TREND MICRO™

2.5 TREND MICRO™ Deep Discovery Web Inspector

Installation and Deployment Guide

Advanced Protection Against Targeted Web Attacks

Endpoint Security

Network Security

Protected Cloud

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/

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

Copyright © 2019. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM28795/190819

Release Date: December 2019

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 at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that Deep Discovery Web Inspector collects and provides detailed instructions on how to disable the specific features that feedback the information.

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

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

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Preface vii

Documentation viii

Audience ix

Document Conventions ix

About Trend Micro x

Chapter 1: Introduction

Overview of Deep Discovery Web Inspector 1-2

Features and Benefits 1-2

- Flexible Deployment 1-2
- Visibility, Analysis, and Action 1-2
- Easy-to-Use Policy Management 1-2
- Advanced Detection 1-3
- HTTP/2 Scanning 1-4
- HTTPS Inspection 1-4
- Custom Threat Simulation Sandbox 1-4
- Patient Zero Protection 1-5
- Access Log Offload to a Syslog Server 1-5
- Integration with Microsoft Active Directory 1-5
- Integration with Deep Discovery Analyzer 1-6
- Integration With Deep Discovery Director 1-6
- Integration With Trend Micro Apex Central 1-7

New Features and Enhancements 1-8

Chapter 2: Preparing for Deployment

Pre-deployment Tasks 2-2

Network Deployment Mode Overview 2-3

- Forward Proxy Mode 2-3

Transparent Bridge Mode 2-4
Transparent HA Mode 2-8
Multi-Bridge Mode 2-14
LACP Deployments 2-16

Adding a Second Bypass Adapter to the Appliance 2-21

Recommended Network Environment 2-27

System Requirements 2-27
Enabling and Starting the SSH Service 2-28

Ports Used by the Appliance 2-29

Items to Prepare 2-32

Apex Central Deployment 2-38

Chapter 3: Deployment

Setting up the Hardware 3-2

Configuring Management Console Access 3-2

Opening the Management Console 3-5
Changing Your Password 3-6

Activating the License 3-6

Performing the Initial Deployment 3-9
Initial Deployment for Forward Proxy Mode 3-9
Initial Deployment for Transparent Bridge Mode 3-12
Initial Deployment for Transparent HA Mode 3-15
Initial Deployment for Multi-Bridge Mode 3-19
Initial Deployment for LACP 3-22

Chapter 4: Getting Started

Management Console Navigation 4-2

Getting Started Tasks 4-2
Managing Your Product License 4-5
Configuring Network Settings 4-5
Configuring the Notification SMTP Server 4-8
Importing Virtual Analyzer Images 4-9

Virtual Analyzer Network 4-13
Virtual Analyzer Integration with Deep Discovery Analyzer 4-16
Configuring Proxy Settings 4-17
Alerts 4-19
Managing User-Defined Settings 4-21
Managing Policies 4-26
Managing HTTPS Decryption Rules 4-31
Apex Central 4-39
Deep Discovery Director 4-42

Performing Additional Configuration Tasks 4-43
Configuring X-Header Handling Settings 4-44

Chapter 5: Updating Deep Discovery Web Inspector

Hotfixes and Patches Overview 5-2

Managing Patches 5-2

Upgrading Firmware 5-3

Chapter 6: Backing Up or Restoring a Configuration

Settings That Are Backed Up or Restored 6-3

Backing Up a Configuration 6-4

Restoring a Configuration 6-5

Chapter 7: Reinstalling Deep Discovery Web Inspector

Before Reinstalling 7-2

Performing a Fresh Install of Deep Discovery Web Inspector 7-2

Chapter 8: Using the Command Line Interface

Entering the CLI 8-2

Normal and Privileged Commands 8-3

Entering Privileged Mode 8-3

CLI Command Reference 8-3
configure deploy reset 8-4

configure module 8-4
configure network 8-8
configure service 8-24
configure system 8-27
enable 8-29
exit 8-30
help 8-30
history 8-31
logout 8-31
ping 8-32
reboot 8-32
resolve 8-33
restart service 8-33
show kernel 8-35
show memory 8-37
show module 8-38
show network 8-40
show process 8-45
show kernel 8-48
show service 8-50
show storage statistic 8-52
show system 8-53
shutdown 8-57
start service 8-58
stop process 8-59
stop process core 8-59
stop service 8-60
traceroute 8-61

Chapter 9: Technical Support

Troubleshooting Resources 9-2
Using the Support Portal 9-2
Threat Encyclopedia 9-2

Contacting Trend Micro 9-3
Speeding Up the Support Call 9-4

Sending Suspicious Content to Trend Micro 9-4
Email Reputation Services 9-4
File Reputation Services 9-5
Web Reputation Services 9-5

Other Resources 9-5
Download Center 9-5
Documentation Feedback 9-6

Index

Index IN-1

Preface

Preface

Topics include:

- *Documentation on page viii*
- *Audience on page ix*
- *Document Conventions on page ix*
- *About Trend Micro on page x*

Documentation

The documentation set for Deep Discovery Web Inspector includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to deploy, