select any certificate to modify by using the search bar or scroll bar to find them.



Note

A certificate cannot be updated to the same status as it is currently set.

3. Do one of the following:
 - To change a CA to trusted:

- a. Click **Trust Authentication of Certificate**.
A **Trust Authenticity of Certificate** window appears.
 - b. Click **Trust**.
 - To change a CA to not trusted:
 - a. Click **Do Not Trust Authentication of Certificate**.
A **Do Not Trust Authenticity of Certificate** window appears.
 - b. Click **Not Trust**.
 4. At the status change confirmation window, click **OK**.
The status is changed for all selected certificates in the Deep Edge certificate store.
-

Deleting a Certificate

Procedure

1. Go to **Policies > HTTPS Inspection > Digital Certificates > Certificate Management** tab.
 2. Select any certificate to delete.
 3. Click the **Delete** icon ()
 4. Click **Delete** in the confirmation dialog box.
-

The certificate is deleted from the Deep Edge certificate store.

About Bandwidth Control

Peer-to-peer downloading, video streaming and instant message applications consume network bandwidth and can impact productivity. Bandwidth control reduces network congestion by controlling communications, reducing unwanted traffic and allowing

critical traffic or services the appropriate bandwidth allocation. Bandwidth control gives all users fair access to resources and ensures better access to resources that are more central to the organization. Similar to policy rules, bandwidth control can limit traffic based on source or destination IP address, traffic type or service, and time of day.

Bandwidth control rules can be as general or specific as needed. The bandwidth control rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic uses the remaining bandwidth.

To create bandwidth control rules, first create some policy objects, which are used to define the parameters of the policy rules. For more information, see [About Policy Rules on page 4-2](#).

The **Bandwidth Control** page at **Policies > Bandwidth Control** allows users to:

- View the list of existing rules
- Add, copy, prioritize, and prioritize rules
- Enable or disable rules

**Note**

Bandwidth control policies cannot exceed the interface bandwidth settings.

Adding Bandwidth Rules

Use the **Bandwidth** page to determine bandwidth allocations for network sessions based on specified traffic attributes. After creating a new rule, configure the rule by using the tabs to specify the appropriate information.

Procedure

1. Go to **Policies > Bandwidth Control**.
2. Click **Add New**.

3. Optionally disable the rule.
 4. Specify a policy name between 1 and 32 characters, consisting of letters, numbers, or underlines.
 5. Type an optional **Description**.
 6. Configure sources address and user rules.
See *[Configuring Sources and Users Rules on page 4-62](#)*.
 7. Configure destination address rules.
See *[Configuring Destination Rules on page 4-63](#)*.
 8. Configure traffic type rules.
See *[Configuring Traffic Type Rules on page 4-64](#)*.
 9. Configure schedule and bandwidth rules.
See *[Configuring Schedule and Bandwidth Rules on page 4-65](#)*.
 10. Click **OK**.
-

Configuring Sources and Users Rules

Before you begin

Add a new bandwidth control policy at **Policies > Bandwidth Rules > Add New** as shown in *[Adding Bandwidth Rules on page 4-61](#)*.

Use the **Sources and Users** tab to define rules enforced on traffic coming from the designated source IP addresses, source users and groups, and/or source zones.

Procedure

1. Click the **Sources and Users** tab.
2. Under **Source Addresses**, select one of the following parameters:
 - **Any**: Includes all source addresses. (Default)

- **Selected addresses:** Displays a list of previously configured source addresses available or to add a new IP address.

**Note**

To add new address objects, see [Configuring Address Objects on page 3-11](#).

3. Select from the following under **Users and groups**

OPTION	DESCRIPTION
Anyone	Rule affects all known and unknown users.
Known users	Rule affects authenticated users via captive portal or identified users via transparent authentication. For details about user identification, see About Authentication on page 4-72 .
Unknown users	Rule affects users that transparent authentication cannot identify. For details about user identification, see About Authentication on page 4-72 .
Selected users	Rule affects specified users and groups (local user or LDAP). For details about user management, see End User Management on page 6-9 .

What to do next

Continue to configure destination rules, as shown in [Configuring Destination Rules on page 4-63](#).

Configuring Destination Rules**Before you begin**

- Add a new bandwidth control policy at **Policies > Bandwidth Rules > Add New** as shown in [Adding Bandwidth Rules on page 4-61](#).
- If needed, configure the sources and users as shown in [Configuring Sources and Users Rules on page 4-62](#).

Use the **Destinations** tab to define rules for traffic ending at the specified destination IP addresses and destination zones.

Procedure

1. Click the **Destinations** tab.
2. Under **Destination Addresses**, select one of the following parameters:
 - **Any:** Includes all destination addresses
 - **Selected addresses:** Displays a selectable list of previously configured destination addresses to use. Use this option to add address objects, if needed.

**Note**

To add destination addresses, see [Configuring Address Objects on page 3-11](#)

What to do next

Continue to configure traffic type rules, as shown in [Configuring Traffic Type Rules on page 4-64](#).

Configuring Traffic Type Rules

Before you begin

- Add a new bandwidth control policy at **Policies > Bandwidth Rules > Add New** as shown in [Adding Bandwidth Rules on page 4-61](#).
- If needed, configure the sources and users as shown in [Configuring Sources and Users Rules on page 4-62](#) and the destination as shown in [Configuring Destination Rules on page 4-63](#).

Use the **Traffic Type** tab to define rules for traffic matching any specified applications, URL categories, or services.

Procedure

1. Click the **Traffic Type** tab.
2. Under **Applications and URL categories**, select one of the following parameters:
 - **Any:** Include all application groups and URL categories (Default)

- **Selected:** Include only selected applications and URL categories

**Note**

For more information about adding new applications, URL category groups, or custom URL categories, see:

- [Adding a New Application Object on page 4-15](#)
 - [Adding a New URL Category Object on page 4-25](#)
 - [Adding a Custom URL Category on page 4-27](#)
-

3. Select **Enable service rules** to enforce rules on specific services.

- **Any:** Include all services
- **Selected:** Include only selected services

For details about adding service objects, see [Adding a Custom Service Object on page 4-13](#)

What to do next

Continue to configure schedules and bandwidth rules, as shown in [Configuring Schedule and Bandwidth Rules on page 4-65](#).

Configuring Schedule and Bandwidth Rules

Before you begin

- Add a new bandwidth control policy at **Policies > Bandwidth Rules > Add New** as shown in [Adding Bandwidth Rules on page 4-61](#).
- If needed, configure the sources and users as shown in [Configuring Sources and Users Rules on page 4-62](#), the destination as shown in [Configuring Destination Rules on page 4-63](#), and the traffic type shown in [Configuring Traffic Type Rules on page 4-64](#).

Use the **Schedule and Bandwidth** tab to enforce rules based on selected timetables and bandwidth consumption.

Procedure

1. Click the **Schedules and Bandwidth** tab.
2. Specify the schedule and downstream bandwidth settings.

Schedule	Select a schedule from the drop-down list. • Always: (default) Includes all schedules. • Schedule name: Displays names of available schedule objects. • Add new: Access the Add/Edit schedule object creation dialog box.  Note For more information on creating schedule objects see: Adding a Schedule Object on page 4-29.
Egress interface	Select the appropriate interface from the drop-down list.
Guaranteed bandwidth	Specify the guaranteed downstream bandwidth.
Maximum bandwidth	Specify the guaranteed downstream bandwidth.

3. Optional: Specify **Advanced Settings**.

Guaranteed bandwidth	Specify the guaranteed upstream bandwidth.
Maximum bandwidth	Specify the guaranteed upstream bandwidth.
Service priority level	Select the service priority level from the drop-down list. If the network is congested, network traffic with bandwidth control rules set to a higher service level have priority over traffic with a lower service level.

4. Click **OK**.
-

Enabling/Disabling Bandwidth Rules

Policies can be provisioned disabled. This procedure applies to policy rules already created but not enabled.

Procedure

1. Go to **Policies > Bandwidth Control**.
 2. Click the name of the policy rule to enable or disable
 3. Do one of the following:
 - Select the check box to enable the policy
 - Deselect the check box to disable policy
 4. Click **OK**.
-

About Approved/Blocked URLs

Approved and blocked URLs allow traffic to override the defined categories of URL Filtering, IPS, WRS, and Anti-malware settings. When adding URLs to the lists, keep the following in mind:

- URLs can use an asterisk (*) as a wildcard, which should only be typed at the beginning or ending of the string.
- The Approved list takes precedence over the Blocked list.

Configuring Approved or Blocked URLs

Procedure

1. Go to **Policies > Approve/Block URLs**.
2. Do one of the following:

- Select the **Approved URLs** tab to add an allowed URL.

**Note**

Carefully approve websites. Not scanning or blocking a website could pose a security risk.

- Select the **Blocked URLs** tab to block a URL to be prohibited.

3. Specify the appropriate string in the text box:

- For a website, type `www.example.com/*`
- For a keyword, type `*keyword_example*`
- For a string, type `string_example` or `123.123.123.123`

**Note**

Use a comma or semi-colon to separate multiple entries.

4. Click **OK**.

Enabling/Disabling the Approved List or Blocked List

Procedure

1. Go to **Policies > Approve/Block URLs**.
2. Click the tab of the list to enable or disable, either **Approved URLs** or **Blocked URLs**.
3. Do one of the following:
 - To enable the list, select the enable list check box.
 - To disable the list, deselect the enable list check box.

4. Click **OK** to save changes.
-

About Anti-DoS

A Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack is an attempt to make a machine or network resource unavailable to users, and is intended to temporarily or indefinitely interrupt or suspend services to a host connected to the Internet.

Typical attacks involve saturating the target machine with external communication requests, such that the machine can no longer respond to legitimate traffic, or responds so slowly it is rendered unavailable. Such attacks usually lead to server overload.

The three most common methods of attack include:

TCP SYN flood

A Transmission Control Protocol (TCP) Synchronous Transmission (SYN) flood occurs when a malicious host sends a flood of TCP/SYN packets - often with a forged sender address. Each of these packets is handled like a connection request, causing the server to spawn half-open connections by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet). However, because the sender address is forged, the response never arrives. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack is over.

UDP flood

A User Datagram Protocol (UDP) flood overloads the target server by repeatedly sending an overwhelming number of UDP packets.

ICMP/Ping flood

An Internet Control Message Protocol (ICMP) flood sends its victims an overwhelming number of ping packets, usually by using the "ping" command. It is simple to launch with the purpose of gaining access to a greater amount of bandwidth than its victim.

Configuring Flood Protection

With user-defined thresholds, Deep Edge limits the number of packets per second that can flood a server. The packets are forwarded through Deep Edge and divided into Transmission Control Protocol (TCP) Synchronous Transmission (SYN), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) flood protection categories.

Procedure

1. Go to **Policies > Anti-DoS > Flood Protection**.
 2. Check the appropriate boxes and specify flood limitations on the packets per second fields for TCP SYN, UDP, or ICMP flood protection.
 - Limit traffic by source or destination addresses for the various flood types
 - Specify the threshold limitations
 3. Click **OK**.
-

Adding Address Exceptions

Deep Edge maintains an exception source address list specifying the IP addresses to the list that will not be limited or filtered.

Procedure

1. Go to **Policies > Anti-DoS > Address Exceptions** tab.
2. Click **Add New**.

The **Add/Edit Address Object** page appears.
3. Specify the IP address, IP address range, or the IP address/netmask of the address objects not to limit or filter.
4. Select the type of packets to apply to this particular exception list:

OPTION	DESCRIPTION
TCP SYN	Transmission Control Protocol/Synchronous Transmission
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol

5. Click **OK**.
-

Modifying Address Exceptions

Procedure

1. Go to **Policies > Anti-DoS > Address Exceptions**.
 2. Click the address to be modified.
 3. Modify the address object as necessary.
 4. Click **OK**.
-

Deleting Address Exceptions

Procedure

1. Go to **Policies > Anti-DoS > Address Exceptions**.
 2. Select the check box of the address to delete.
 3. Click the **Delete** icon (.
 4. Click **Delete** in the confirmation dialog box.
-

About Authentication

By default, Deep Edge only allows traffic that is explicitly allowed by policy rules. Users from specified IP addresses are identified using User Identification and authentication methods. Other policies are enforced by source and destination IP address, profiles, service, schedule, and/or application type.

A UserID Agent is a Deep Edge application installed on the network to obtain needed mapping information between IP addresses and network users. The UserID Agent collects user-to-IP address mapping information automatically and provides it to the firewall for use in security policies and logging.

Configure specific IP addresses or IP address ranges to use specific authentication approaches:

- For transparent authentication, Deep Edge retrieves the login log information from the Domain Controller periodically, which makes it possible to map a user to an IP address. If this fails, Deep Edge directly connects to the client machine (the one trying to access a location outside the network) to query for the current logged-in user. (This requires that the LDAP settings account has the appropriate privileges.)
- For captive portal, if an IP address is not authenticated yet, and if the current request is a HTTP request, the user is directed to a web page to provide domain account login information.

For user/group information, Deep Edge periodically synchronizes the overall LDAP user tree to a local cache. Subsequent user-group relationship queries are resolved locally.



Note

User identification mapping requires that the firewall obtain the source IP address of the user before the IP address is translated with NAT. If multiple users appear to have the same source address, due to NAT or use of a proxy device, accurate user identification is not possible.

The list of UserID policies uses the **Policies > Objects > Addresses** entries.

The custom captive portal sign-in can be accessed from the **Policies > Authentication > Captive Portal** page. If the UserID Agent is unable to associate a user with an IP

address, a captive portal can take over and authenticate the user. For more information, see [About Captive Portal on page 4-74](#).

User Identification Methods

User identification identifies which IP address belongs to which user. This allows a method of user identification to be built using an IP address-to-user mapping cache for policy matching. For details about adding rules, see [Adding Authentication Rules on page 4-73](#).

By default, all IP addresses do not automatically work with user identification. Make sure to define which source IP addresses or range of IP addresses must work with user identification. If a source IP address is not in the defined ranges, the IP address will not work for user identification. (In such cases, the policy source IP address must be set to "Any" for user or group policies to work.)

For the specified IP addresses or ranges of IP addresses, define user identification methods including:

- Transparent authentication (using Windows Client Query and Domain Controller Event Log Query)
- Captive Portal

Adding Authentication Rules

Procedure

1. Go to **Policies > Authentication > Endpoint Identification**.
2. Click **Add New**.
3. Select whether to use **Captive Portal**.
See [About Captive Portal on page 4-74](#).
4. Specify a name for the policy.
5. Select an existing address object or add a new one.

For details about address objects, see [About Addresses and Address Objects on page 3-9](#).

6. Click **OK**.

What to do next

Verify that the name appears in the Authentication policy list at **Policies > Authentication > Endpoint Identification**.

About Captive Portal

If the user identification agent is unable to associate a user with an IP address, a captive portal can take over and authenticate the user with a web form.

To receive the web form, users must be using a web browser and be in the process of connecting. Upon successful authentication, users are automatically directed to the originally requested website. The firewall can now execute policies based on the user information for any applications passing through the firewall, not just for applications that use a web browser.



Important

To enable captive portal, see [Enabling Captive Portal on page 4-75](#).

The following rules apply to captive portals:

- Captive portal rules work only for web (HTTP) traffic.
- A web page prompts the user to specify a user name and password.

If the above-mentioned captive portal rules do not apply because the traffic is not HTTP or there is no rule match, then the firewall applies its IP address-based security policies.

Deep Edge validates the user name and password against LDAP server. If successfully authenticated, Deep Edge adds the IP address-to-user mapping to local cache for the time-to-live (TTL) life cycle. If authentication fails, Deep Edge notifies the user that authentication was not successful.

You can also design and create the text that users see when they sign on. The customizable message includes:

- Company logo
- Company name
- A welcome message
- External HTTP link (URL)

Enabling Captive Portal

Procedure

1. Go to **Administration > Device Management > Management Service** tab and select **Web Console** on the appropriate interface.
 2. Make sure that clients using captive portal can resolve the Deep Edge host name.
-

Configuring the Captive Portal Settings

The Captive Portal Sign-on page can require all users to specify a user name and password (assigned by an Administrator) before accessing the network or Internet. If the UserID Agent is unable to associate a user with an IP address, a captive portal takes over and authenticates the user.

Procedure

1. Go to **Policies > Authentication > Captive Portal**.
2. Click **Browse** to browse to the location of a .PNG or .GIF file of the company logo to display on the Captive Portal sign-on page.



Note

The image must be less than 700 x 200 pixels and 1MB in size.

3. Click **Upload** to upload the image.

4. Add the appropriate **Company name**.
 5. (Optional) Customize the **Welcome message**.
 6. (Optional) Add an external HTTP link to your company website.
 7. Click **Preview** to display and verify the message.
 8. Close the tab displaying the preview.
 9. Click **Apply** if satisfied or **Reset** to return to the default values.
-

About User Notifications

Use the setting on the appropriate page to notify the end-user about violations that occur.

To configure end-user notifications, see the following:

- [*Configuring WRS Violation Notifications on page 4-76*](#)
- [*Configuring URL Filtering Violation Notifications on page 4-77*](#)
- [*Configuring Application Control Violation Notifications on page 4-78*](#)
- [*Configuring Anti-Malware Violation Notifications on page 4-79*](#)
- [*Configuring Blocked URL Violation Notifications on page 4-79*](#)
- [*Configuring File Extension Violation Notifications on page 4-80*](#)
- [*Configuring IPS Violation Notifications on page 4-81*](#)
- [*Configuring Server Certificate Failure Notifications on page 4-82*](#)
- [*Configuring Client Certificate Failure Notifications on page 4-83*](#)

Configuring WRS Violation Notifications

A default WRS violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for WRS violations.

Procedure

1. Go to **Policies > User Notifications > WRS Violation**.
2. Click in the displayed message and make the necessary change.

**Note**

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize your message:
 - %U: to show the URL accessed by the end-user
 - %W: to show the web reputation score about the URL accessed by the end-user
 - %H: to show the host name of the Deep Edge appliance
 4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring URL Filtering Violation Notifications

A default URL filtering violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for URL filtering violations.

Procedure

1. Go to **Policies > User Notifications > URL Filtering Violation**.
2. Click in the displayed message and make the necessary change.

**Note**

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:

- %U: to show the URL accessed by the end-user
 - %C: to show the URL category accessed by the end-user
 - %H: to show the host name of the Deep Edge appliance
4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring Application Control Violation Notifications

A default Application Control violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for Application Control violations.

Procedure

1. Go to **Policies > User Notifications > Application Control Violation**.
2. Click in the displayed message and make the necessary change.



Note

To make HTML changes, click the **HTML** icon at the top-left corner of the formatting bar.

3. Use the following tokens to customize the message:
 - %U: to show the URL accessed by the end-user
 - %T: to show the application type of the URL accessed by the end-user
 - %H: to show the host name of the Deep Edge appliance
 4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring Anti-Malware Violation Notifications

A default anti-malware violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for anti-malware violations.

Procedure

1. Go to **Policies > User Notifications > Anti-malware Violation** link.
2. Click in the displayed message and make the necessary change.



Note

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:
 - %U: to show the URL accessed by the end-user
 - %V: to show the virus name in the URL accessed by the end-user
 - %H: to show the host name of the Deep Edge appliance
 4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring Blocked URL Violation Notifications

A default end-user notification exists for blocked URL violation notifications. Use this procedure to edit and preview the message used in the end-user notifications for blocked URL violations.

Procedure

1. Go to **Policies > User Notifications > Blocked URL Violation** link.
2. Click in the displayed message and make the necessary change.

**Note**

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:
 - %U: to show the URL accessed by the end-user
 - %H: to show the host name of the Deep Edge appliance
 4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring File Extension Violation Notifications

A default file extension violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for file extension violations.

Procedure

1. Go to **Policies > User Notifications > File Extension Violation** link.
2. Click in the displayed message and make the necessary change.

**Note**

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:
 - %U: to show the URL accessed by the end-user
 - %M: to show the matched file extension in the URL accessed by the end user
 - %H: to show the host name of the Deep Edge appliance
4. Click **Preview** to review changes.

5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Configuring IPS Violation Notifications

A default IPS violation notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for IPS violations.

Procedure

1. Go to **Policies > User Notifications > IPS Violation** link.
2. Click in the displayed message and make the necessary change.



Note

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:
 - %U: to show the URL accessed by the end-user
 - %V: to show the violated IPS rule ID
 - %H: to show the host name of the Deep Edge appliance
 4. Click **Preview** to review changes.
 5. Click **OK** to save changes or **Cancel** to revert to the default message.
-

Certificate Failure Notifications

When Deep Edge detects an attempt to access a URL in violation of an HTTP inspection policy with a blocking action, a warning screen displays in the requesting clients browser to indicate that the URL was blocked. For HTTPS decryption, there are three kinds of notifications: HTTPS scanning, HTTPS certificate failure, and client certificate block. The HTTPS scanning notification and the normal HTTP traffic notification are the same. For details, see [About User Notifications on page 4-76](#).

Configuring Server Certificate Failure Notifications

A default server certificate failure notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for server certificate failures.

Whenever users are denied access to a website whose certificate does not pass the verification tests, they will see this HTML warning message. Users have the option to do one of the following:

- Review the certificate.
- Continue accessing the website (not recommended).

Procedure

1. Go to **Policies > User Notifications > Server Certificate Failure**.
2. Click in the displayed message and make the necessary change.



Note

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize a message:
 - %U: to show the URL accessed by the end-user
 - %H: to show the host name of Deep Edge
4. Click **Preview** to review changes.

The **HTTPS Certificate Failure** preview appears.

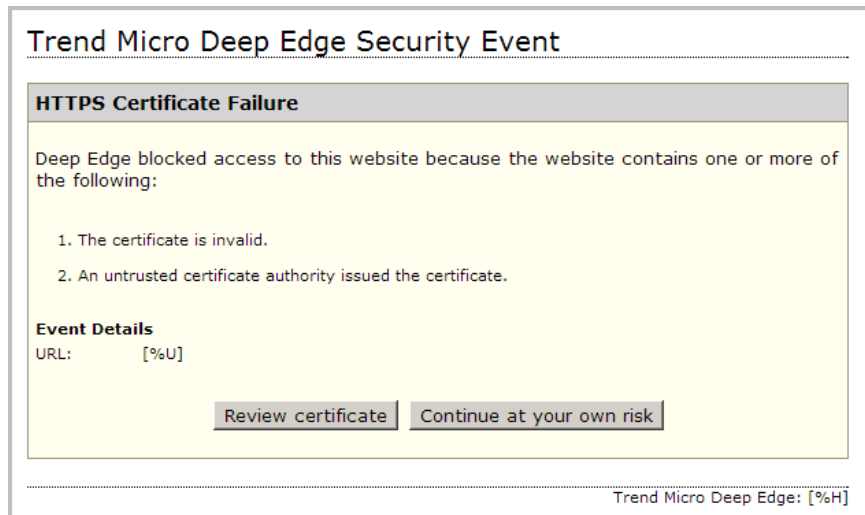


FIGURE 4-2. HTTPS Certificate Failure Notice

5. Click **OK** to save changes or **Cancel** to revert to the default message.

Configuring Client Certificate Failure Notifications

A default client certificate failure notification exists in Deep Edge. Use this procedure to edit and preview the HTML message used in the end-user notifications for client certificate failures.

Procedure

1. Go to **Policy > User Notifications > Client Certificate Failure** link.
2. Click in the displayed message and make the necessary change.



Note

To make change in the HTML, click the first icon on the tool bar of the message.

3. Use the following tokens to customize the message:

- %U: to show the URL accessed by the end-user
- %H: to show the host name of Deep Edge

4. Click **Preview** to review the changes.

The **Client Certificate Failure** preview appears.



FIGURE 4-3. Client Certificate Failure Notice

5. Close the preview to return to the configuration screen.
 6. Click **OK** to save your changes or **Cancel** to revert to the default message.
-

Chapter 5

Intelligent Daily Monitoring

Deep Edge intelligently monitors the network and how policies are enforced. After configuring network settings to process and identify traffic passing through the network, you have a variety of monitoring capabilities to actively be aware of new or emerging security threats.

Topics include:

- *Dashboard and Widgets on page 5-2*
- *Analysis and Reports on page 5-30*
- *Log Settings on page 5-39*
- *Device Logs on page 5-40*

Dashboard and Widgets

The dashboard and widgets inform you about all network activity monitored or controlled by Deep Edge. Deep Edge collects substantial log data about your network traffic. Rather than sifting through massive log data, you can acquire actionable intelligence via graphical representations of logs in the dashboard widgets to quickly learn about which threats are affecting the network and how Deep Edge protects your clients from harm.

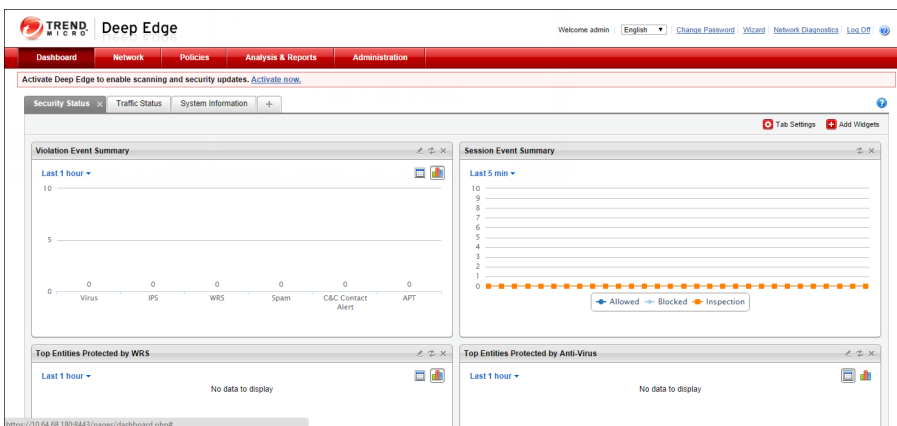


FIGURE 5-1. Deep Edge Dashboard



Note

For more information about widgets, see *Using Widgets on page 5-8*.

About Tabs

To customize the Deep Edge Dashboard, you can add additional tabs, name the new tabs as needed, and add the appropriate widgets. Added tabs can be modified and deleted. The default tabs cannot be deleted, but may be modified.

The default tabs display status widgets in the following three categories:

- Security
- System
- Traffic

Adding a New Tab

Procedure

1. Go to the **Dashboard**.
2. Click the  to the right of the last named tab.
The **New Tab** screen appears.
3. Specify a name for the **Title** of the new tab.
4. Select the radio button for the appropriate layout style.
5. Select **Auto-fit On** to make the height all widgets on the tab consistent.
6. Click **Save**.

The new tab is added to the right of existing tabs.

Modifying Tab Settings

Procedure

1. Go to the **Dashboard**.
2. Click the tab to modify.
3. Click the **Tab Settings** link.
4. Make the changes needed to:
 - **Title**

- **Layout**

5. Click **Save**.

Deleting a Tab

It is only possible to delete tabs that were added. Only added tabs can be deleted. The default tabs (Security Status, Traffic Status, and System Status) are not deletable.

Procedure

1. Go to the **Dashboard**.
 2. Click the **X** beside the name of an added tab.
 3. Click **OK** to confirm the deletion.
-

About Widgets

Customizable widgets can be added to or removed from dashboard tabs. Each widget includes a description of its purpose.

TABLE 5-1. Deep Edge Widgets

TAB	WIDGETS
Security Status	• Violation Event Summary* • Session Event Summary* • Top Entities Protected by Anti-Virus* • Entity Risk Summary • Top Entities Protected by WRS* • Top Entities Protected by IPS • Top Entities Protected by Anti-Spam • C&C Contact Alert • Top Entities Protected by Advanced Threat Scanning
Traffic Status	• Session Summary* • Top Users* • Top Applications* • Bandwidth Summary* • Bandwidth Control • Top Domains • Top URL Categories
System Information	• Interface Information* • Network Information* • System Information* • System Resource* • Pattern Information • Hardware Monitor

* denotes widgets displayed by default.

Customizing Widgets

Widgets can be manually updated and configured/filtered to display needed information.

Widgets can be customize to display information about a specific time period. For some widgets, the information can be displayed in graph or table format.

Procedure

1. Go to the **Dashboard**.
 2. Select a widget to customize.
 - a. Select the time period to be displayed by clicking on the time link in the upper left corner of the widget.
 - b. (For applicable widgets) Select the style in which information will be displayed by clicking the chart or list icon in the upper right corner of the widget.
 - c. Mouse over the data displayed and click to magnify the details.
 3. For some widgets, click the legend at the bottom of the widget to filter the information displayed.
 4. For other customizations, see the figure and table that follow. Also see *[Using Widgets on page 5-8](#)*
-

Widget Options

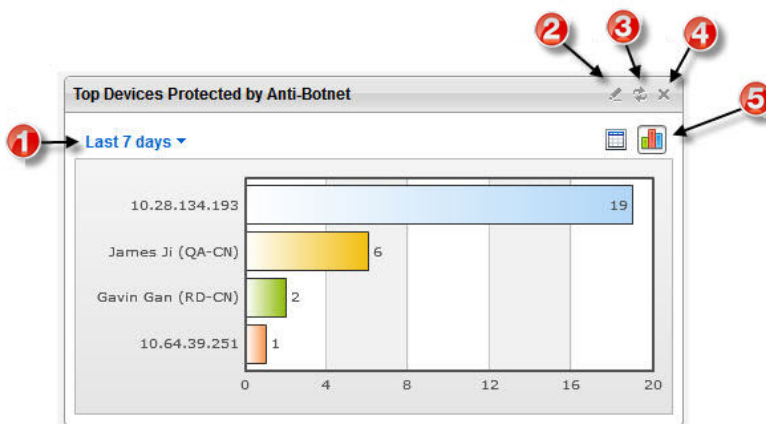


FIGURE 5-2. Widget Options

CALL-OUT	DESCRIPTION
1	Change the time period for displayed data.
2	Filter information according to the widget purpose.
3	Manually refresh the displayed information.
4	Delete the widget from the dashboard.
5	Change the graphic format for displayed data: bar chart, pie graph, or table.

Adding New Widgets

Procedure

1. Click the **Add Widgets** icon (+) in the upper right corner of the Dashboard.
The **Add Widgets** selection screen appears.

2. Select one or more widgets from the list of predefined widget designs that appear.

**Note**

To sort widgets by category, click a category on the left side of the screen.

3. Click **Add**.

Added widgets can be deleted or dragged-and-dropped to various locations within the widget container, and their configuration can still be modified.

Deleting Widgets

Procedure

1. Click the **X** in the upper left corner of the widget.
-

Using Widgets

Deep Edge uses a widget framework for dashboard implementation that allows you to select which widgets to display. The Deep Edge Summary Dashboard includes support for traffic status, system information, and security widgets.

**Note**

Deep Edge does not support widget customization. See more about adding widgets at [Adding New Widgets on page 5-7](#).

About Security Status Widgets

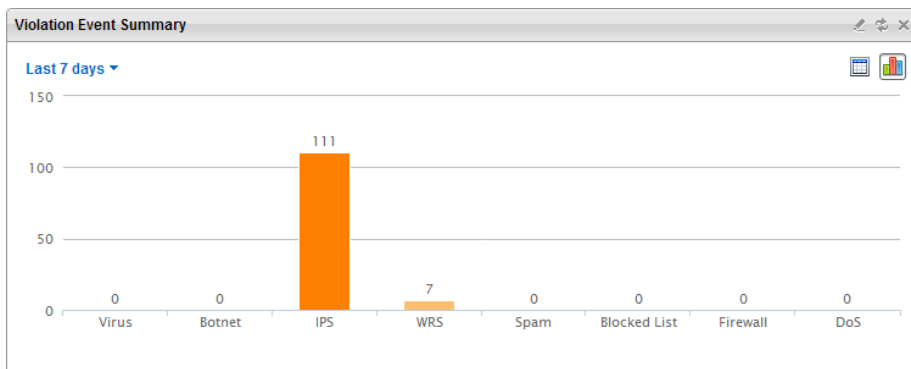
The security status category shows threat trigger times in the last hour by category: Firewall, Virus, WRS, URL Filtering, Spam, and Blocked List. The security status category contains the following widgets:

- [Violation Event Summary Widget on page 5-9](#)

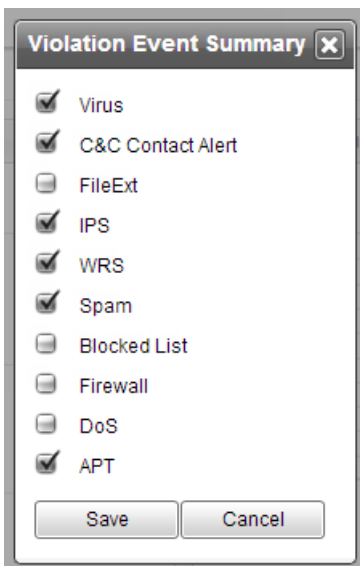
- [Session Event Summary Widget on page 5-11](#)
- [Top Entities Protected by WRS Widget on page 5-12](#)
- [Top Entities Protected by Anti-Virus Widget on page 5-13](#)
- [Entity Risk Summary Widget on page 5-13](#)
- [Top Entities Protected by IPS Widget on page 5-15](#)
- [Top Entities Protected by Anti-Spam Widget on page 5-16](#)
- [C&C Contact Alert Widget on page 5-16](#)
- [Top Entities Protected by Advanced Threat Scanning on page 5-18](#)

Violation Event Summary Widget

The **Violation Event Summary** widget shows found violations for virus, botnet, IPS, WRS, and spam in a bar chart. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



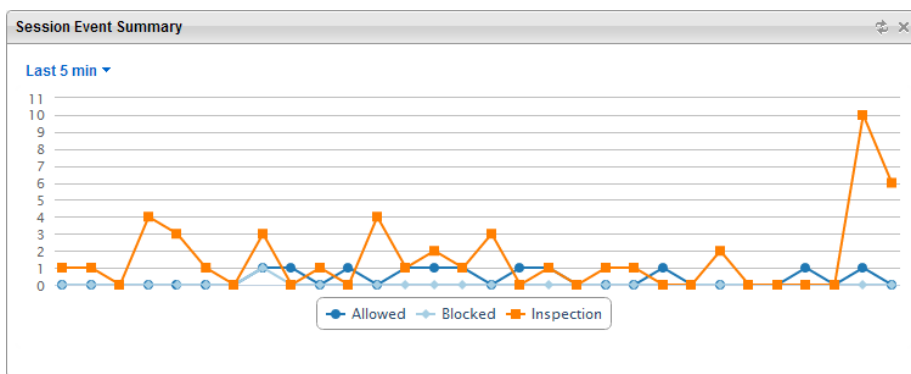
To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears. The default display is bar-chart style, but it can be toggled to display in table format.



To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

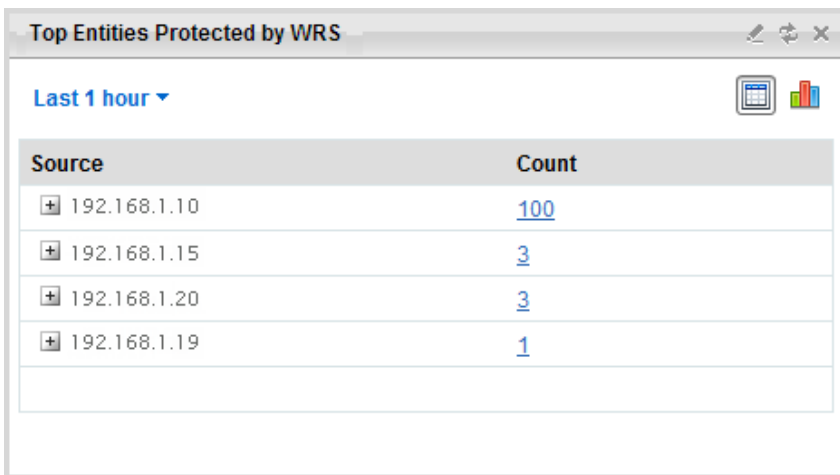
Session Event Summary Widget

The **Session Event Summary** widget shows the session events over the specified period, including how many sessions were allowed, blocked, or inspected. The widget refreshes automatically.



Top Entities Protected by WRS Widget

The **Top Entities Protected by WRS** widget shows Web Reputation Services (WRS) reputation violations. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



Source	Count
+ 192.168.1.10	100
+ 192.168.1.15	3
+ 192.168.1.20	3
+ 192.168.1.19	1

The default display is bar-chart style. Click on the table icon () located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

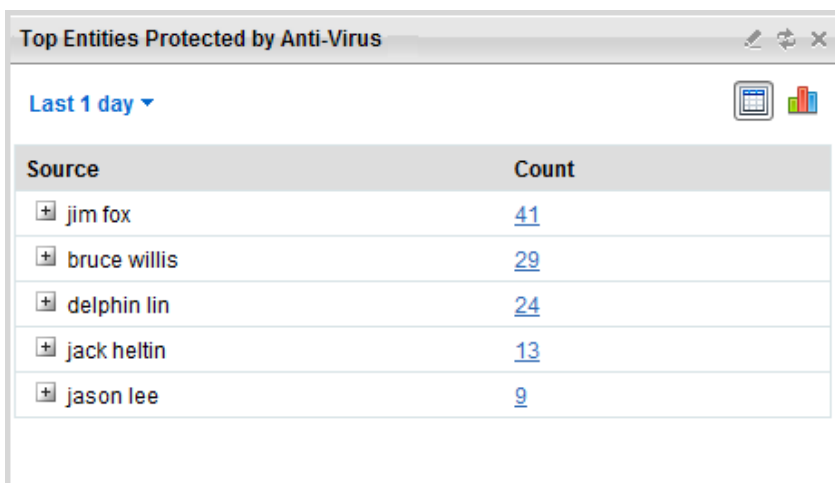
If user information is available (if the IP address is mapped to a user), the widget displays the source column as user. If the IP address is not mapped, the source IP address displays.

To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Entities Protected by Anti-Virus Widget

The **Top Entities Protected by Anti-Virus** widget shows virus-related violation information. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



The default display is bar-chart style. Click on the table icon () located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

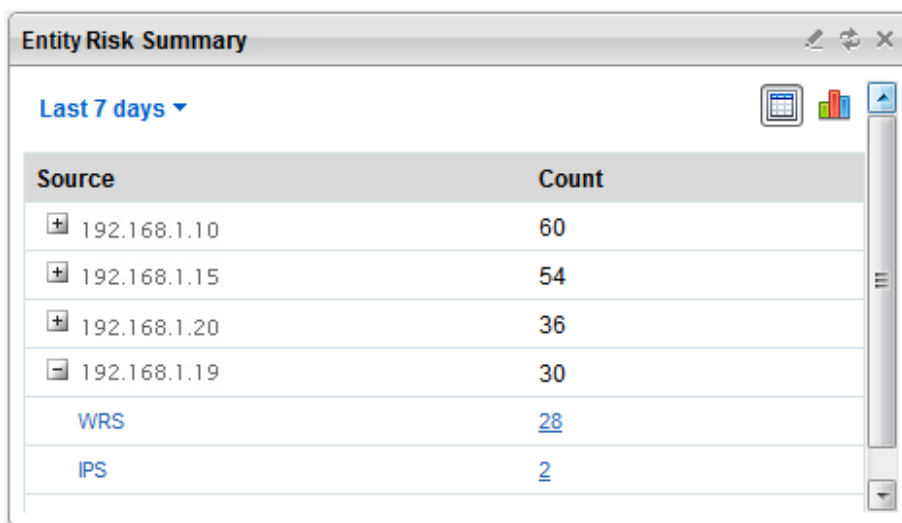
To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Entity Risk Summary Widget

The **Entity Risk Summary** widget shows the top entities with security violations. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours,

last 7 days. Based on the violation numbers, this widget combines data aggregated from the following widgets:

- **Top Entities Protected by IPS**
- **Top Entities Protected by Anti-Virus**
- **Top Entities Protected by Anti-Botnet**
- **Top Entities Protected by WRS**
- **C&C Contact Alert**
- **Top Entities Protected by Advanced Threat Scanning**



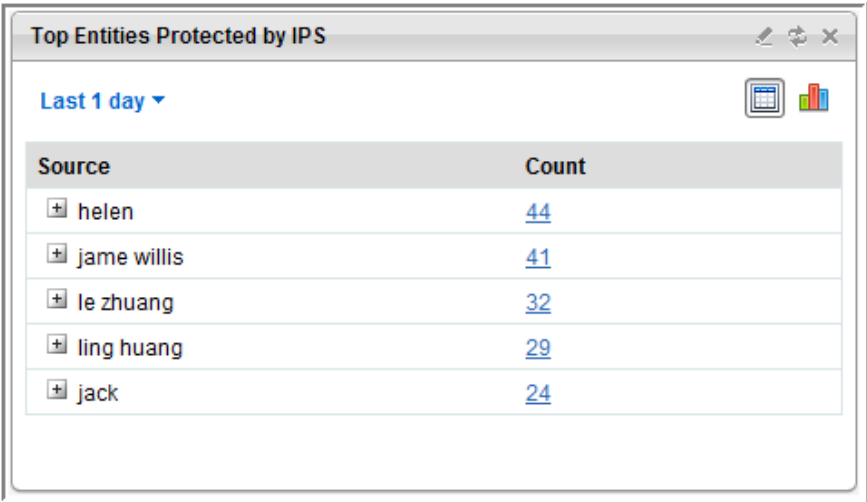
The default display is bar-chart style. Click on the table icon (📊) located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

The number of entities displayed is configurable. The top 5 show by default. To configure the displayed data sources, click the ⚙️ icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Entities Protected by IPS Widget

The **Top Entities Protected by IPS** widget shows IPS violations. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



Source	Count
 helen	44
 jame willis	41
 le zhuang	32
 ling huang	29
 jack	24

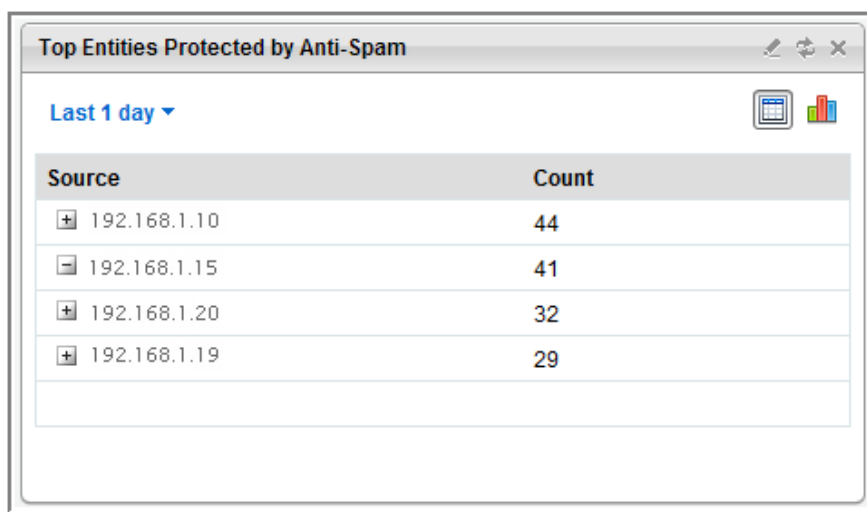
The default display is bar-chart style. Click an the table icon () located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Entities Protected by Anti-Spam Widget

The **Top Entities Protected by Anti-Spam** widget shows spam-related violations. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



The default display is bar-chart style. Click on the table icon (📊) located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

To configure the displayed data sources, click the ⚙️ icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

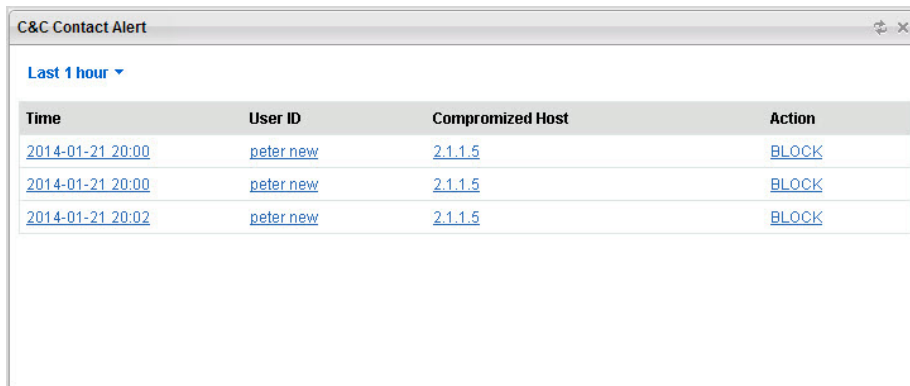
To manually refresh the data, click the ↻ icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

C&C Contact Alert Widget

Once a piece of malicious software runs, it may immediately initiate communication to a command-and-control (C&C) server for further instructions or lie dormant on a system

for hours in an attempt to remain hidden. One of two things usually happens when the software accesses the C&C server. First, the software may automatically download and install additional malware. This type of malware is called a “downloader”. Second, the software can communicate back to the C&C server. A human monitoring the C&C server (attacker) would then notice the new connection and initiate some sort of action. This type of software, called a “remote access Trojan” (RAT), gives an attacker the ability to examine a system, extract files, download new files to run on a compromised system, turn on a system’s video camera and microphone, take screen captures, capture keystrokes, and run a command shell.

The **C&C Contact Alert** widget shows all attempts by compromised hosts to connect to C&C servers. When Deep Edge detects a C&C callback attempt, the traffic is controlled based on the policy action configuration.



The screenshot shows a window titled "C&C Contact Alert" with a refresh icon and a close button in the top right corner. Below the title bar is a dropdown menu set to "Last 1 hour". The main content area contains a table with four columns: Time, User ID, Compromized Host, and Action. The table lists three entries, all with the same data: Time 2014-01-21 20:00, User ID peter.new, Compromized Host 2.1.1.5, and Action BLOCK.

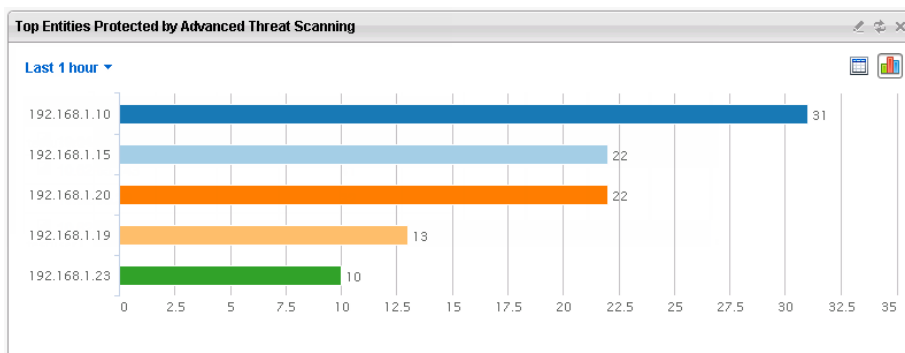
Time	User ID	Compromized Host	Action
2014-01-21 20:00	peter.new	2.1.1.5	BLOCK
2014-01-21 20:00	peter.new	2.1.1.5	BLOCK
2014-01-21 20:02	peter.new	2.1.1.5	BLOCK

The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Entities Protected by Advanced Threat Scanning

The **Top Entities Protected by Advanced Threat Scanning** widget shows targeted attack detections. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



The default display is bar-chart style. Click on the table icon () located at the top-right of the chart to display the information in table format. If user information is available (if the IP address is mapped to a user), the widget displays the **Source** column as the user. If the IP address is not mapped, the source IP address displays.

To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.



Note

For information about configuring anti-malware security settings, advanced threat scanning, or Deep Discovery Advisor settings, see [Anti-Malware Security on page 4-38](#).

About Traffic Status Widgets

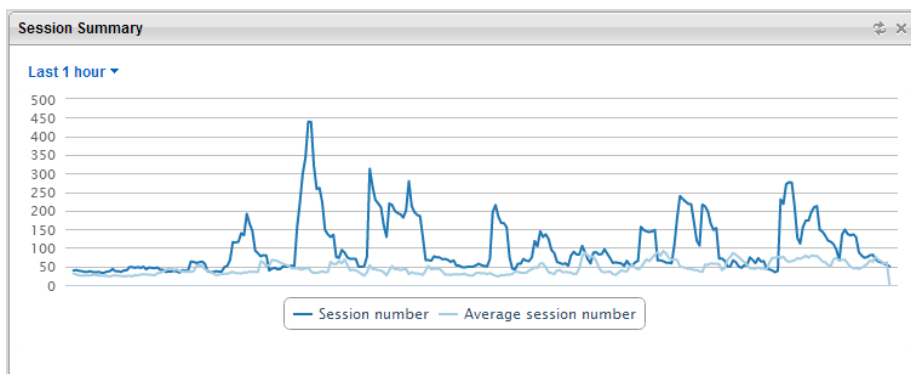
The traffic status category contains the following widgets:

- [Session Summary Widget on page 5-19](#)
- [Top Users Widget on page 5-20](#)
- [Top Applications Widget on page 5-21](#)
- [Bandwidth Summary Widget on page 5-22](#)
- [Bandwidth Control Widget on page 5-23](#)
- [Top Domains Widget on page 5-24](#)
- [Top URL Categories Widget on page 5-24](#)

Session Summary Widget

The **Session Summary** widget shows the TCP/UDP sessions status of the system.

Click the items in the legend at the bottom of the widget to filter the information displayed. Hover the mouse over the points in the line graph for more details.



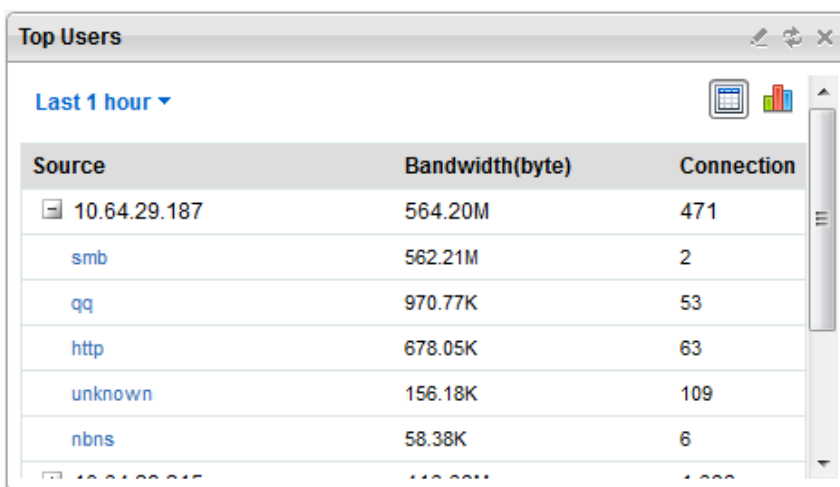
To manually refresh the data, click the  icon in the upper right corner of the widget. The refresh rate varies with the time displayed. The **Last 5 minutes** time setting refreshes every 10 seconds. Other time settings refresh every minute.

Top Users Widget

The **Top Users** widget shows the most active users on the network. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.

The default display is bar chart, but it can be toggled to display in table format. To show top applications, expand the user data.

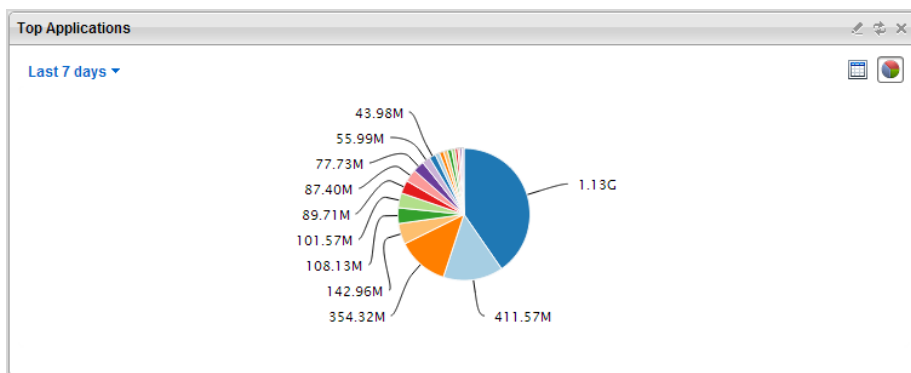
To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.



To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Applications Widget

The **Top Applications** widget shows the top applications passed through Deep Edge (configurable to be counted by bandwidth or by connection). The number of devices displayed is configurable. The top 5 show by default.



The data is for the last hour on the clock. (Example: if the current time is 2:08 pm, then the data is for 2:00 PM to 2:08 PM only.)

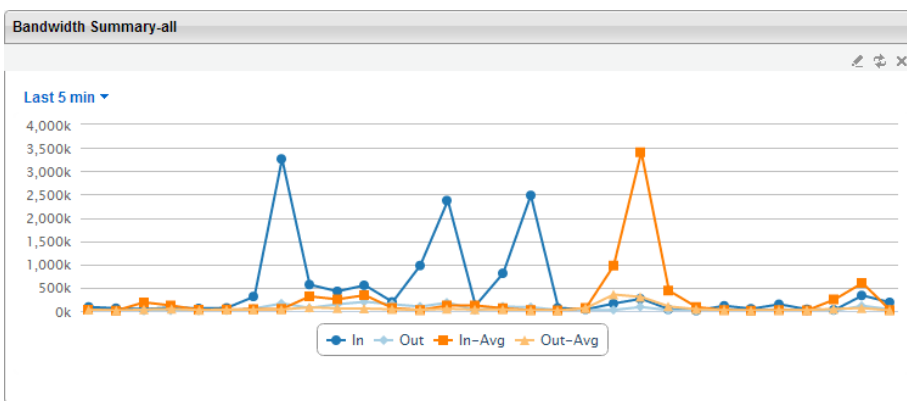
Users can set the how many applications display. Based on that information, the applications are sorted by bandwidth or connection. To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

The screenshot shows the 'Top Applications' configuration dialog box. It has a title bar with the text 'Top Applications' and a close button (X). Inside the dialog, there are two main settings: 'Top application number' and 'Top by'. The 'Top application number' is set to 5, and the 'Top by' dropdown is set to 'Bandwidth'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Bandwidth Summary Widget

The **Bandwidth Summary** widget displays bandwidth in/out information based on IP addresses. Mouse-over a point on a line to view details for specific interfaces. Data is real-time data, but the widget itself also accumulates data.



The in/out traffic count is based on the packets' source address. If the source address is an internal address, then it is displayed as 'out', otherwise it is 'in'. The internal address is configured at **Network > Address Group > Default Internal Address**. The average value calculation is based on the same time period from the previous day. For example, if the current value is 10:05, then the corresponding average value is calculated using the last seven days' values from the same time.

The traffic for one interface can appear at a time. The title of the widget denotes which interface traffic currently appears in the widget. To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Bandwidth Control Widget

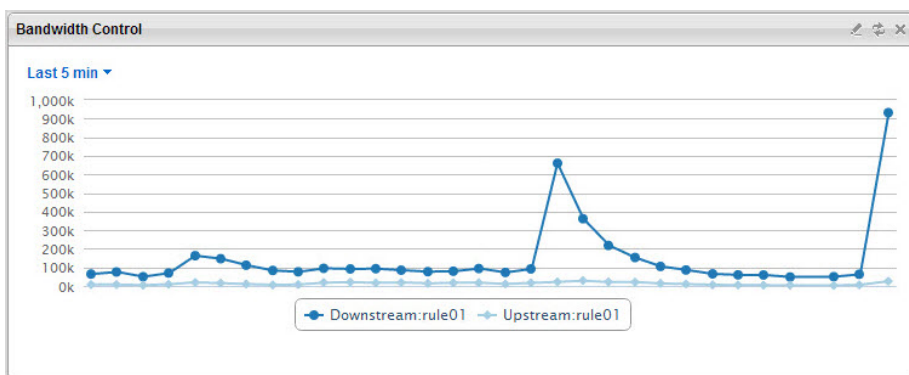
The **Bandwidth Control** widget shows the upstream and downstream bandwidth for selected bandwidth control policies for a selected period.



Note

The **Bandwidth Control** widget requires that bandwidth control policies are set. For details about bandwidth control policies, see [About Bandwidth Control on page 4-60](#).

Click the items in the legend at the bottom of the widget to filter the information displayed. Hover the mouse over the points in the line graph for more details.



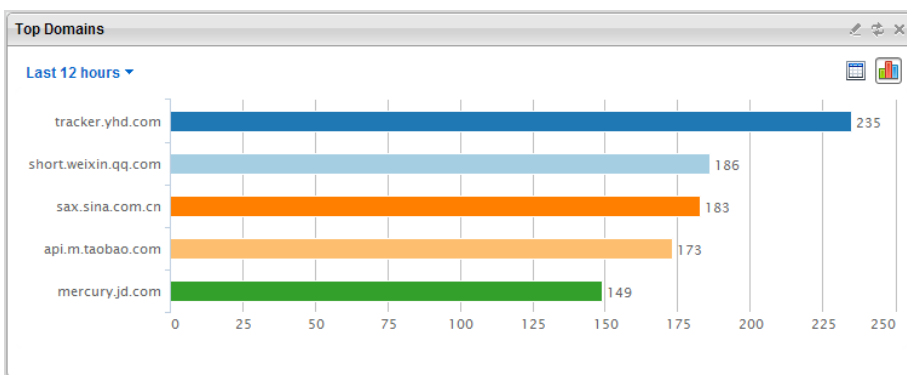
To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

The 'Bandwidth Summary' dialog box is shown. It contains a 'Select Interface' dropdown menu with 'all' selected. Below the menu are 'Save' and 'Cancel' buttons.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top Domains Widget

The **Top Domains** widget shows the most accessed domains in the network. The number of domains displayed is configurable. The top 5 show by default. The time period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



The default display is bar-chart style, but it can be toggled to display in table format.

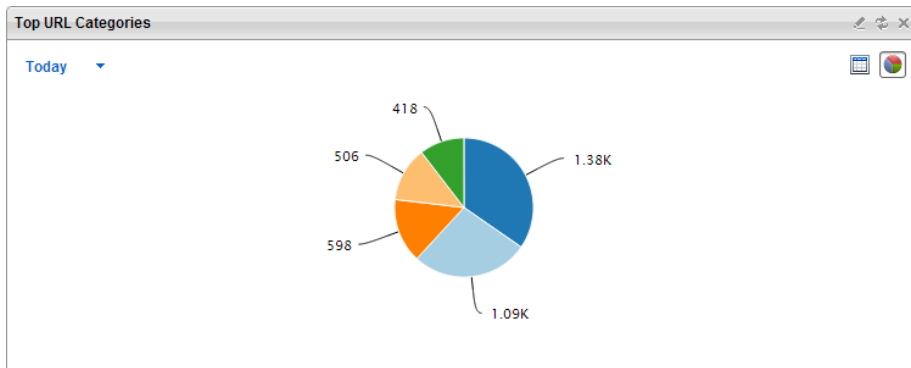
To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

Top URL Categories Widget

The **Top URL Categories** widget shows URL category-related violations. Also, the time period displayed can show information for the last hour, day, week, or month. The time

period displays information about today, last 1 hour, last 12 hours, last 24 hours, last 7 days.



The default display is bar-chart style, but it can be toggled to display in table format. To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears.

To manually refresh the data, click the  icon in the upper right corner of the widget. The widget automatically refreshes data every minute.

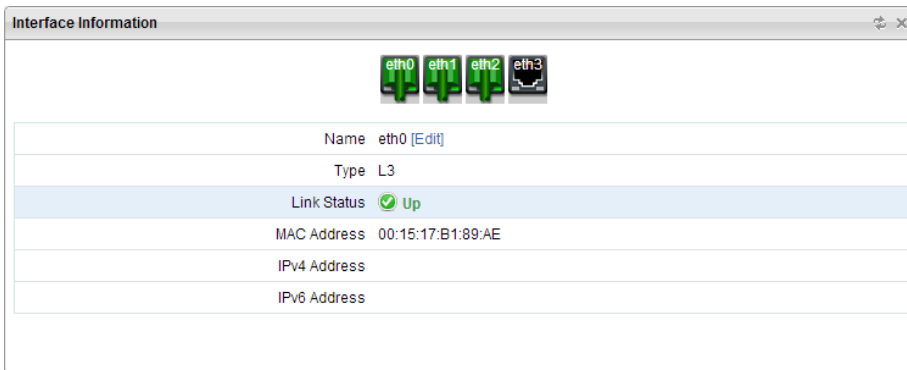
About System Information Widgets

The system information category contains the following widgets:

- [Interface Information Widget on page 5-26](#)
- [System Information Widget on page 5-26](#)
- [System Resource Widget on page 5-27](#)
- [Network Information Widget on page 5-28](#)
- [Pattern Information Widget on page 5-29](#)
- [Hardware Monitor Widget on page 5-30](#)

Interface Information Widget

The **Interface Information** widget shows the interface information of the system. Current status for the interfaces in near real time.

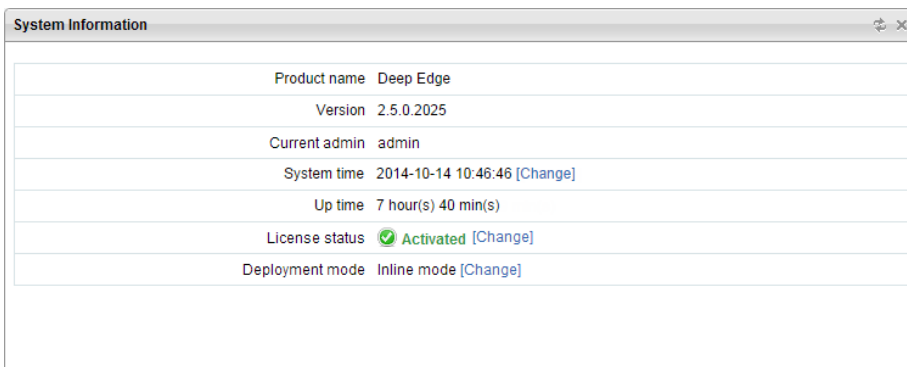


To make changes to the interface, click **Edit** to go to the **Network > Interfaces** screen.

To manually refresh the data, click the  icon in the upper right corner of the widget.

System Information Widget

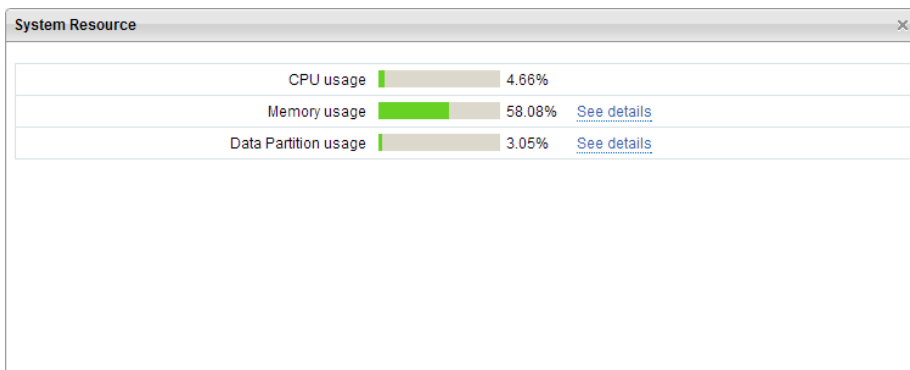
The **System Information** widget shows system related information. System information in near real time.



- Click **Change** by the System time information to go to the **Administration > System Settings** page and update the system time
- Click **Change** by the License status to go to **Administration > License**
- Click **Change** by the Deployment mode to go to **Network > Deployment**

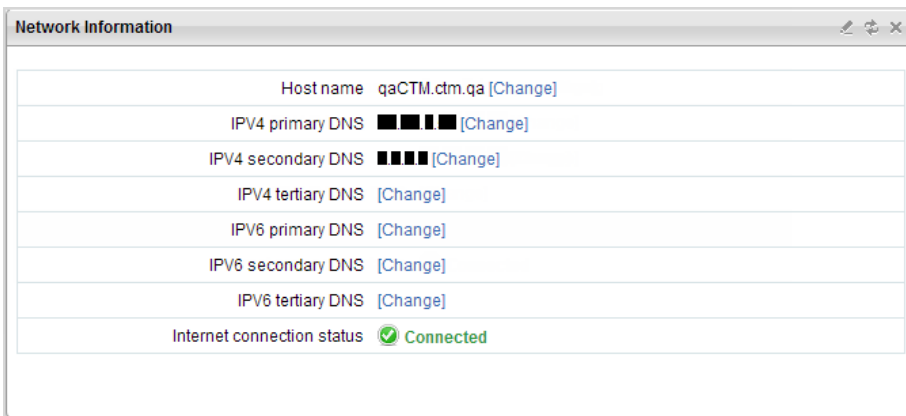
System Resource Widget

The **System Resource** widget shows CPU, memory and data partitions usage information in near real time.



Network Information Widget

The **Network Information** widget shows network-related information, such as system settings related to the network.

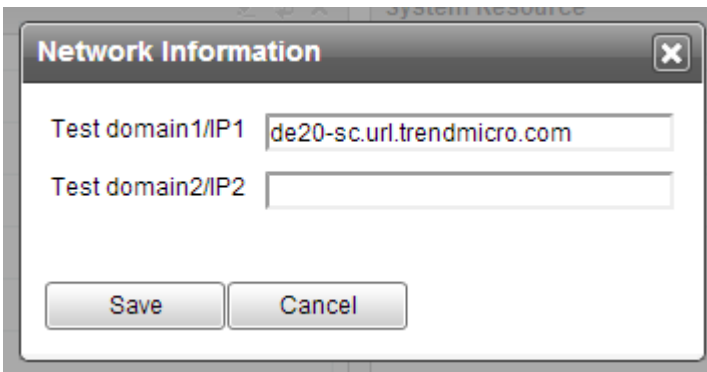


The screenshot shows a window titled "Network Information" with a list of network settings. Each setting has a "Change" link next to it. The settings are:

Host name	qaCTM.ctm.qa	[Change]
IPv4 primary DNS	■■■■■	[Change]
IPv4 secondary DNS	■■■■■	[Change]
IPv4 tertiary DNS		[Change]
IPv6 primary DNS		[Change]
IPv6 secondary DNS		[Change]
IPv6 tertiary DNS		[Change]
Internet connection status	✔ Connected	

Click **Change** to go to the **Administration > System Settings** page and update name or IP address information.

To configure the displayed data sources, click the  icon in the upper right corner of the widget, and then set the widget parameters in the screen that appears. Specify the test domain IP addresses.



The screenshot shows a configuration dialog titled "Network Information" with a close button (X) in the top right corner. It contains two text input fields:

- Test domain1/IP1: de20-sc.url.trendmicro.com
- Test domain2/IP2: (empty)

At the bottom, there are two buttons: "Save" and "Cancel".

**Note**

By default, the test domain is the Trend Micro domain: `de20-sc.url.trendmicro.com`

If this test domain is down, the Internet connection status shown in the **System Resource** widget may show “Disconnected” when in fact it is connected.

To manually refresh the data, click the  icon in the upper right corner of the widget.

Pattern Information Widget

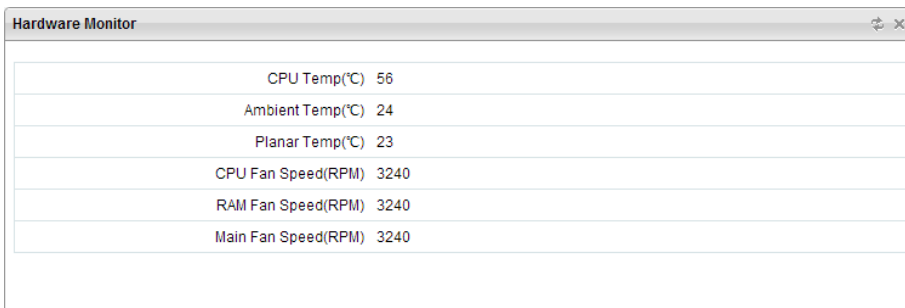
The **Pattern Information** widget shows the latest pattern for each component. Click **View** next to any component to go to the **Component Updates** screen. For details about updating components, see [Updateable Program Components on page 7-2](#).

Pattern Information			 
Anti-Malware Virus Pattern	1.11323.00	[View]	
IPS Pattern	1.14346.00	[View]	
IPS engine	1.0.10	[View]	
Virus scanning engine	9.700.1001	[View]	
Virus scanning engine_64	9.700.1001	[View]	
Virus pattern	10.550.60	[View]	
IntelliTrap exceptions pattern	0.945.00	[View]	
IntelliTrap pattern	0.171.00	[View]	
spyware pattern	1.462.00	[View]	
Spam engine	7.5.1017	[View]	

To manually refresh the data, click the  icon in the upper right corner of the widget.

Hardware Monitor Widget

The **Hardware Monitor** widget shows the temperature and performance of the Deep Edge appliance hardware.



The screenshot shows a window titled "Hardware Monitor" with a table of hardware metrics. The table has two columns: the metric name and its value. The metrics include CPU Temp, Ambient Temp, Planar Temp, and Fan Speeds for CPU, RAM, and Main fans. All fan speeds are 3240 RPM.

CPU Temp(°C)	56
Ambient Temp(°C)	24
Planar Temp(°C)	23
CPU Fan Speed(RPM)	3240
RAM Fan Speed(RPM)	3240
Main Fan Speed(RPM)	3240

When specific events occur, Deep Edge notifies the system administrator with an email message. Configure the system administrator at: **Administration > Notifications > SMTP Settings**. For details about configuring other notifications, go to **Administration > Notifications > Notification Events > Hardware Monitor**.

To manually refresh the data, click the  icon in the upper right corner of the widget.

Analysis and Reports

Deep Edge can generate reports about virus and malicious code detections, files blocked, and URLs accessed. You can use this information about Deep Edge events to optimize network routing settings and fine tune security policies.

Log Analysis

View and analyze logs about bandwidth consumption, how policies control traffic, which sites users access, and whether scan engines protect users from malware, network threats, and other potential harm.

**Note**

To view detailed log information, including examples, see [Detailed Logs on page B-1](#).

Application Bandwidth Logs

View and analyze bandwidth consumption across IP addresses, users, and applications on the network. After reviewing the logs, adjust the allocated upstream and downstream bandwidth to control communications, block unwanted traffic, and allocate the appropriate bandwidth to critical traffic and services.

Policy Enforcement Logs

View and analyze how policies control network traffic. After reviewing the logs, adjust policy rules to allow or filter certain traffic and to troubleshoot improperly configured policies.

Internet Access Logs

View and analyze the websites and domains accessed by specific users. After reviewing the logs, add custom URL categories to filter certain types of traffic and approve or block specific URLs beyond those categories as necessary.

Internet Security Logs

View and analyze how scan engines protect users from malware, network threats, and other potential harm. After reviewing the logs, enable or disable security features and adjust actions, schedules, or user policies to better protect the network.

Log Analysis Interface

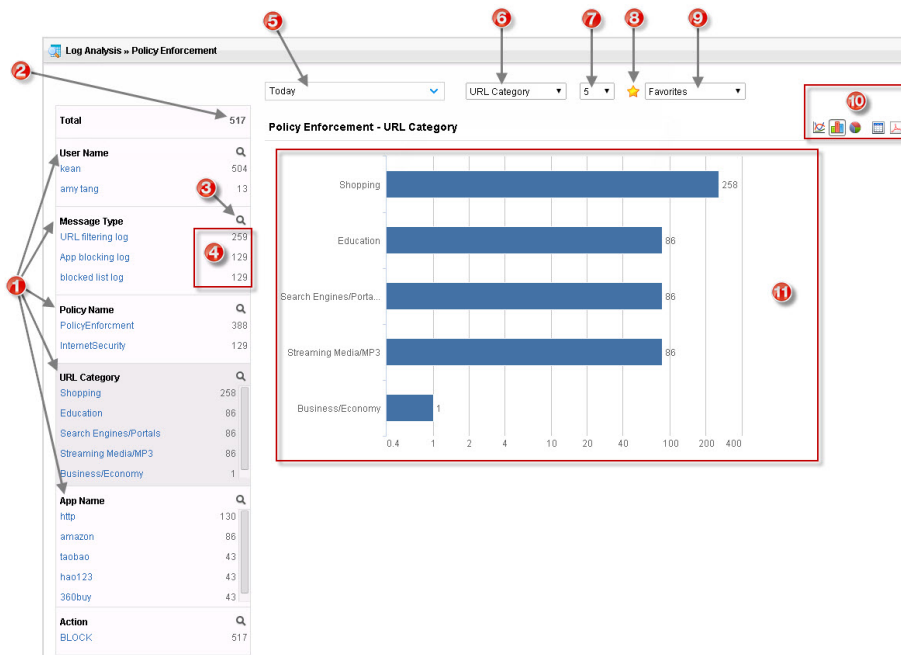


TABLE 5-2. Log Analysis Interface Description

CALL-OUT	DESCRIPTION
1	Click any entity to display its collected logs.
2	View the total number of policy violations or detections.
3	Click  and then specify a term to search for a unique log entry.

CALL-OUT	DESCRIPTION
4	View the count for each item. Each log screen represents different log data. • Application Bandwidth: traffic size • Policy Enforcement: policy violations • Internet Access: visits • Internet Security: threats
5	Select the time range to show logs.
6	Select a filtering option for how the logs display.
7	Select the most relevant logs to display. For example, select the top 10 policy violations in Policy Enforcement .
8	Add a new favorite to bookmark the log results for reporting.
9	Select from the saved favorites to view and analyze updated logs.
10	Control the graphical layout. The options include: bar graph, line graph, pie chart, table, and PDF.
11	Analyze log results for specified filters shown in the selected graphical representation.

Log Analysis Menu Options

The following table describes the available menu options to filter and control the **Log Analysis** graphs. Use it to understand the drop-down menus located at **Analysis & Reports > Log Analysis**.

TABLE 5-3. Log Analysis Menu Option Descriptions

MENU OPTION	EXAMPLE	DESCRIPTION
User Name	Joe User	The user consuming traffic or affected by malware.  Note If there is no user name information, the User Name appears as the client's IP address.
Client IP	123.123.123.123	The source or destination IP address for upstream or downstream traffic. Always the source IP address
App Name	Google Picassa, Groupon	The name of the application controlled by policy rules.
Policy Name	Global URL Filtering	The policy name specified by the Deep Edge administrator.
URL Category	Adult/Mature Content	A collection of websites based on the type of hosted content to approve, filter, or block.
Message Type	HTTP Inspection Log, APT detection	The different security violations based on VSAPI, TMASE or other scan engines. To see the options available, go to Policies > Security Settings (IPS, Anti-Malware, Anti-Spam, WRS).
Action	Block, Monitor	The action enforced by a policy after receiving a packet that meets the policy rule criteria.
Domain	www.google.com	The host name of the source or destination IP address.
Malware Name	HTTP_REQUEST_GET_PRORAT_URI	The name of the malware threatening the network.

Log Favorites

Add a log favorite to create a customized log analysis bookmark for future reference. Use favorites to include this information in custom reports. Go to **Analysis & Reports > Log Favorites** to search for or delete a log favorite.

Reports

Trend Micro Deep Edge can generate reports about virus and malicious code detections, files blocked, and URLs accessed. administrators can use this information about Trend Micro Deep Edge program events to help optimize program settings and fine tune security policies.

Trend Micro Deep Edge can generate both scheduled or manual reports.

Report Categories

Trend Micro Deep Edge has five report categories available:

- Bandwidth
- Policy Enforcement
- Internet Access
- Internet Security
- Custom Reports

About Manual Reports

Reports are based on log data. Configure Deep Edge to generate manual reports for any of the following time sequences:

- On demand (in near real-time)
- Once
- Daily

- Weekly
- Monthly

Generating Manual Reports

Purpose: Generate manual reports.

Location: Analysis & Reports > Reports

Procedure

1. Select the preferred "On Demand" report templates to run.
 2. Click **Run Now**.
-

About Scheduled Reports

Generate scheduled reports on a one-time, daily, weekly, or monthly basis. Reports are based on log data uploaded from the registered devices.

About Custom Reports

Use custom reports to save "favorite log facets," then when creating a report template, the related "custom report" type can also be added in.

About Report Templates

Use report templates to generate reports at recurring scheduled intervals. The parameters defined in a report template determine the scope and amount of data that shows in the generated report.

About Report Template Settings

Configure the report template setting: data range, frequency, the number of reports to save, and other settings.

Managing Report Templates

Purpose: Manage report templates by adding, editing, duplicating, or deleting existing report templates.

Location: Analysis & Reports > Reports

Procedure

- Open any desired report template you want to change, or click the appropriate button to, copy, delete, or add a report template.
-

Adding/Editing Report Templates

Purpose: Add/Edit report templates by defining the report template name and other settings.

Location: Analysis & Reports > Reports

Procedure

1. Click **Add** or select the item you would like to change and then click **Edit**.
2. Specify a report template name and a short description of the report.
3. Enable or disable the report feature.
4. Indicate the desired report settings including the date range, and the frequency.

If you set **Generate Report** to “On Demand”, the report template will not be scheduled. In all other instances, the report templates are scheduled.

5. To send an email notification when the report generates, enable **Email the report**, and then specify the email addresses of your report recipients as well the subject and content of this email template.

Separate multiple entries with commas.



Important

Makes sure to configure the SMTP server and port information at **Administration > Notifications > SMTP Settings**.

6. Indicate the users from whom you would like reports included, whether all users, specific users or groups, or specific IP addresses or ranges.
 7. Define individual report templates by selecting the appropriate types, formats, and options. If log favorites exist, custom reports can be selected as extra report types as well.
 8. Click **Save**.
-

Deleting Report Templates

Purpose: Deletes multiple report templates.

Location: Analysis & Reports > Reports

Procedure

1. Select the desired report template(s).
 2. Click **Delete**.
-

Duplicating Report Templates

Purpose: Duplicate multiple report templates.

Location: Analysis & Reports > Reports

Procedure

1. Select the desired report template(s).
2. Click **Copy**.

3. Click **OK** to confirm.
-

Log Settings

Go to **Analysis & Reports > Log Settings** to configure the global settings which apply to all logs, including:

Log Options

Select the profiles to log and enable Internet access statistics logging.

Log Management

Purge logs after a specified number of days or when the log size increases to a certain threshold.

Syslog Server

Enable syslogs and syslog forwarding.

Configuring Global Log Settings

Procedure

1. Go to **Analysis & Reports > Log Settings**.
2. Under **Log Options**, set the following parameters:
 - a. Select the violation types to log.



Note

Enable violation logs for additional information about traffic activity or for troubleshooting. Disabling violation logs may improve performance.

- b. Select **Enable Internet access log** to enable network traffic statistics logging.

**Note**

To capture log data, also enable Internet access logging from the policy rule. For details, see [Adding Policy Rules on page 4-3](#).

Turning on the Internet access log consumes much more storage than the violation logs alone. Use a syslog server to offload the logs from the box to keep logs for a longer period

3. Under **Log Management**, set the following limits as needed:

OPTION	DESCRIPTION
Limit log storage to [x] GB	Default: System defined
Automatically delete logs older than [x] days	Default: 62 days

4. If needed, change the purge value for the number of days to retain logs before deleting logs.

**Note**

Setting the value to less than 62 days may prevent monthly report generation. Setting the value to more than 62 days could cause the accumulated data size to affect performance. Older logs are automatically removed when the logs exceed the size limitation.

5. Under **Syslog Server**, select the **Enable syslog and forward all logs to syslog server** check box, if needed.
- a. Specify the IP address and port number to forward syslogs.
6. Click **Apply**.
-

Device Logs

Deep Edge detects and acts upon security risks according to the policy settings affecting each risk type. These events are recorded in the logs. Log query parameters vary slightly between log types.

Device logs include auditing when an administrator logs on the appliance, system events, and VPN connections.

Audit Logs

Audit log include the following information:

- All the network change/setting events
- All the Administrator change setting events (includes who, change rule, save rule, commit rule)
- VPN user - add/delete/edit or change password
- Manual operation for the AU update/rollback
- Log query shows user, date, and action
- Default time period is the current day
- Time range with current system date, showing current day in range
- All the users with admin roles listed Log results can be sorted by time or user
- Ability to view, print, or export to CSV the generated log

System Event Logs

System event logs include the following information:

- All the Deep Edge service starts/stops/restarts
- All the system restarts/reboots
- AU-related events
- Admin notification events

User interface includes:

- Default the time period is the current day

- Time range loads the current system date and shows the range including the current day
- Log results can be sorted by time
- Ability to view, print, or export to CSV the generated log

Query results include:

- Date time
- Source (service, system, AU)
- Description

VPN Logs

VPN logs for remote access mode include the following information:

- Timestamp
- Start time
- End time
- VPN protocol
- VPN user
- Event (dial in, dial out)
- VPN query input: Time range, user name or blank
- Query result: Date, time, user, event
- VPN and PPPOE debug logs kept for 15 days
- Lists the latest 15 days and downloads the log file from UI
- Ability to view, print, or export to CSV the generated log

Querying Logs

This procedure gives the general process for querying logs.

Procedure

1. Go to **Administration > Device Logs**.
 2. Select one of the following logs to query:
 - Audit log
 - VPN log
 - System Events log
 3. Select a **Time Period** or **Custom Range** by which to filter the log.
 4. Specify the log query parameters.
 5. Click **Query**, **Print**, or **Export to CSV**.
-

Querying the Audit Log

Procedure

1. Go to **Administration > Device Logs**.
2. Click **Audit Log**.
3. Select a **Time Period** or **Custom Range** by which to filter the log.
4. From the right side of the table, click the  icon next to one or more accounts to audit.

The account moves to the left side under **Selected accounts**.

5. To add all accounts, click **Add all** in the upper right corner.

6. Click **Query**, **Print**, or **Export to CSV**.
-

Querying the System Events Log

Procedure

1. Go to **Administration > Device Logs**.
 2. Click **System Events Log**.
 3. Select a **Time Period** or **Custom Range** by which to filter the log.
 4. Click **Query**, **Print**, or **Export to CSV**.
-

Querying the VPN Log

Procedure

1. Go to **Administration > Device Logs**.
 2. Click **VPN Log**.
 3. Select a **Time Period** or **Custom Range** by which to filter the log.
 4. Specify the user name or IP address of the VPN user.
 5. Click **Query**, **Print**, or **Export to CSV**.
-

Chapter 6

Administration

Topics include:

- *System Settings on page 6-3*
- *Device Management on page 6-5*
- *About Notifications on page 6-19*
- *LDAP User Identification on page 6-11*
- *Administrative Accounts on page 6-7*
- *Product License on page 8-3*
- *System Maintenance on page 6-27*
- *Diagnostics on page 6-29*
- *About Deep Edge on page 6-34*
- *Smart Protection Network: Cloud-based Services on page 6-34*

Switching the Language Settings

Deep Edge offers English and Simplified Chinese language support.

Procedure

1. Expand the drop-down list box at the upper right corner of the Deep Edge web console.
 2. Select the appropriate language.
-

Configuring Getting Started Settings

Getting Started helps you complete basic settings to set up the Deep Edge appliance. Run the Wizard for step-by-step required configurations and validation. For details, see [Accessing the Setup Wizard on page 2-2](#).

Getting Started configurations include the following:

- Basic networking settings
 - Deployment mode settings
 - Management interface and proxy settings
 - Access to the Deep Edge documentation
-

Procedure

1. Go to **Administration > Getting Started**.
-

System Settings

Use the **System Settings** page to specify global settings for the Deep Edge appliance, such as the host name and the time and date settings. Other advanced settings include session timeouts and proxy settings.

General System Settings

Go to **Administration > System Settings > General** to configure the Deep Edge host name, time, and location settings.

Configuring Time and Date Settings

Procedure

1. Go to **Administration > System Settings > General** tab.
2. Under **Time Settings**, manually set the time or set the time to sync with the NTP server:
 - To synchronize with the NTP server, select the **Enable NTP Server** check box and add the NTP server IP address.
 - To set the time manually, select the **Set Time Manually** check box, and specify the current time in the time value field in the following format: `yyyy-mm-dd hh:mm:ss`. For example: `2012-01-16 13:03:28`
3. Under **Location Settings**, set the appropriate time zone by selecting the location and city closest to Deep Edge appliance.



Note

Trend Micro maintains location-specific security services. Deep Edge uses the Trend Micro ActiveUpdate service to update to the latest patterns and Web Reputation technology to filter URLs. For example, the China region uses ActiveUpdate and Web Reputation services specific to China. Regions outside of China use ActiveUpdate and Web Reputation for other locations.

4. Click **Apply**.
-

About Console Settings

The Deep Edge web console settings include the following options:

- **Idle Timeout:** Disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using the web console from a PC that is logged into Deep Edge and then left unattended.
- **Certificate:** Browse to and select an SSL certificate for the web console.

Configuring the Web Console Timeout

Procedure

1. Go to **Administration > System Settings > Console Settings** tab.
 2. In the **Idle Timeout** section, set the session timeout as required.
 3. In the **Certificate Settings** section, add the certificate settings.
 - SSL certificate
 - SSL password
 4. Click **Apply**.
-

About Proxy Settings

Configure Deep Edge to use an HTTP proxy server for product updates, license updates, and Web Reputation queries.

Configuring Proxy Settings

Procedure

1. Go to **Administration > System Settings > Proxy Settings** tab.
 2. Select the **Use an HTTP proxy server** check box.
 3. Specify the HTTP proxy server IP address and port number.
 4. If required, specify the user name and password required by the server.
 5. Click **Apply**.
-

Experience Improvement

Select the **Join Experience Improvement** check box to contribute system configuration information to Trend Micro™ to improve this product. No device name or IP information is ever sent to Trend Micro. Trend Micro only acquires information about which features are in use. There is no way for Trend Micro to know how the features are configured.

Device Management

Configure whether specific services (SSH, SNMP) are accessible or not. Device management also provides an access point to the Deep Edge CLI.

Administrative Access

Configure the Deep Edge management interface to allow or block specific types of management services (or traffic) that originates from devices behind the Deep Edge appliance. There are three locations to control administrative access to the Deep Edge appliance:

- Modify device management settings at **Administration > Device Management > Administrative**
- Modify network interface settings at **Network > Interface**
- Modify network bridge settings at **Network > Bridge**

Enabling Management Service (Web Console, Ping, SSH, and SNMP)

Enabling the management services allows remote access. By enabling SNMP support, users can obtain the supported objects information by using an SNMP manager.

Procedure

1. Go to **Administration > Device Management > Administrative Access**.
2. In the field below the table, specify all addresses allowed to access the appliance.



Note

This setting determines the IP address ranges that can remotely access the appliance. Single IP addresses are supported and the '-' symbol can be used as a range mark. Format the IP address and netmask as 192.168.1.1/24. If nothing is specified, all IP addresses are allowed.

3. To enable the **Web Console, Ping, SSH, or SNMP** service for an interface, select the appropriate check box.
 4. Click **Apply**.
-

Configuring SNMP Settings

Procedure

1. Go to **Administration > Device Management > SNMP Settings**.

2. Select the **Enable SNMP** check box .

**Note**

If SNMP management is enabled, users can manage the device using an SNMP manager.

3. Specify SNMP settings.

OPTION	DESCRIPTION
Email address	Specify the email address of the contact.
Location	The location of the contact, such as "China office, IT room."
Community name	Specify the community string required to retrieve information from Deep Edge (default: public).

**Note**

Email address and location information of the appliance contact can be viewed in an SNMP manager. An SNMP manager can only manage the appliance if the Community String specified is a valid v2 community string.

Administrative Accounts

Multiple users can access Deep Edge as administrative users. These users can make configuration changes that are recorded in the audit log. Access rights can also give you the ability to audit what is being changed in Deep Edge. Having additional administrative accounts can be crucial if you must comply with certain government agency or corporate information security standards.

Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console, including creating, deleting, and modifying user accounts.

Displaying the List of Accounts

Procedure

- Go to **Administration > Device Management > Administrative Accounts**.
-

Adding a New Account

All users have the same privileges.

Procedure

1. Go to **Administration > Device Management > Administrative Accounts**.
 2. Click **Add New**.
 3. Specify the user name, password, password confirmation, and an optional description of the user.
 4. Click **Add**.
-

Modifying a User Description or Password

To change an account, delete the administrator completely and then add a new user with the same credentials.

Procedure

1. Go to **Administration > Device Management > Administrative Accounts**.
2. Click the name of the account to modify.
3. Optionally do the following:
 - To change the password, click **Reset**, and type a new password and confirmation.

- To edit the description, edit the text in the description field.
4. Click **Apply**.
-

Deleting an Administrative Account

Procedure

1. Go to **Administration > Device Management > Administrative Accounts**.
 2. Click the **Delete** icon ()
 3. Click **Delete** in the confirmation dialog box.
-

Web Shell

The **Web Shell** tab provides access to the Deep Edge Command Line Interface (CLI) for advanced configuration. It is strongly recommended that a Trend Micro Support representative work with you while using the CLI to avoid configuration errors.

End User Management

Deep Edge controls access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or VPN tunnel, the user must:

- Belong to one of the user groups allowed access
- Correctly specify a user name and password to prove his or her identity, if asked to do so

About General Settings

Define global settings for end user authentication, including:

- User authentication via Local User account or LDAP.
- Deep Edge supports two kinds LDAP Authentication Cache Time to Live (TTL) options:
 - Fixed TTL (first hit)—Cache the last time that the user authenticated. Default: 1 hour
 - Last active TTL (last hit)—Cache the last time that the user interacted with Deep Edge. Default: 2 hours
- LDAP Sync Interval-Sync every (Hours 1-48)—Deep Edge auto-synchronizes user-group mapping from LDAP server periodically. (Default is 24 hours.)

Configuring General Settings

Use general settings to configure global settings for CommonLDAP.

Procedure

1. Go to **Administration > End User Management**
2. Open the **LDAP Server** tab.
3. Under **User Type**, select one of the following options:

OPTION	DESCRIPTION
Local User	Users log on with the credentials configured in Deep Edge. For details, see Local User and Group Management on page 6-14.  Note Select Local User to automatically authenticate VPN users.
LDAP	Users log on using LDAP authentication. For details, see LDAP User Identification on page 6-11.

4. Under **Authentication Cache**, select one of the following:
 - Fixed TTL (hours)
 - Last Active TTL (hours)

See [About General Settings on page 6-9](#).

5. Click **Apply**.
-

Configuring Synchronization Settings

Procedure

1. Go to **Administration > End User Management > General Settings**
 2. Open the **Synchronization** tab.
 3. Use the **Frequency (hours)** to set the LDAP sync interval.
 4. Click **Refresh** to perform a manual refresh of the LDAP servers.
-

LDAP User Identification

Configure how Deep Edge identifies clients to define the scope of HTTP virus scanning, URL filtering, and Application Control policies. The chosen user identification method also determines how security events are traced to the affected systems in the log files and reports.

Deep Edge provides a user identification method that identifies clients by IP address and then applies the appropriate policy.

About LDAP Integration

Deep Edge supports the most common Lightweight Directory Access Protocol (LDAP) vendors: Microsoft and Linux. Using an LDAP server, it is convenient to create user- or group-specific policies with Deep Edge. Event logs, reports, and notifications will use your LDAP hierarchies for user identification.

LDAP Authentication

Use LDAP settings to designate which LDAP servers are integrated with Deep Edge. Deep Edge uses the designated LDAP servers to do the following:

- Authenticate users to be identified in the captive portal
- Use a Domain Controller agent to query the DC event log
- Use a Windows Management Instrumentation (WMI) client query for the administrator account
- Use policy settings and policy matching for user/group policies

To simplify user's configuration for LDAP, Deep Edge offers basic and advanced methods of LDAP authentication.

Configuring LDAP Authentication Settings

Procedure

1. Go to **Network > DNS** to ensure that DNS is correctly configured.
2. Go to **Administration > End User Management > LDAP Settings**.
3. Click the **LDAP Server** tab.
4. Select one of the following options:

OPTION	DESCRIPTION
Basic	Specify the Domain name , User name , and Password . For details, see Basic LDAP Authentication on page 6-13 .
Advanced	Specify the authentication server, add LDAP servers, and select the authentication method. For details, see Advanced LDAP Authentication on page 6-13 .

5. Click **Test LDAP Server Connection**.
 6. Click **Apply**.
-

Basic LDAP Authentication

Deep Edge provide simple LDAP configuration for the most widely used LDAP service: MS Active Directory (AD). If you use AD, they input the basic information into the web console to configure the user identification method: domain name, user name, and password.

With this information, Deep Edge uses the AD auto-discover tool to obtain the necessary information, including:

- LDAP servers addresses
- Base Domain Name
- Authentication information (Kerberos Realm/domain/KDC)

That information populates the **Advanced LDAP Authentication** fields. If an Administrator decides that the auto-discovered result is incorrect or does not work, the Administrator can switch to Advanced Mode and modify the settings.

For LDAP server addresses, the auto-discovery tool determines all of the Domain Controllers for the domain, and Deep Edge selects and uses the two fastest servers.

Advanced LDAP Authentication

Deep Edge provides an advanced authentication mode configuration for users familiar with LDAP.

Deep Edge supports the following LDAP server types:

- MS Active Directory
- OpenLDAP

For server relationships, Deep Edge only supports “fail-over” for the previously mentioned these servers. If authentication against the primary server fails, Deep Edge will attempt to authenticate against a secondary server.



Note

Deep Edge only supports multiple LDAP servers in same domain for fail-over. Deep Edge does not support multiple domains for different LDAP servers.

For LDAP authentication method, Deep Edge supports the following LDAP authentication methods for both MS Active Directory and OpenLDAP:

- Simple
- Kerberos

For both Basic and Advanced Modes, click the **Test Connection** button to verify the ability to authenticate against the configured LDAP servers, and to report the results.

Local User and Group Management

Local user and group management is mechanism to allow for authentication (and the associated user identification policy rules) when an organization does not use Active Directory or LDAP authentication. For details about LDAP authentication, see [LDAP User Identification on page 6-11](#).

For details about user identification policies, see [About Authentication on page 4-72](#).

For details about configuring the captive portal for user authentication, see [About Captive Portal on page 4-74](#).

Configuring Local User Account Authentication

Procedure

1. Create the local user accounts.
See [Adding a Local User on page 6-15](#).
2. Configure the address objects.
See [Configuring Address Objects on page 3-11](#)
3. Set the user identification policy rules.
See [Adding Authentication Rules on page 4-73](#)
4. Enable the Deep Edge web console on the interface that is part of the internal network.

See [Enabling Management Service \(Web Console, Ping, SSH, and SNMP\) on page 6-6](#).

5. Configure DNS settings.

See [Configuring DNS Settings on page 3-8](#).

**Note**

A DNS server must exist in the internal network for local users to authenticate.

Local Users

Once the local user accounts are created, go to [User VPN on page 3-58](#) to configure User VPN rules.

Adding a Local User

Procedure

1. Go to **Administration > End User Management > Local User**.
2. Click **Add New**.
3. To allow the user to log on, select **Enable user**.
4. Specify the following details:
 - User name
 - Alias
 - Email address
 - Password
 - Description



Note

A strong password is required for every user. The Local User account can also be used for VPN through the web service from an external interface.

5. Specify group membership.

See *Local Groups on page 6-18*

6. Click **OK**.
-

The local user is added.

Editing a Local User

Procedure

1. Go to **Administration > End User Management > Local User**.
 2. In the **User Name** column, click the user name of the local user account to edit.
 3. Make appropriate changes.
 4. Click **OK**.
-

The local user is edited.

Deleting a Local User

Procedure

1. Go to **Administration > End User Management > Local User**.
 2. Select the check box next to the local user account.
 3. Click the **Delete** icon ().
 4. Click **Delete** in the confirmation dialog box.
-

The local user is deleted.

Importing Local Users From a File

Deep Edge Local User import accepts comma-separated value (CSV) files in the following format:

User name, Alias, Email address, Group, Description, Enable, Password



Note

A strong password is required for every user. The Local User account can also be used for VPN through the web service from an external interface.

Separate each new Local User with a line break.

Procedure

1. Go to **Network > User Management > Local User >** tab.
2. Click **Import**.
The **Import Users** window appears.
3. Optional select whether to clear all existing users and groups.
4. Click **Browse** and select the properly-formatted CSV file.

All accounts in the CSV file are imported as local users.

Exporting Local Users to a File

Procedure

1. Go to **Network > User Management > Local User >** tab.
 2. Click **Export**.
-

All local user accounts are automatically downloaded in a comma-separated value (CSV) file to the location specified by the browser.

Local Groups

Adding a Local Group

To add or edit local group, either add a new local user account or open an existing local user account.

Procedure

1. Go to **Administration > End User Management > Local User**.
2. Either click an existing local user account or click **Add New**.
3. In the **Groups** section, select the check box next to the group to delete.
4. Specify or change the group details.
5. Click **Apply**.

The local group is added.

Editing a Local Group

To add or edit local group, either add a new local user account or open an existing local user account.

Procedure

1. Go to **Administration > End User Management > Local User**.
2. Either click an existing local user account or click **Add New**.
3. In the **Groups** section, click the name of the group to edit.

The **Edit Group Properties** window appears.

4. Specify or change the group details.
 5. Click **Apply**.
-

The local group is edited.

Deleting a Local Group

Procedure

1. Go to **Administration > End User Management > Local User**.
 2. Either click an existing local user account or click **Add New**.
 3. In the **Groups** section, click the name of the group to edit.
The **Edit Group Properties** window appears.
 4. Click the **Delete** icon ()
 5. Click **Delete** in the confirmation dialog box.
-

The local group is deleted.

About Notifications

The Notifications section allows the user to configure notifications for the following events:

- Security violations
- Hardware monitoring
- System resource warnings
- Status after a successful or unsuccessful update

Use the **SMTP Settings** tab to configure SMTP notifications (SMTP server name, sender, recipient). For details about configuring SMTP notifications, see [SMTP Settings for Notifications on page 6-24](#).

System Notifications and Alerts

Deep Edge supports email system notifications (alerts) for security-related events for: firewall, Web Reputation Service (WRS), Malware, Intrusion Protection Services (IPS), URL Filtering, and Application Control violations. Email notifications can also be sent to warn of hardware failures such as a rise CPU temperature, fan speed, or any chassis intrusion.

Configure the following notifications:

- Trend Micro Deep Edge security violations
- Trend Micro Deep Edge hardware monitoring
- Trend Micro Deep Edge system resource warnings
- Trend Micro Deep Edge schedule updates

Configuring Notifications for Security Violations

Procedure

1. Go to **Administration > Notifications**.
2. Click **Security Violation**.
3. Check the **Enable** check box to enable the notification.
4. Specify the following information:
 - **Limit 1 notification per:** Select **1 hour, 6 hours, 12 hours, or 24 hours**, depending on how frequent to receive notifications.
 - **Email from:** Specify the email address from which the notification should display that it is sent.

- **Email to:** Specify the email address where the notification should be sent.

5. Click **Apply**.

Configuring Notifications for Hardware Monitoring

Procedure

1. Go to **Administration > Notifications**.
2. Click **Hardware Monitor**.
3. Check the **Enable** check box to enable the notification.
4. Specify the following information:

OPTION	DESCRIPTION
Email from	Specify the email address from which the notification should display that it is sent.
Email to	Specify the email address where the notification should be sent.
Limit 1 notification per	Select 30 minutes , 1 hour , 4 hours , or 12 hours , depending on how frequently you should receive notifications.
Security Events	Select one or more of the events that should trigger a notification: • CPU Temp • Ambient Temp • Planar Temp • Fan Speed
Threshold Usage	For each selected event, select the percentage of the threshold that should trigger a notification. The defaults values are: • CPU Temp: 80°C

OPTION	DESCRIPTION
	• Ambient Temp: 40°C • Planar Temp: 40°C • Fan Speed: 5500 rpm

5. Click **Apply**.
-

Configuring Notifications for System Resource Warnings

Procedure

1. Go to **Administration > Notifications**.
2. In the **Notification Events** tab, click **System Resource Warning**.
3. Select **Enable system resource notifications** to enable the notification.
4. Specify the following information:

OPTION	DESCRIPTION
Sender	Specify the email address from which the notification should display that it is sent.
Recipient	Specify the email address where the notification should be sent.
Frequency	Select how often you should receive notifications.
Resource Usage	Select one or more of the resources that should trigger a notification: • CPU • Data partition • Memory
Threshold	For each selected resource, select the percentage of the threshold that should trigger a notification. The defaults percentages are:

OPTION	DESCRIPTION
	• CPU Usage - 90% • Data Partition Usage - 90% • Memory Usage - 90%

5. Click **Apply**.
-

Configuring Notifications for Scheduled Updates

Procedure

1. Go to **Administration > Notifications**.
 2. Click **Schedule Update**.
 3. Select either check box to send a notification for the related update events.
 - **Send notification when system updates successfully**
 - **Send notification when system fails to update**
 4. Specify the email address from which the notification is sent and the email address(es) to which it is sent.

Use commas to separate multiple addresses.
 5. Click **Apply**.
-

Stopping Notifications

Procedure

1. Go to **Administration > Notifications**.
2. Click the name of the notification to stop.

3. Deselect the **Enable** check box to disable the notification.
 4. Click **Apply**.
-

SMTP Settings for Notifications

To generate email messages for security violations, system resource warnings, or scheduled update log entries, make sure to specify the email settings. After defining the email settings, enable email notification as shown in [System Notifications and Alerts on page 6-20](#)

Configuring SMTP Settings for Notifications

Email settings used in any system settings, configuration log settings, or logging profiles cannot be deleted.

Procedure

1. Go to **Administration > Notifications > SMTP Settings**.
2. Specify the following:
 - **SMTP Server name and port number:** Specify the IP address or host name and port number of the Simple Mail Transport Protocol (SMTP) server used to send the email.
 - **Email from:** Specify the “From” email address, such as “security_notification@company.com.”
 - **Email to:** Specify the email address of the recipient.
3. Click **Test SMTP Server Connection**.

You receive two confirmations. One says the connection was successful. The second says the settings were successfully applied.

4. If not testing the connection, click **Apply** to save the new settings.
-

Product License

The Product License function allows organizations to register and license Deep Edge. Fully activating Deep Edge is a two-step process. First, register Deep Edge with Trend Micro. After registering, a valid Deep Edge Activation Code (AC) is provided to license the product.

For more information about updating and maintaining the product license, see [Keeping Updated on page 7-1](#).

Updates

New malicious programs and offensive websites are developed and launched daily. Deep Edge has several methods to stay up-to-date. From the Deep Edge web console, go to **Administration > Updates** for updates about the latest pattern files and software patches to keep Deep Edge protected.

For more information about updating Deep Edge product components, see [Keeping Updated on page 7-1](#).

Device Logs

Deep Edge detects and acts upon security risks according to the policy settings affecting each risk type. These events are recorded in the logs. Log query parameters vary slightly between log types. Log settings for enabling logs, log retention duration, and syslog forwarding are configurable.

Device logs include auditing when an administrator logs on to Deep Edge, system events, and VPN connections. For more information about analyzing device logs, see [Device Logs on page 5-40](#).

Mail Quarantine

The quarantine query is used for mail exporting, deleting, and resending. When a message matches a policy and the action is Quarantine, Deep Edge moves the message

to the quarantine area. To prevent negatively impacting performance, you must set proper constraints for keeping quarantined message storage low. A manual purge function is provided.

Querying the Mail Quarantine

If the **Quarantine** action was selected for spam email messages, those message are moved to the quarantine area. It is possible to query all quarantined messages.

Procedure

1. Go to **Administration > Mail Quarantine > Query**.
2. Set the following search filters as needed:
 - **Time period** or **Custom Range**
 - **Protocol**
 - **Status**
 - **Quarantine Reason**
 - **Sender, Recipient, or Subject**
3. Click **Query**.
4. In the returned results, click the icon in the **Details** column for more information about a particular message in quarantine.
5. Do one of the following:
 - Resend the email message if needed.



Note

If no resend SMTP server is configured, then the email message is resent to the original IP address when quarantined. For information about configuring the SMTP resend server, see [Configuring Mail Quarantine Settings on page 6-27](#).

- Delete the email message if it is not needed.

- Export the email message to the appropriate user, if the downstream mail server is not available.
-

Configuring Mail Quarantine Settings

Designate the quarantine storage size and the purge frequency. Resend settings for the SMTP mail server can also be enabled and configured.

Procedure

1. Go to **Administration > Mail Quarantine > Settings**.
2. Specify the size (in GB) of the quarantine area. (Default: 4 GB)
3. Specify the number of days to retain quarantined messages. (Default: 10 days)



Note

The quarantine area can be purged by size or date.

4. Enable the SMTP server used to resend email messages, if needed.
 5. Specify the SMTP server IP address, port, and authentication credentials.
 6. Click **Apply**.
-

System Maintenance

Use the **Maintenance** page to shutdown and restart Deep Edge, and back up and restore configurations.

For more details about maintenance, see [Product Maintenance on page 8-1](#).

Performing System Maintenance

Deep Edge provides system maintenance functionality.

**WARNING!**

Applying system maintenance actions disconnects all users.

Procedure

1. Go to **Administration > Maintenance > System Maintenance** tab.
 2. Select the appropriate option:
 - **Shutdown**—Stops services, shuts down the appliance, and powers off.
 - **Restart**—Stops services and restarts the appliance.
 - **Restore to factory settings**—Restores the original hardware box settings to the appliance.
 3. Under **Message**, optionally specify a message (up to 100 characters) to accompany the event in the log.
 4. Click **Apply**.
-

Configuration Backup and Restore

Use the **Backup/Restore** tab at **Administration > Maintenance** page to:

- Create a backup file of existing configuration settings
- Restore configuration settings from a backup file

Backing Up the Current Configuration

Deep Edge configuration back ups can be restored after a patch has been applied.

Procedure

1. At the web console, go to **Administration > Maintenance > Backup/Restore**.
2. Under **Backup Configuration**, click **Create a Backup**.

The backup file downloads.

The current Deep Edge configuration is now saved.

Restoring the Previous Configuration

A previous Deep Edge configuration can be restored after a system failure or upgrade.

Procedure

1. At the web console, go to **Administration > Maintenance > Backup/Restore**.
 2. In the **Restore Configuration** section, click **Browse**.
A **Open** dialog box appears.
 3. Navigate to the folder with the stored the backup file, select the file, and then click **Open**.
 4. Click **Restore**.
-

The Deep Edge configuration backup is restored. You are now ready to make further configuration changes or begin using Deep Edge.

Diagnostics

Use the Deep Edge's diagnostic tools to:

- Run network packet captures for traffic debug and analysis.
- Determine the route taken by packets across an IP network.
- Create a case diagnostic file for Trend Micro technical support.

Packet Capture

The Packet Capturing wizard is located at **Administration > Diagnostics > Packet Capture**. Use the captured packet to perform traffic debug or analysis.

Choose a single or multiple network interfaces on which to simultaneously capture network packets. After the capture starts, the elapsed time displays. The capture operation stops when the administrator clicks **Stop capture** or when the configured time or size criteria is met.

The packet capture for each interface saves as an individual file using the naming convention of “capture-{interface}-{date:time}.pcap”. For example capture-eth0-2013-07-02.1329518492.75.pcap.tar.gz would be the file name for the packet capture on the eth0 network interface performed on July 2, 2013.

After the network packet capture completes, all packet capture files are saved in one compressed package file named to “capture-{date}.tgz”. This file displays in the downloadable list. Either download or delete the compressed file.

To determine some of the components for the filter, run a packet capture on the HTTP requests or responses. See the sample capture in [Figure 6-1: Packet capture for a Google](#)

search on page 6-31 and the explanation in *Table 6-1: Components shows in the packet capture on page 6-31.*

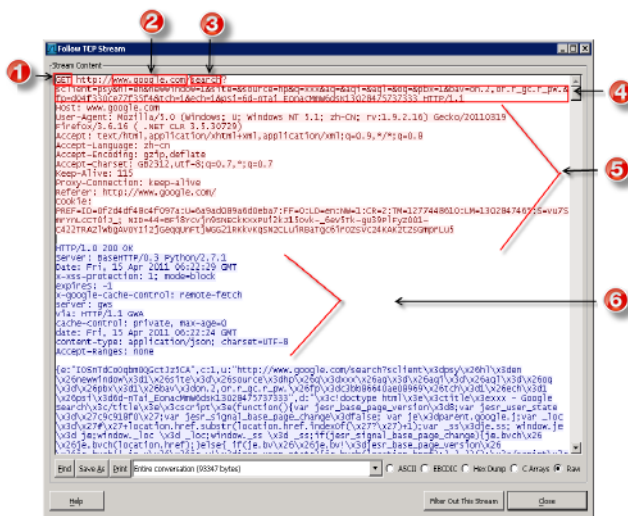


FIGURE 6-1. Packet capture for a Google search

TABLE 6-1. Components shows in the packet capture

CALL-OUT	COMPONENT
1	Request method
2	URL host
3	URL path
4	URL query
5	Request header
6	Response header

Capturing Network Packets

Capture packets to analyze traffic on selected interfaces or a single interface.

Procedure

1. Go to the **Administration > Diagnostics** and click **Packet Capture**.
2. Select the appropriate interface(s) from the **Interface** column.
3. Complete the following fields:

- Specify IP address on which to capture packets
- Specify a port on which to capture packets
- **Size Limit (MB)** (Default: 500MB)
- **Timeout (minutes)** (Default: 30 minutes)

4. Click **Start Capture**.

The elapsed time displays. The capture stops when the maximum files size of 500MB is reached, unless a smaller size was configured for the **Capture packet limit (MB)** option.

5. If necessary, click **Stop Capture** to stop the packet capture before reaching the maximum file size.
 6. When the capture finishes, check the check box of the captured file and select an action:
 - Click the icon in the **Action** column and open or the capture file.
 - Click the **Delete** icon to delete the selected generated files.
-

Traffic Tracing

Use traffic tracing to generate detailed session information to help diagnose any problems with an application. This network tool determines the route taken by packets across an IP network.

Procedure

1. Go to **Administration > Diagnosis > Traffic Tracing**.
 2. Specify the **IP address** and **port** from which traffic will be traced.
 3. Select the action to trace from the **Action** drop-down list box: **All**, **Allow**, or **Block**.
 4. Click **Start**.
 5. Click **Stop** to stop the trace.
 6. View the results under the **Captured Sessions** section. Click a session to see session details.
-

Generating Diagnostic Files

The Trend Micro Case Diagnostic Tools (CDT) uses diagnostic files to create a file that helps Trend Micro Technical Support diagnose problems with an appliance.

Procedure

1. Go to **Administration > Diagnosis > Diagnostic Files**.
 2. Click **Generate Diagnostic Files**.
-

Support

To get support information from the web console, go to **Administration > Support**. For additional troubleshooting, maintenance, and support information, see [Technical Support on page A-1](#).

About Deep Edge

The **Administration > About** page provides product version and license agreement information.

Smart Protection Network: Cloud-based Services

Smart Protection Network (SPN) is the industry's highest performing cloud-based malware protection service. Smart Protection Network has the following malware detection components:

TABLE 6-2. SPN Services

SERVICE	DESCRIPTION
Web Reputation Services (WRS)	Comprised of several correlated services providing proactive detection and blocking against known bad websites, domains, files and objects, as well as email-related items - including anti-pharming and anti-phishing detection. • Domain reputation • Page reputation • Email reputation • File reputation
URL Filtering Service	Stores a URL database in the cloud for rapid updates and protects Trend Micro's global user base without the must download and update URL database files on the Deep Edge server. This provides up-to-date URL information to every customer and accelerates the proactive protection capabilities to reduce the time between the discovery of a bad site and the time it is added to the URL database to protect all customers.

SERVICE	DESCRIPTION
Feedback Loop	Provides real-time information from all of Trend Micro's products to update the SPN cloud-based components and URL filtering databases. Malware detected on customer equipment are fed back into the cloud architecture and used to fine-tune information in real time. This provides fast proactive protection with low false positives to Trend Micro's global customer base.

DNS Best Practice Suggestions

Smart Protection Network (SPN) uses cloud-based services and relies on DNS queries for lookups. To ensure fast response and minimum latency, the Deep Edge device must be configured with a DNS server. You can set up to three DNS servers.

The DNS servers must be able to support the volume of DNS requests made by Deep Edge. In general, before Deep Edge builds up its local DNS cache, two DNS requests will be made for each URL accessed. Make sure your DNS server is installed on a server with enough resources and performance to handle the extra DNS volume.

To reduce latency, each DNS server should have a fast network card and be installed on a fast network switch.

Trend Micro recommends on-site DNS servers versus ISP-provided DNS servers that are housed outside of the company's network. In general, ISP DNS servers have higher latency and do not support large numbers of DNS queries from a single IP address. Many ISP DNS servers have throttling mechanisms that limit the number of DNS requests per second and can affect Deep Edge's Web Reputation Services (WRS) performance.

To improve network response time and performance, try to place the DNS server as close to the Deep Edge unit(s) as possible to eliminate unnecessary network hops between the devices.

WRS and URL Filtering requests are made over HTTP port 80. Do not block the Deep Edge management IP address for these ports on the firewall.

Chapter 7

Keeping Updated

New malicious programs and offensive websites are developed and launched daily. Deep Edge has several methods to stay up-to-date. From the Deep Edge web console, go to **Administration > Updates** for updates about the latest pattern files and software patches to keep Deep Edge protected.

Topics include:

- *Updateable Program Components on page 7-2*
- *ActiveUpdate on page 7-6*
- *Manual Updates on page 7-8*
- *Scheduled Updates on page 7-11*

Updateable Program Components

To ensure up-to-date protection against the latest risks, there are several pattern files components you can update.

These files contain the binary “signatures” or patterns of known security risks. Deep Edge uses them to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the protocol and IPS pattern files are updated less frequently.

Anti-Malware Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly pernicious risk is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature (see [ActiveUpdate on page 7-6](#) for details) can detect whenever a new virus pattern is available at the server, and can be scheduled to automatically poll the server every hour, day, week, and so on, to get the latest file.

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (typically several times per week), and recommends configuring a hourly automatic update on the **Administration > Updates > Components Updates** screen. Updates are available to all Trend Micro customers with valid maintenance contracts.



Note

There is no need delete the old pattern file or take any special steps to “install” the new one.

Anti-Malware Protocol Pattern File

The Network Content Inspection Engine (NCIE) uses the anti-malware pattern file to perform network scanning.

C&C Contact Information Pattern

Command & Control (C&C) Contact Information Pattern provides Deep Edge with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.

IPS Pattern and Engine

Deep Edge uses the IPS pattern file and engine to block IPS vulnerabilities. If a comparison between patterns suggests that a network connection has a vulnerability, Deep Edge proceeds with the configured action.

Virus Scan Engines and Pattern

The virus scan engine analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.

IntelliTrap Pattern and Exceptions

IntelliTrap detection uses a scan option in the Trend Micro's virus scanning engine with IntelliTrap pattern (for potentially malicious files) and IntelliTrap Exception pattern (as an allowed list). Deep Edge uses the IntelliTrap option and patterns available for detecting malicious compressed files, such as bots in compressed files. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides a heuristic evaluation of compressed files to help reduce the risk that a bot or any other malicious compressed file might cause to a network.

Spyware Pattern

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the spyware/grayware pattern file.

Anti-Spam Pattern and Engine

The spam pattern helps Deep Edge identify the latest spam in messages and attachments. The anti-spam engine detects spam in messages and attachments.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web Reputation Services assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

URL Database

The URL database resides in the cloud with other Trend Micro™ Smart Protection Network™ servers. When a user attempts to access a URL, Deep Edge retrieves information about this URL from the database and stores it in the local cache. Having the URL database in the cloud and building the local cache with this database information reduces the overhead on Deep Edge and improves performance.

Information retrieved for a requested URL that passes through Deep Edge includes:

- Web category used with URL Filtering policies to control access to web sites.
- Web Reputation score used to block URL access based on a specified sensitivity level (See [Configuring WRS Profiles on page 4-54.](#))

The URL database is updated with the latest categorization and reputation of web pages on a real-time basis to provide the most up-to-date information about any URL an end-user might try to visit.

If the reputation of a URL is believed to be misclassified or you want to know the reputation of a URL, use the link below to notify Trend Micro:

<http://SiteSafety.trendmicro.com>

Email Reputation Database

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Email Reputation filters spam by blocking the IP addresses stored in this database.

By default, anti-spam profiles in Deep Edge use Email Reputation, which is a Smart Protection Network™ component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Incremental Updates of the Pattern Files

ActiveUpdate supports incremental updates of the latest pattern files. Rather than downloading the entire file each time, ActiveUpdate can download only the new portion of the file and append it to the existing file. This efficient update method can substantially reduce the bandwidth needed to update the antivirus software or deploy pattern files throughout the environment.

Component Version Information

To know which pattern file or application build is running, click **Dashboard** in the main menu. The application version in use is shown in the **System Information** widget. The **Pattern Information** widget shows the pattern version. (If either widget is not displayed, click **Add Widgets** and add the needed widget(s) to the Dashboard.)

Component version information is also available at **Administration > Updates > Component Updates**.

ActiveUpdate

Deep Edge uses ActiveUpdate, the Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, spyware or grayware pattern files. ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of the latest pattern files and engines. ActiveUpdate does not interrupt network services, or require endpoints to reboot. Updates are available on a regularly scheduled interval or on demand.

About Updating from the Web Console

Deep Edge polls the ActiveUpdate server directly. Updated components are deployed to Deep Edge on a schedule that you define, such as the following:

- Hourly
- Weekly
- Daily
- On demand (manually)



Note

Trend Micro recommends daily updates of the pattern files.

Configuring Proxy Settings for Updates

If a proxy server is used to access the Internet, specify the proxy server information using the Deep Edge web console before attempting to update components. Specified proxy information is used for the following:

- Updating components from Trend Micro's update servers

- Product registration and licensing
- Web reputation queries

Procedure

1. From the Deep Edge web console, go to **Administration > System Settings > Proxy Settings**.
2. Select **Use HTTP proxy server (for system updates, license updates, and others)** to specify a proxy server or port.
3. If the proxy server requires authentication, select the check box and specify a user ID and password.



Note

Leave these fields blank if the proxy server does not require authentication.

4. Click **Apply**.



Note

In bridge mode, the Deep Edge has an internal interface and an external interface. To ensure updates function properly, the configuration of the ActiveUpdate proxy and server settings must be done on the same side. If Deep Edge is deployed with other proxy servers, the next hop proxy settings for the ActiveUpdate proxy and server should be the same server on the same side of the interface.

Selecting the Update Source

Procedure

1. Go to **Administration > Updates**.
2. Click the **Components** tab.
3. Under **Source**, select the update source.

- **Trend Micro ActiveUpdate server**

Select this option to automatically receive updates from ActiveUpdate.

- **Other Internet source**

Select this option to specify the URL of your own update source.

4. Click **Apply**.
-

Manual Updates

The effectiveness of Deep Edge depends upon using the latest pattern files. Signature-based virus scanning works by comparing the binary patterns of scanned files against binary patterns of known risks in the pattern files. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks. Similarly, new versions of the Phish pattern are released as new phishing URLs are identified.

Applying a Software Patch

After downloading the product patch and optionally backing up the current configuration, apply the update to Deep Edge.

The manual update feature is also useful when a pattern file is corrupted and must be downloaded again from the update server.

Procedure

1. Download the patch.

Contact Trend Micro Technical Support for information about available patches.

2. At the web console, go to **Administration > Updates > Software Patches**.

3. Under **Select a Patch to Install**, click **Browse**.

A **Open** dialog box appears.

4. Navigate to the folder with the downloaded file, select the file, and then click **Open**.
5. Click **Upload**.

You are ready to restore the configuration that was previously saved or begin a new configuration.

What to do next

Follow the patch on-screen instructions to apply the patch.

Updating Components

No components are updated if Deep Edge is already using the latest version of the components.

Procedure

1. Go to **Administration > Updates**.
2. Click the **Component Updates** tab.
3. Select some or all of the components to be updated and click **Update Now**

The **Availability** column shows whether a component has a new version available.

A message box appears if the version of the pattern file on Deep Edge is greater than or equal to the counterpart on the remote download server. If the pattern file on Deep Edge is older than the one on the remote download server, the newer pattern file is downloaded.

Verifying a Successful Update

The **Dashboard** screen of the Deep Edge web console displays the version of the component in use in the Pattern Information widget.

Procedure

1. Go to **Administration > Updates > Component Updates**
 2. Verify that a manual or scheduled update has completed successfully.
-

About Update Maintenance

Deep Edge helps maintain updates in two ways. It helps you know when the last update occurred, offers notifications about upcoming updates, and allows you to roll back to previous versions of software and components.

See more at:

- [*Verifying a Successful Update on page 7-9*](#)
- [*Update Notifications on page 7-12*](#)
- [*Rolling Back an Update on page 7-10*](#)

Rolling Back an Update

Deep Edge checks the program directory and uses the latest pattern file to scan inbound/outbound traffic. Occasionally, a new pattern file might incorrectly detect a non-infected file as a virus infection (known as a “false positive”). If necessary, revert to the previous pattern file.

Procedure

1. Go to **Administration > Updates > Component Updates**
2. Select the component(s) to roll back and click **Roll back**.
3. Click **OK** to confirm the rollback.

A progress bar indicates the rollback progress, and a message screen then displays the outcome of the rollback. After the rollback, find the current version on the Dashboard screen in the Pattern Information widget.



Note

The **Pattern Information** widget does not display by default. See more about adding widgets at: [Adding New Widgets on page 5-7](#).

Scheduled Updates

Deep Edge can schedule updates for any product component listed at [Updateable Program Components on page 7-2](#).



Note

Updates cannot be scheduled for software patches.

Scheduling Component Updates

Procedure

1. Go to **Administration > Updates > Component Updates**.
2. For each type of component, select the update interval.

OPTION	DESCRIPTION
Hourly	Schedule updates to run every hour at 00, 15, 30, or 45.
Daily	Schedule updates to run at a specific time every day. (Default)
Weekly	Schedule updates to run at a specific day and time every week.

3. Click **Apply**.

**Note**

Use **Dashboard > Pattern Information** in the Deep Edge web console to verify the current version of a pattern file. If the network configuration includes a cache server, Trend Micro recommends clearing the cache and rebooting the cache server after updating the pattern files to force scanning all URL requests, ensuring better network protection. Consult the cache server documentation for information about clearing the cache and rebooting the server.

Update Notifications

Deep Edge can issue notifications to proactively inform you about the pattern or engine update status. For more information about configuring update-related notifications, see [*Configuring Notifications for Scheduled Updates on page 6-23*](#).

Configuring Notifications for Scheduled Updates

Procedure

1. Go to **Administration > Notifications**.
 2. Click **Schedule Update**.
 3. Select either check box to send a notification for the related update events.
 - **Send notification when system updates successfully**
 - **Send notification when system fails to update**
 4. Specify the email address from which the notification is sent and the email address(es) to which it is sent.

Use commas to separate multiple addresses.
 5. Click **Apply**.
-

Chapter 8

Product Maintenance

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees. This chapter explains how to manage your maintain agreement and product license.

Topics include:

- *Maintenance Agreement on page 8-2*
- *Product License on page 8-3*

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

<https://olr.trendmicro.com/registration/>

Renewing the Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which renewal maintenance must be purchased.

If the Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

Procedure

1. To renew the Maintenance Agreement, do one of the following:
 - To purchase renewal maintenance, contact the same vendor from whom the product was purchased. A Maintenance Agreement extending protection for

another year will be sent by post to the primary company contact listed in your company's Registration Profile.

- To view or modify the company's Registration Profile, log on the account at the Trend Micro online registration website: <https://olr.trendmicro.com/registration/us/en-us>
2. To view the Registration Profile, specify the Logon ID and password created when the product was first registered with Trend Micro (as a new customer), and then click **Login**.

Product License

The Product License function allows organizations to register and license Deep Edge. Fully activating Deep Edge is a two-step process. First, register Deep Edge with Trend Micro. After registering, a valid Deep Edge Activation Code is provided to license the product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only.

To activate Deep Edge, obtain a Registration Key during product registration. The Registration Key allows you to obtain an Activation Code. Activate Deep Edge at a later time using the Deep Edge web console.

License Expiration Warnings

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting them of the upcoming discontinuance. Update the Maintenance Agreement by purchasing renewal maintenance from a reseller, Trend Micro sales, or on the Trend Micro Online Registration at: <https://olr.trendmicro.com/registration/>

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solution DVD
- License Certificate (obtained after purchasing the product)

Registering and activating Deep Edge entitles the following benefits:

- Updates to the Deep Edge pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information, and renewal reminders
- Easy access in renewing the license and updating the customer profile

Registration Keys have 18 characters and appear as follows:

XX-XXXX-XXXX-XXXX-XXXX

Registering Deep Edge

Procedure

1. Click the Trend Micro Product Registration Server link in the product at **Administration > License**.
2. Click the **Activate License** link.
3. In the Activation Wizard window, click the **register online** link.
 - **New users:** Click the **Continue** button under **Not registered** and create a new account and click **Submit**.
 - **Returning users:** Specify your Login ID and password.
4. In the **My Products** screen, click **Add Products** and specify the Registration Key.
5. To edit your company profile, click **View/Edit Company Profile**.

The Activation Code appears on the next screen.

6. To receive a copy of the Activation Code at the registered email address, click **Send Now**.

**Note**

For maintenance renewal, contact Trend Micro sales or the reseller. Click **Check Status** at **Administration > License** to manually update the maintenance expiration date on the Product License screen.

Obtaining the Activation Code

When the full version expires, Deep Edge security updates will be disabled; when the evaluation period expires, both the security updates and scanning capabilities will be disabled. Use the **Product License** screen to obtain an Activation Code online, view renewal instructions, and check the status of the product.

To activate Deep Edge, acquire an Activation Code by do one of the following:

- Automatically receive an evaluation Activation Code after downloading Deep Edge from the Trend Micro website.
- Use a Registration Key to obtain an Activation Code online.

Activation Codes have 31 characters and appear in the following format:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX

Updating the License

Procedure

1. To obtain the latest license, go to **Administration > License**.
2. Click **Check Status**.

3. For more renewal instructions, see https://olr.trendmicro.com/registration/us/en-us/instruction_renew.aspx
-

Renewing the Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which renewal maintenance must be purchased.

If the Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

Procedure

1. To renew the Maintenance Agreement, do one of the following:
 - To purchase renewal maintenance, contact the same vendor from whom the product was purchased. A Maintenance Agreement extending protection for another year will be sent by post to the primary company contact listed in your company's Registration Profile.
 - To view or modify the company's Registration Profile, log on the account at the Trend Micro online registration website: <https://olr.trendmicro.com/registration/us/en-us>
 2. To view the Registration Profile, specify the Logon ID and password created when the product was first registered with Trend Micro (as a new customer), and then click **Login**.
-

Appendix A

Technical Support

This appendix describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

- *Troubleshooting Resources on page A-2*
- *Contacting Trend Micro on page A-3*
- *Sending Suspicious Content to Trend Micro on page A-5*
- *Other Resources on page A-6*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

<http://community.trendmicro.com/>

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cyber-security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtual security, and data encryption.

Go to <http://www.trendmicro.com/us/security-intelligence/index.html> to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass endpoint security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://www.trendmicro.com/vinfo> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://ers.trendmicro.com/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<http://esupport.trendmicro.com/solution/en-us/1036097.aspx>

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<http://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

<http://trendedge.trendmicro.com/>

Known Issues

Known issues are features in your the product or software that might temporarily require a workaround. Known issues are typically documented in section 7 of the Readme file. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Download Center:

<http://www.trendmicro.com/download/>

Known issues can be found in the technical support Knowledge Base:

<http://esupport.trendmicro.com>

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

TrendLabs

TrendLabsSM is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

Appendix B

Detailed Logs

This appendix provides detailed information about Deep Edge log data content.

Topics include:

- *Policy Enforcement Logs on page B-2*
- *Application Bandwidth Logs on page B-3*
- *Internet Security Logs on page B-4*
- *Internet Access Logs on page B-6*
- *VPN Logs on page B-8*
- *System Event Logs on page B-9*
- *Audit Logs on page B-11*

Policy Enforcement Logs

LOG ITEM	DESCRIPTION	EXAMPLE
Time	Date and time when recorded	2014-02-11 22:51:00
User Name	The user account if Deep Edge is configured as LDAP or Local User authentication. Otherwise, it will be the Client IP address	Lily Jerry
Message Type	Firewall/URL Filtering/blocked list/App blocking	App blocking log
Group Name	The group name of authenticated user (Default is empty)	English-Club
URL	URL visited by clients, if applicable	u034024.778669.com/
Client IP	Source IP address	192.168.1.101
Server IP	Destination IP address	192.168.1.119 10.64.1.55
Domain	The domain visited by clients, if applicable	www.google.com
URL Category	The URL Category name identified by Deep Edge	Shopping Spyware
App Name	The application name identified by Deep Edge	DNS HTTP Sina Weibo
Action	Block/Monitor	Block
WRS Score	The score of URL queried by WRS, if applicable. The scope is 0 ~ 100. A higher value has a better reputation.	49

LOG ITEM	DESCRIPTION	EXAMPLE
Source Port	Port Number	42074 39199
Destination Port	Port Number	53 80
IPS Rule	The IPS rule name if it is triggered by IPS Scan	--
ERS Category	1 = blocked by ERS; 0 = otherwise	0
Mail Sender	The message traffic mail sender. Default is empty.	--
Mail Receiver	The message traffic mail recipient. Default is empty.	--
Mail Subject	The message traffic mail subject. Default is empty.	--
Transfer Protocol	TCP/UDP/ICMP/ICMPv6	TCP
App Attribute Name	The granular application name	Sina Weibo-Post Message
Policy Name	The security policy name for traffic control	Default known-user

Application Bandwidth Logs

LOG ITEM	DESCRIPTION	EXAMPLE
Time	Date and time when recorded	2014-02-11 22:51:00
User Name	The user account if Deep Edge is configured as LDAP or Local User authentication. Otherwise, it will be the Client IP address	Lily Jerry

LOG ITEM	DESCRIPTION	EXAMPLE
App Name	The application name identified by Deep Edge	DNS HTTP Sina Weibo
Client IP	Source IP address	192.168.1.101
Policy Name	The security policy name for traffic control	Default known-user
In Byte	Inbound Byte	552
Out Byte	Outbound Byte	910

Internet Security Logs

Deep Edge Internet Security logs are categorized by eleven types of violation logs identified by “Message Type”. The following table explains the details of each item in a violation log.

LOG ITEM	DESCRIPTION	EXAMPLE
Time	Date and time when recorded	2014-02-11 22:51:00
Message Type	Anti-malware/Anti-spam/Anti-APT/Anti-DoS/Anti-APT/WRS/IPS/Botnet/C&C Contact Alert/Blocked file extensions/ HTTP Cert Error/Client Cert Error	Anti-Malware
User Name	The user account if Deep Edge is configured as LDAP or Local User authentication. Otherwise, it will be the Client IP address	Lily Jerry
Group Name	The group name of authenticated user (Default is empty)	English-Club
URL	URL visited by clients, if applicable	u034024.778669.com/

LOG ITEM	DESCRIPTION	EXAMPLE
Client IP	Source IP address	192.168.1.101
Server IP	Destination IP address	192.168.1.119 10.64.1.55
Domain	The domain visited by clients, if applicable	www.google.com
URL Category	The URL Category name identified by Deep Edge	Shopping Spyware
File Name	The file name downloaded by clients if applicable	eicar.zip
Malware Name	The virus name blocked by an Anti-Malware scan	Eicar
Action	Block/Monitor	Block
Policy Name	The security policy name for traffic control	Default known-user
WRS Score	The score of URL queried by WRS, if applicable. The scope is 0 ~ 100. A higher value has a better reputation.	49
Source Port	Port Number	42074 39199
Destination Port	Port Number	53 80
IPS Rule	The IPS rule name if it is triggered by IPS Scan	--
ERS Category	1 = blocked by ERS; 0 = otherwise	0
Mail Sender	The message traffic mail sender. Default is empty.	--

LOG ITEM	DESCRIPTION	EXAMPLE
Mail Receiver	The message traffic mail recipient. Default is empty.	--
Mail Subject	The message traffic mail subject. Default is empty.	--
Transfer Protocol	TCP/UDP/ICMP/ICMPv6	TCP
App Name	The application name identified by Deep Edge	DNS HTTP Sina Weibo
App Attribute Name	The granular application name	Sina Weibo-Post Message

Internet Access Logs

Deep Edge logs every session traversing the network. From Internet access logs you can obtain greater visibility and detailed information about network traffic. The following table has detail information.

LOG ITEM	DESCRIPTION	EXAMPLE
Time	Date and time when recorded	2014-02-11 22:51:00
User Name	The user account if Deep Edge is configured as LDAP or Local User authentication. Otherwise, it will be the Client IP address	Lily Jerry
Message Type	Access log	access log
URL	URL visited by clients, if applicable	u034024.778669.com/
Client IP	Source IP address	192.168.1.101

LOG ITEM	DESCRIPTION	EXAMPLE
Server IP	Destination IP address	192.168.1.119 10.64.1.55
Domain	The domain visited by clients, if applicable	www.google.com
File Name	The file name downloaded by clients if applicable	eicar.zip
App Name	The application name identified by Deep Edge	DNS HTTP Sina Weibo
App Attribute Name	The granular application name	Sina Weibo-Post Message
URL Category	The URL Category name identified by Deep Edge	Shopping Spyware
Session Start Time	Start time of the traffic	2014-02-11 15:50:53
Session End Time	End time of the traffic	2014-02-11 15:53:28
Source Interface	Source network interface	eth0
Destination Interface	Destination network interface	eth1
Source Port	Port Number	42074 39199
Destination Port	Port Number	53 80
Transfer Protocol	TCP/UDP/ICMP/ICMPv6	TCP
Policy Name	The security policy name for traffic control	Default known-user

LOG ITEM	DESCRIPTION	EXAMPLE
IPS Rule	The IPS rule name if it is triggered by IPS Scan	--
Malware Name	The virus name blocked by an Anti-Malware scan	Eicar
WRS Score	The score of URL queried by WRS, if applicable. The scope is 0 ~ 100. A higher value has a better reputation.	49
ERS Category	1 = blocked by ERS; 0 = otherwise	0
Mail Sender	The message traffic mail sender. Default is empty.	--
Mail Receiver	The message traffic mail recipient. Default is empty.	--
Mail Subject	The message traffic mail subject. Default is empty.	--
Action	Default is empty. If specified, Allow/ Block/Monitor	Allow

VPN Logs

When a VPN connection is established or disconnected, Deep Edge generates a VPN log with detailed information about the time, user name and IP address. PPTP VPN and SSL VPN generate VPN logs.

LOG ITEM	DESCRIPTION
Log time	Log date and time
Type	SSL VPN or PPTP VPN
IP address	VPN service IP address
User	VPN user account

LOG ITEM	DESCRIPTION
Event	There are four types of Event: • VPN service UP • VPN service DOWN • VPN client connects (It also shows the client IP address.) • VPN client disconnects (It also shows transferred/received bytes.)

TABLE B-1. VPN Log Example

LOG TIME	TYPE	IP ADDRESS	USER	EVENT
2013-01-25 13:43:59	SSL VPN	222.94.7.186	vpn01	SSL VPN client(192.168.150.6) disconnect,bytes_received: 684436,bytes_sent:31375
2013-01-25 13:43:59	SSL VPN	192.168.150.1	tun0	SSL VPN Service Down
2013-01-25 13:40:15	SSL VPN	222.94.7.186	vpn01	SSL VPN client(192.168.150.6) connect
2013-01-25 09:55:36	SSL VPN	192.168.150.1	tun0	SSL VPN Service UP

System Event Logs

When an important event occurs, the Deep Edge generates an event. Events can be related to low system resources and failed security updates.

LOG ITEM	DESCRIPTION
Log Time	Log date and time

LOG ITEM	DESCRIPTION
Type/Service	Deep Edge service which this event is related. It mainly includes the following services: zebra, ripngd, ospf, rip, bgp, openvpn, pptp, sshd, ipsec, hostapd, dnsmasq, dhcp, pppoe, snmp, httpd, postgres, memcached, postfix, imss, imssManager, dpid, vtmservice, sysmon
Description	There are two types of events: 1. Service started/stopped 2. System resources status(memory, CPU, disk space)

TABLE B-2. System Event Log Example: Important Service Start/Stop Event

EVENT TIME	SERVICE	EVENT CONTENT
2013-01-25 13:44:03	openvpn	Service has started
2013-01-25 13:43:59	openvpn	Service has stopped
2013-01-25 11:14:41	dpid	Service has started
2013-01-25 11:14:40	dpid	Service has stopped
2013-01-25 09:56:54	imssd	Service has started
2013-01-25 09:56:54	imssd	Service has stopped
2013-01-25 09:55:39	vtmservice	Service has started
2013-01-26 19:51:39	OS	System has started
2013-01-26 19:52:49	OS	System has stopped

TABLE B-3. System Event Log Example: System Resource Status Event

EVENT TIME	TYPE/SERVICE	EVENT CONTENT
2013-01-25 13:42:43	sysmon	Memory usage rate (91.13%) exceeds 90% in 5 minutes. (Event is sent only once every hour.)

EVENT TIME	TYPE/SERVICE	EVENT CONTENT
2013-01-25 12:38:29	sysmon	Memory usage rate (92.69%) exceeds 90% in 5 minutes. (Event is sent only once every hour.)

Audit Logs

An audit event is created whenever an administrator logs on Deep Edge and makes changes. Audit logs also include events about unsuccessful authentication attempts or invalid access rights.

LOG ITEM	DESCRIPTION
Log Time	Log date and time
Hostname	The Deep Edge appliance IP address or host name.
IP Address	The client IP address
Admin User	The logon account name, if applicable.
Action	The event that occurred.
Object	The objects that were affected by the event.
Result	Shows whether the event activity was successful or unsuccessful
Source	The location that the event occurred: WebUI, CLI, System

TABLE B-4. Audit Log Examples

LOG TIME	HOSTNAME	IP ADDRESS	ADMIN USER	ACTION	OBJECT	RESULT	SOURCE
2014-05-22 16:46:16 +0800	192.168.150.254	192.168.151.172	admin	Logon	Account	Successful	WebUI

LOG TIME	HOSTNAME	IP ADDRESS	ADMIN USER	ACTION	OBJECT	RESULT	SOURCE
2014-05-22 16:30:53 +0800	192.168.150.254	10.64.1.62	admin	Generate	ReportTemplate	Successful	WebUI
2014-05-22 16:30:01 +0800	192.168.150.254	10.64.52.6	root	Logon	SSH	Successful	CLI
2014-05-22 15:42:12 +0800	192.168.150.254	10.66.15.2	Unknown	Accepted	Ping Request	Successful	System

Audit Log Objects

The table below provides a description and menu path for the **Objects** column of audit logs.

OBJECT NAME	DESCRIPTION	MENU PATH
SecurityPolicy	Security rules	PoliciesRules
AddressObj	Address object	Network > Addresses
ZoneObj	Zone object	Policies > Objects > Zones
ServiceObj	Service Object	Policies > Objects > Services
AppldObj	Application Object	Policies > Objects > Applications
UrlFilteringObj	URL category object	Policies > Objects > URL Categories
SchedulerObj	Scheduler Object	Policies > Objects > Schedules
ProfileObj	Profile object	Policies > Objects > Action Profiles
IpsProfile	IPS Profile	Policies > Security Settings > IPS

OBJECT NAME	DESCRIPTION	MENU PATH
AntiMalwareSetting	Anti-Malware settings	Policies > Security Settings > Anti-Malware
ErsObj	Email Reputation Service settings	Policies > Security Settings > Anti-Spam
MailSecurity	Mail security settings	Policies > Security Settings > Anti-Spam
WrsObj	Web Reputation Service settings	Policies > Security Settings > WRS
HttpsCAAuth	HTTPS certificate settings	Policies > HTTPS Inspection > Digital Certificates
HttpsInspectionSettings	HTTPS inspection settings	Policies > HTTPS Inspection > General Settings
UrlWhiteBlackList	URL white/black list settings	Policies > Approve/Block URLs
AntiDosSetting	Anti-DoS settings	Policies > Anti-DoS
IdPolicy	User identification policy	Policies > Authentication > Endpoint Identification
EndUserNotifSetting	End user notification settings	Policies > User Notifications
NetworkInterface	Network interface settings	Network > Interfaces
VlanInterface	VLAN interface settings	Network > Interfaces
PppoeSetting	PPPoE settings	Network > Interfaces
WorkModeObj	System working mode setting	Network > Deployment
InternalAddress	Internal address setting	Network > Deployment > Internal address
Bridge	Bridge settings	Network > Bridge

OBJECT NAME	DESCRIPTION	MENU PATH
StaticRoute	Static route settings	Network > Routing > Static Routes
StaticRoute6	Static route settings of IPv6	Network > Routing > Static Routes
RipSetting	RIP settings	Network > Routing > RIP
RipngSetting	RIPng settings	Network > Routing > RIP
OSPF	OSPF settings	Network > Routing > OSPF
Ospf6d	OSPF settings of IPv6	Network > Routing > OSPF
RouteTable	Routing table	Network > Routing > Routing Table
RouteTable6	Routing table of IPv6	Network > Routing > Routing Table
NatRule	NAT rule settings	Network > NAT
DnsForward	DNS forward settings	Network > Services > DNS Forwarding
DhcpServer	DHCP server settings	Network > Services > DHCP
Dhcp6s	DHCP server settings of IPv6	NetworkServicesDHCP
DDNSConfig	Dynamic DNS settings	Network > Services > Dynamic DNS
PptpSetting	PPTP VPN settings	Network > User VPN > PPTP VPN
OpenVpnSetting	SSL VPN settings	Network > User VPN > SSL VPN
MobileSetting	Mobile VPN settings	Network > User VPN > Mobile VPN
IpssecSetting	Site-to-Site VPN settings	Network > Site-to-Site VPN
LogSetting	Log setting	Analysis & Reports > Log Settings

OBJECT NAME	DESCRIPTION	MENU PATH
MailQrtMgmt	Mail quarantine management setting	Administration > Mail Quarantine > Query
QareaPurge	Quarantine mail purge settings	Analysis & Reports > Mail Quarantine > Settings
ReportTemplate	Report template settings	Analysis & Reports > Reports
SystemSetting	System settings	Administration > System Settings
ProxySetting	Proxy settings	Administration > System Settings > Proxy Setting
Certificate	Web console certification settings	Administration > System Settings > Console Settings
ExperienceImprovement	Experience improvement setting	Administration > System Settings > Experience Improvement
ManagementService	Management service	Administration > Management
template	Notification event template settings	Administration > Notifications > Notification Events
SMTP	SMTP settings	Administration > Notifications > SMTP Settings
UserID	LDAP settings	Administration > LDAP Settings
User	Administrator account setting	Administration > Device Management > Administrative Accounts
EndUser	End user management	Administration > End User Management
PrSetting	Product registration setting	Administration > License
patch	System patch update setting	Administration > Updates > Software Patches

OBJECT NAME	DESCRIPTION	MENU PATH
AuSetting	Active update setting	Administration > Updates > Component Updates
SystemMaintenance	System maintenance	Administration > Maintenance
Configuration	System configuration setting	Administration > Maintenance > Backup/Restore
PacketCapture	Packet capture	Administration > Diagnostics > Packet Capture
TrafficTracing	Traffic tracing	Administration > Diagnostics > Traffic Tracing
CDT	Diagnostic files generation	Administration > Diagnostics > Diagnostic Files
ConnectionTestSetting	Network connectivity testing setting	Dashboard > System Information > Network Information
Policy	System policy	N/A
Account	Administration account actions	N/A
ErrorLang	Web console language setting	N/A

Index

A

about

- anti-DoS, 4-69
- digital certificates, 4-56
- HTTPS inspection, 4-54
- LDAP user identification, 6-11
- Local user identification, 6-14
- product license, 6-25, 8-3
- security settings, 4-34

about product, 6-34

accounts

- adding, 6-8
- administrator, deleting, 6-9

action

- security, 4-30

action profiles, 4-30

- adding, 4-32
- deleting, 4-34
- editing, 4-33
- viewing, 4-30, 4-32

activation code, 8-5

ActiveUpdate, 7-6

adding

- accounts, 6-8
- action profiles, 4-32
- application objects, 4-15
- bandwidth rules, 4-61
- IPsec connections, 3-105
- NAT rules, 3-46, 3-47
- OSPF area, 3-40
- policy rules, 4-3, 4-61
- rules, 4-3
- schedule objects, 4-29
- service objects, 4-13

static route, 3-25

tabs, 5-3

user id policies, 4-73

VLAN subinterfaces, 3-6

VPN site-to-site policies, 3-107

address objects, 3-9, 4-11

configuring, 3-11

deleting, 3-11

viewing, 3-11

administration, 6-1

about, 6-34

language settings, 6-2

overview, 6-1

support, 6-33

system settings, 6-3

system settings, general, 6-3

administrator

accounts, deleting, 6-9

Administrator's Guide, x

advanced

IPsec configuration, 3-110

advanced settings

PPTP VPN, 3-60

SSL VPN, 3-65

Advanced Threat Scan Engine, 4-39

about, 4-39

Advanced Threat Scan Engine (ATSE)

scan engine, 4-39

alerts:

notifications, 6-20

anti-DoS

about, 4-69

exceptions

adding, 4-70

- deleting, 4-71
 - modifying, 4-71
- flood protection
 - configuration, 4-70
- anti-malware, 7-2
 - anti-malware profiles, 4-38
 - file extension, 4-46
- anti-malware pattern files, 7-2
- anti-malware protocol pattern files
 - pattern files
 - anti-malware protocol, 7-3
- anti-spam
 - anti-spam profiles, 4-48
 - security settings, 4-47
- anti-spam profiles
 - configuring, 4-49
 - content settings, 4-52
 - disabling, 4-48
 - enabling, 4-48
 - modifying, 4-51
- anti-spam protocol pattern files, 7-4
- anti-virus pattern files, 7-2
- application
 - group objects, 4-15, 4-16
- application control
 - notifications, 4-78
- application control notifications, 4-78
- application objects, 4-15
 - adding, 4-15
 - deleting, 4-16
 - viewing, 4-16
- approved list
 - URL, 4-67
- area OSPF, 3-39
- Asset/Data Discovery, 4-44
- ATSE, 4-39

- about, 4-39
- audit logs
 - about, 5-41
 - querying, 5-43
- authentication
 - captive portal, 4-74
 - LDAP, advanced, 6-13
 - LDAP, basic, 6-13
 - LDAP, configuring, 6-12
 - user, 4-74
- authentication method
 - LDAP, 6-11

B

- backup, 6-28
 - system, 6-28
- bandwidth control
 - network settings, 3-5
 - policy settings, 4-61
 - widgets, 5-23
- bandwidth summary
 - widget, 5-22
- best practices
 - DNS servers, 3-7, 6-35
 - suggestions, 3-7, 6-35
- blocked list
 - URL, 4-67
- blocked URL
 - notifications, 4-79
- blocked URL notifications, 4-79
- bridge
 - interfaces, 3-20
 - settings, 3-21, 3-23

C

- CA, 4-56, 4-57
- cache server, 7-12

- captive portal, 4-72
 - about, 4-74
 - configuring, 4-75
 - settings, 4-75
- certificate authority
 - exporting, 4-57
 - importing, 4-56
 - managing, 4-57
- certificate failure notifications, 4-81
- changing
 - NAT rules, 3-49
- changing bridge settings, 3-21
- client
 - SSL VPN, installation, 3-67
- client certificate failure
 - notifications, 4-83
- client certificate failure notifications, 4-83
- clients
 - viewing mobile VPN, 3-81
 - viewing PPTP VPN, 3-61
 - viewing SSL VPN, 3-66
- cloud-based services, 6-34
- codes
 - routing table, 3-45
- Command & Control Communication, 4-44
- community, A-2
- components
 - updates, 7-2
- component version, 7-5
- configuring
 - address objects, 3-11
 - alerts for security violations, 6-20, 6-21
 - application control notifications, 4-78
 - blocked URL notifications, 4-79
 - bridge, 3-21, 3-23
 - captive portal, 4-75
 - console settings, 6-4
 - DDNS client, 3-56
 - deployment, 3-19
 - DNS forwarding, 3-50
 - file extension notifications, 4-80
 - IPS violation notifications, 4-81
 - LDAP, basic and advanced, 6-12
 - malware notifications, 4-79
 - notifications for scheduled updates, 6-23, 7-12
 - proxy settings, 6-5
 - routing, 3-25
 - server certificate failure notifications, 4-82, 4-83
 - SMTP notifications, 6-24
 - SSL VPN advanced settings, 3-65
 - SSL VPN IP address pools, 3-64
 - SSL VPN local networks, 3-64
 - system resource warnings, 6-22
 - system settings, 6-3
 - time and date settings, 6-3
 - URL filtering notifications, 4-77
 - user notifications, 4-76
 - WRS notifications, 4-76
 - zone objects, 4-11
- configuring:
 - PPTP VPN general settings, 3-59
- configuring general settings, 3-59
- connections
 - IPsec, 3-104
- console certificate, 6-4
- console settings, 6-4
 - configuring, 6-4
 - console, 6-4
- console timeout, 6-4
- cryptography

- SSL, 4-54
- TLS, 4-54
- custom
 - report, 5-36
- customizing
 - widgets, 5-8
- D**
- dashboard
 - widgets, 5-8
- Data Exfiltration, 4-45
- DDNS
 - configuring client, 3-56
 - Dyn DNS, 3-55
 - FreeDNS, 3-55
 - IPv6, 3-55
 - overview, 3-54
 - status, 3-57
 - status messages, 3-57
- DDNS client, 3-56
- dead peer detection, 3-110
- debugging
 - IPsec, 3-110
- debug mode
 - enabling PPTP VPN, 3-60
- Deep Discovery Advisor, 4-39
 - about, 4-42
 - Virtual Analyzer, 4-39
- Deep Discovery Inspector
 - about, 4-43
- deep packet inspection, 4-36
- deleting
 - action profiles, 4-34
 - address objects, 3-11
 - administrative accounts, 6-9
 - application objects, 4-16
 - NAT rules, 3-50

- OSPF area, 3-41
- services objects, 4-14
- static route, 3-28
- tabs, 5-4
- zone objects, 4-12
- denial of service attack, 4-69
- deployment
 - bridge, 3-20
 - configuring, 3-19
 - inline mode, 3-13, 3-19
 - monitoring mode, 3-17, 3-19
 - settings, 3-12
 - static route, 3-25
- Deployment Guide, x
- Deployment Modes
 - Bridge mode, 3-12
 - Bridge Mode, 3-13
 - Monitoring mode, 3-12
 - Monitoring Mode, 3-17
 - Routing mode, 3-12
 - Routing Mode, 3-15
- detection
 - dead peer, 3-110
- devices
 - management, accounts, 6-7
- DHCP
 - advanced settings, 3-52
 - interface configuration, 3-51
 - lease time, 3-52
 - modifying services, 3-53
 - modifying settings, 3-53
 - static mapping, 3-52
 - viewing services, 3-52
 - viewing settings, 3-52
- DHCP services, 3-53
- diagnosis

- files, 6-33
- trace traffic, 6-32
- traffic tracing, 6-32
- troubleshooting
 - traffic tracing, 6-32
- diagnostic:
 - about, 6-29
- diagnostic files
 - generating, 6-33
- diagnostics
 - about, 6-29
 - network packet capture, 6-30
 - packet capture, 6-30
- digital certificates
 - about, 4-56
 - adding new, 4-59
 - certificate authority
 - exporting, 4-57
 - importing, 4-56
 - changing status, 4-59
 - deleting, 4-60
 - managing, 4-57
 - viewing, 4-58
- displaying
 - list of users, 6-8
- DNS, 3-7, 6-35
 - configuring forwarding, 3-51
 - forwarding configuration, 3-51
 - forwarding settings, 3-51
- DNS forwarding configuration, 3-50
- DNS servers, 3-7, 6-35
- documentation set, xi
- DoS attack
 - ICMP/Ping flood, 4-69
 - TCP SYN flood, 4-69
 - UDP flood, 4-69
- dynamic domain name system service, 3-54
- dynamic source translation, 3-45
- Dyn DNS, 3-55
- E**
- editing
 - action profiles, 4-33
 - schedule objects, 4-29
- editing interfaces, 3-2
- Email Reputation
 - database, 7-5
- email reputation services, 4-47
- email reputation technology, 4-47
- enabling
 - advanced RIP global settings, 3-34
 - debug mode, 3-60
 - ping, 6-6
 - policy rules, 4-9, 4-67
 - PPTP VPN, 3-59, 3-60
 - RIP global settings, 3-33
 - rules, 4-9, 4-67
 - SNMP, 6-6
 - SSH, 6-6
 - SSL VPN, 3-63
 - static route, 3-27
- encapsulated security payload
 - ESP, 3-104
- encryption level
 - PPTP VPN, 3-60
- End user
 - settings, global, 6-11
- entity risk summary
 - widget, 5-13
- error messages
 - PPTP VPN, 3-62
 - SSL VPN, 3-77
- example

- IPsec NAT configuration, 3-113
- IPsec office configuration, 3-111
- site-to-site VPN, 3-111, 3-113
- experience improvement
 - join, 6-5
- expiration
 - license, 8-3
 - warning, 8-3

F

- false positive, 7-10
- file extension
 - notifications, 4-80
 - types to scan, 4-46
- file extension notifications, 4-80
- file extension verification, 4-46
- FreeDNS, 3-55

G

- general system settings, 6-3
- generating
 - manual reports, 5-36
- getting started
 - summary, 2-5
- global log settings, 5-39

H

- hardware monitor
 - widget, 5-30
- HTTPS inspection
 - about, 4-54
 - adding exceptions, 4-55
 - settings, 4-55

I

- ICMP, 4-70
- IKE, 3-104, 3-107
- IKE debugging, 3-110

- incremental updates, 7-5
- inline mode, 3-13
 - bridge, 3-20
- installing:
 - SSL VPN client, 3-67
- integration
 - LDAP, 6-11
- Intelligence Gathering, 4-44
- IntelliTrap, 7-3
- interface
 - OSFP, 3-42
- interface information
 - widgets, 5-26
- interfaces, 3-2, 3-7
 - editing, 3-2
 - OSPF, 3-41
- Internet Key Exchange, 3-104
- introductions
 - notifications, 6-19
- IP address pools
 - SSL VPN, 3-64
- IPS
 - about, 4-35
 - categories, 4-36
 - categories and actions, 4-37
 - instant message, 4-36
 - intrusion prevention system, 4-35
 - peer-to-peer, 4-36
 - policies, 4-37
 - profiles, 4-36
- IPsec, 3-111
 - adding connections, 3-105
 - advanced configuration, 3-110
 - connections, 3-104
 - generate RSA key, 3-110
 - NAT configuration example, 3-113

- office configuration example, 3-111
- RSA key, 3-110
- status, 3-111
- troubleshooting, 3-111

IPS pattern files, 7-3

IPS violation

- notifications, 4-81

IPS violation notifications, 4-81

IPv4 or IPv6, 3-58

K

Knowledge Base, A-6

- URL, x

known issues

- readme, A-6

L

language, change, 6-2

Lateral Movement, 4-44

LDAP, 4-74

- advanced authentication, 6-13
- authentication method, 6-11
- basic authentication, 6-13
- configuring, basic and advanced, 6-12
- integration, 6-11
- method of user identification, 4-73
- settings, global, 6-9, 6-10

LDAP user identification

- about, 6-11

lease time, 3-52

license, 6-25, 8-3

- activation code, 8-5
- expiration, 8-3
- registration, 8-4
- registration key, 8-4
- updating, 8-5

local groups, 6-18

Local user identification

- about, 6-14

local users, 6-15

logs

- about, 5-40, 6-25
- audit, about, 5-41
- introduction, 5-40, 6-25
- querying, 5-43
- querying audit logs, 5-43
- querying system event logs, 5-44
- querying VPN logs, 5-44
- settings, 5-39
- settings, global, 5-39
- system events, about, 5-41
- viewing PPTP VPN, 3-61
- viewing SSL VPN, 3-67
- VPN, about, 5-42

M

main features, 1-9

- ActiveUpdate, 1-10
- anti-spam, 1-10
- application bandwidth monitoring, 1-10
- Application Control, 1-10
- LDAP integration, 1-10
- logs, 1-11
- Network Intrusion Protection, 1-9
- reports, 1-11
- security protection, 1-9
- summary dashboard, 1-10
- system notifications and alerts, 1-11
- URL Filtering, 1-10
- virus scanning, 1-9
- Web Reputation, 1-9

maintaining updates, 7-10

maintenance, A-1

- about, 6-27

- backup, 6-28
- maintenance
 - restart, 6-27
- restore, 6-28
- shutdown, 6-27
- system, 6-27
- Maintenance Agreement
 - defined, 8-2
 - expiration, 8-2
 - renewal, 8-2, 8-6
- malware
 - notifications, 4-79
- malware notifications, 4-79
- management
 - about, 6-5
 - device
 - accounts, 6-7
 - enabling
 - management services, 6-6
 - service, 6-5
 - services, enabling, 6-6
 - SNMP, 6-6
- manual reports, 5-35
 - generating, 5-36
- manual updates, 7-8
- mobile VPN
 - viewing clients, 3-81
- mode
 - bridge, 3-20, 3-21, 3-23
 - inline, 3-13
 - monitoring, 3-17
 - routing, 3-25
- modifying
 - DHCP settings, 3-53
 - NAT rules, 3-49
 - OSPF area, 3-41

- OSPF interface, 3-42
- passwords, user, 6-8
- static route, 3-27
- tabs, 5-3
- monitoring mode, 3-17

N

- NAT, 3-45, 4-72
 - adding rules, 3-46, 3-47
 - changing rule priorities, 3-49
 - deleting rules, 3-50
 - IPsec configuration, 3-113
 - modifying rules, 3-49
 - rules, 3-46
 - site-to-site VPN configuration, 3-113
- network
 - bandwidth control, 3-5
 - configuring for SSL VPN, 3-64
- Network Address Translation, 3-45
- network configuration
 - interfaces, 1-11
- network features, 1-11
 - bridge, 1-12
 - mobile virtual private network, 1-12
 - NAT, 1-12
 - routing, 1-12
 - services, 1-12
 - site-to-site virtual private network, 1-12
 - user virtual private network, 1-12
- network information
 - widget, 5-28
- network intrusion prevention, 4-35
- network RIP settings, 3-35
 - adding, 3-35
 - deleting, 3-36
- next-generation firewall, 1-2
- notification

- SMTP, configuring, 6-24
- notifications
 - alerts, 6-20
 - application control, 4-78
 - blocked URLs, 4-79
 - certificate failure, 4-81
 - client, 4-83
 - server, 4-82
 - configuring for security violations, 6-20, 6-21
 - file extension, 4-80
 - introduction, 6-19
 - IPS violation, 4-81
 - malware, 4-79
 - schedule updates, configuring, 6-23, 7-12
 - SMTP, 6-24
 - stopping, 6-23
 - notifications, 6-23
 - updates, 7-12
 - URL filtering, 4-77
 - user policies, 4-76
 - WRS, 4-76

O

- objects
 - address, 3-9, 4-11
 - address parameters, 3-9
 - application objects, 4-15
 - policy, 4-10
 - schedule objects, 4-29
 - service objects, 4-13
 - zone, 4-11
- offline monitoring, 4-44
- online
 - community, A-2
- Online Help, x
- open shortest path first, 3-37

- OSPF, 3-37
 - adding area, 3-40
 - area, 3-39
 - deleting area, 3-41
 - enabling global settings, 3-38
 - enabling OSPF distribute route, 3-38
 - global, 3-38
 - interfaces, 3-41
 - modifying area, 3-41
 - modifying interface, 3-42
 - redistribute, 3-43
 - redistributing link-state advertisement, 3-43
 - router ID, 3-38
- overview
 - advanced IPsec configuration, 3-110
 - DDNS, 3-54
 - DDNS status, 3-57
 - DNS interface configuration, 3-51
 - dynamic domain name system service, 3-54
 - dynamic route management, 3-31
 - global OSPF, 3-38
 - interfaces, 3-2, 3-7
 - NAT, 3-45
 - open shortest path first (OSPF), 3-37
 - OSPF interfaces, 3-41
 - redistribute OSPF, 3-43
 - redistribute RIP settings, 3-36
 - remote access, 3-58
 - remote access for users, 6-9
 - routing information protocol (RIP), 3-32
 - routing table, 3-44
 - services, 3-50
 - site-to-site VPN, 3-104

- SSL VPN, 3-62
- traffic, 3-2
- user management, 6-9
- VLANs, 3-5
- VPN, 3-58

P

- packet capture
 - components, 6-32
- packet captures, 6-30
- parameters, 3-9
 - address objects, 3-9
 - captive portal, 4-75
 - logs settings, global, 5-39
 - reports, 5-36
 - services objects, 4-13
- password
 - users, modifying, 6-8
- pattern files, 7-2
 - anti-spam protocol, 7-4
 - incremental updates, 7-5
 - IPS, 7-3
 - several on server, 7-2
 - virus, 7-2
- pattern information, 7-5
 - widget, 5-29
- ping
 - enabling, 6-6
- Point of Entry, 4-44
- point-to-point tunneling VPN, 3-58
 - overview, 3-58
- policies, 4-76
 - adding bandwidth rules, 4-61
 - adding rules, 4-3
 - adding VPN site-to-site, 3-107
 - addresses, 3-9, 4-11
 - address objects, 3-9, 4-11

- bandwidth control, 4-61
- enabling rules, 4-9, 4-67
- how policies work, 4-1, 4-2
- modifying IPS, 4-37
- objects, 4-10
- rules page, 4-2, 4-61
- user id, adding, 4-73
- user identification, 4-72
- policy objects, 4-10
- PPTP VPN, 3-59
 - advanced settings, 3-60
 - enabling, 3-59
 - encryption level, 3-60
 - error messages, 3-62
 - overview, 3-58
 - troubleshooting, 3-61
 - viewing clients, 3-61
 - viewing logs, 3-61
- product
 - administration, 6-1
 - license, 6-34
 - management, about, 6-5
 - version, 6-34
- product license, 6-25, 8-3
- product overview, 1-2
- product patches
 - Applying patches, 7-8
- Product Patches
 - Backing up current configuration, 6-28
 - Restoring previous configurations, 6-29
- profiles, 4-36, 4-38, 4-48
 - configuring WRS, 4-54
 - web reputation, 4-53
 - WRS, 4-53
- program components
 - updates, 7-2

proxy, 6-4
proxy settings, 6-4, 7-6
 configuring, 6-5

Q

querying
 audit logs, 5-43
 system events logs, 5-44
 VPN logs, 5-44
querying logs, 5-43
Quick Start Guide, x

R

readme, A-6
Readme, x
redistributing OSPF, 3-43
redistribution
 RIP, 3-36
 RIP settings, 3-36
registering product, 3-4
registration
 key, 8-2, 8-6
 profile, 8-2, 8-6
 URL, 8-2, 8-6
registration key, 8-4
remote access, 3-58
 user management, 6-9
removing
 schedule objects, 4-30
removing bridge settings, 3-23
reports, 5-30
 about, 5-35
 custom, 5-36
 dashboard summary, 5-8
 manual, 5-35
 manual, generating, 5-36
 parameters, 5-36

 scheduled, about, 5-36
 settings, 5-36
 templates, 5-36
 types, 5-35
report types, 5-30
restore
 system, 6-28
Restoring, 6-29
RIP, 3-32
 advanced global settings, 3-34
 configuring global settings, 3-33
 deleting a RIP network, 3-36
 enabling global settings, 3-33
 global settings, 3-33
 network setting, 3-35
 redistribution, 3-36
RIP:
 adding a network, 3-35
rolling back updates, 7-10
routing
 dynamic route management, 3-31
 settings, 3-25
 static route management, 3-25
routing information protocol, 3-32
routing table
 indicators, 3-45
 overview, 3-44
 viewing, 3-44
RSA key, 3-110
 generate, 3-110
rules
 adding NA, 3-46, 3-47
 changing NAT priorities, 3-49
 deleting NAT, 3-50
 modifying NAT, 3-49
 NAT, 3-46

- rules page
 - policies, 4-2, 4-61

S

- scan engine
 - ATSE, 4-39
 - hierarchy, 4-38
 - Virtual Analyzer, 4-39
 - VSAPI, 4-39
- scanning
 - by file extension, 4-46
- scheduled reports, 5-36
- scheduled updates, 7-11
 - configuring notifications, 6-23, 7-12
- schedule objects, 4-29
 - adding, 4-29
 - editing, 4-29
 - removing, 4-30
- scheduling updates, 7-11
- secure socket layer VPN, 3-62
- security settings
 - about, 4-34
 - anti-spam, 4-47
- security status
 - widgets, 5-8
- security violations
 - configuring alerts, 6-20, 6-21
- selecting
 - file extension scanning, 4-46
- server certificate failure
 - notifications, 4-82
- server certificate failure notifications, 4-82
- service objects, 4-13
 - adding, 4-13
 - deleting, 4-14
 - parameters, 4-13
- services, 3-50

- DNS forwarding configuration, 3-50
- DNS forwarding settings, 3-51
 - management, 6-5
 - management, enabling, 6-6
- services objects
 - viewing, 4-14
- session event summary
 - widget, 5-11
- session summary
 - widgets, 5-19
- settings, 6-4
 - console, about, 6-4
 - deployment, 3-12
 - DNS forwarding settings, 3-51
 - End user synchronization, 6-11
 - LDAP, global, 6-9, 6-10
 - logs, 5-39
 - logs, global, 5-39
 - network RIP, 3-35
 - PPTP VPN general, 3-59
 - reports, 5-36
 - RIP redistribution, 3-36
 - SMTP notifications, 6-24
 - SSL VPN server, 3-63
- shell
 - about, 6-9
- site-to-site VPN, 3-104
 - configuration sample, 3-111, 3-113
 - IKE, 3-104
 - IPsec, 3-104
 - troubleshooting, 3-111
- smart protection, 7-4
 - Web Reputation Services, 7-4
- Smart Protection Network, 3-7, 6-34, 6-35
- SMTP
 - notifications, 6-24

SNMP

- enabling, 6-6
- management, 6-6

SolutionBank. *See* Knowledge Base

spam detection, 4-47

spyware, 7-4

- patterns, 7-4

SSH

- enabling, 6-6

SSL VPN

- configuring advanced settings, 3-65
- configuring local network, 3-64
- enabling, 3-63
- installing client, 3-77
- IP address pools, 3-64
- overview, 3-62
- server settings, 3-63
- troubleshooting, 3-77
- viewing clients, 3-66
- viewing logs, 3-67

static mapping, 3-52

static routing

- adding, 3-25
- deleting, 3-28
- enabling, 3-27
- modifying, 3-27

status

- IPsec, 3-111

summary dashboard, 5-2

- adding tabs, 5-3
- deleting tabs, 5-4
- modifying tabs, 5-3
- tabs, 5-2

support, 6-33

- knowledge base, A-2
- resolve issues faster, A-4

TrendLabs, A-6

SYN, 4-70

synchronous transmission (SYN), 4-70

system

- backup, 6-28
- restore, 6-28

system alerts

- notifications, 6-20

system events logs

- about, 5-41
- querying, 5-44

system information

- widgets, 5-25, 5-26

system maintenance, 6-27

- about, 6-27

system resources

- widget, 5-27

system resource warnings, 6-22

system settings

- about, 6-3
- configuring, 6-3
- general, 6-3
- proxy, 6-4

T

tabs

- about, 5-2
- adding, 5-3
- deleting, 5-4
- modifying, 5-3
- summary dashboard, 5-2

TCP, 4-70

technical support, A-1

templates

- report, 5-36

top applications

- widget, 5-21

- top devices protected by anti-spam
 - widget, 5-16
- top domains
 - widget, 5-24
- top entities protected by anti-spam
 - widget, 5-16, 5-18
- top entities protected by anti-virus
 - widget, 5-13
- top entities protected by IPS
 - widget, 5-15
- top entities protected by WRS
 - widget, 5-12
- top URL categories
 - widget, 5-24
- top users
 - widget, 5-20
- traffic:routing, 3-25
- traffic overview, 3-2
- traffic status
 - widgets, 5-18
- traffic tracing, 6-32
- transmission control protocol, 4-70
- TrendEdge, xi
- TrendLabs, A-6
- troubleshooting, 3-111
 - diagnosis, 6-29
 - packet capture, 6-30
 - PPTP VPN, 3-61
 - site-to-site VPN, 3-111
 - SSL VPN, 3-77

U

- update
 - cache server, 7-12
- updates, 7-3
 - anti-malware, 7-2
 - anti-malware protocol, 7-3

- anti-spam protocol, 7-4
- anti-virus, 7-2
- component version, 7-5
- incremental, 7-5
- maintaining, 7-10
- manual, 7-8
- notifications, 7-12
- program components, 7-2
- proxy settings, 7-6
- recommendations, 7-6
- rolling back, 7-10
- scheduled, 7-6, 7-11
- scheduling, 7-11
- verifying success, 7-9
- updating
 - web console, 7-6
- updating your license, 8-5
- URL approved/blocked lists, 4-67
 - adding, 4-67
 - enabling/disabling, 4-68
- URL database, 7-4
- URL filtering, 4-67
 - notifications, 4-77
- URL filtering notifications, 4-77
- URLs
 - Knowledge Base, x, A-6
 - readme documents, A-6
 - registration, 8-2, 8-6
 - technical support, A-6
- user
 - VPN, 3-58
- user authentication, 4-74
- user datagram protocol, 4-70
- user identification
 - LDAP, 6-11
 - LDAP, advance, 6-13

- LDAP, basic, 6-13
 - local, 6-14
 - method, LDAP, 4-73
 - policies, 4-72
- user id policies
 - adding, 4-73
- user management, 6-9
 - general settings, 6-10, 6-11
 - remote access, 6-9
- user notifications, 4-76
- users
 - list of, 6-8
 - passwords, modifying, 6-8
- V**
- verifying
 - file extension, 4-46
- verifying updates, 7-9
- viewing
 - action profiles, 4-30, 4-32
 - address objects, 3-11
 - application objects, 4-16
 - DHCP services, 3-52
 - DHCP settings, 3-52
 - list of users, 6-8
 - mobile VPN clients, 3-81
 - PPTP VPN clients, 3-61
 - PPTP VPN logs, 3-61
 - routing table, 3-44
 - service objects, 4-14
 - SSL VPN clients, 3-66
 - SSL VPN logs, 3-67
 - zone objects, 4-12
- violation event status
 - widget, 5-9
- virtual private network, 3-58
- virus patterns, 7-3

- Virus Scan Engine
 - scan engine, 4-39
- virus scan engines, 7-3
- VLANs, 3-5
 - adding subinterfaces, 3-6
- VPN, 3-58, 3-79
 - iOS and Android, 3-79
 - site-to-site, 3-104
 - SSL, 3-62
 - user, 3-58
- VPN logs
 - about, 5-42
 - querying, 5-44
- VPN on Demand, 3-79
- VPN site-to-site
 - adding policies, 3-107
- VPN tunnel
 - IPsec, 3-104

- W**
- warnings
 - system resource, notifications, 6-22
- web reputation, 7-4
 - profiles, 4-53
 - URL database, 7-4
- web shell
 - about, 6-9
- widget
 - bandwidth summary, 5-22
 - pattern information, 7-5
 - top applications, 5-21
- widgets, 5-30
 - about, 5-4
 - adding, 5-7
 - bandwidth control, 5-23
 - customizing, 5-6, 5-8
 - dashboard, 5-8

- deleting, 5-8
- description, 5-8
- entity risk summary, 5-13
- hardware monitor, 5-30
- interface information, 5-26
- network information, 5-28
- pattern information, 5-29
- security status, 5-8
- session event summary, 5-11
- session summary, 5-19
- system information, 5-25, 5-26
- system resources, 5-27
- top devices protected by anti-spam, 5-16
- top domains, 5-24
- top entities protected by anti-spam, 5-16, 5-18
- top entities protected by anti-virus, 5-13
- top entities protected by IPS, 5-15
- top entities protected by WRS, 5-12
- top URL categories, 5-24
- top users, 5-20
- traffic status, 5-18
- violation event status, 5-9

WRS

- configuring profiles, 4-54
- notifications, 4-76
- profiles, 4-53

WRS notifications, 4-76

Z

- zone objects, 4-11
 - configuring, 4-11
 - deleting, 4-12
 - viewing, 4-12
- zones
 - objects, 4-11



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: CTEM26692/140930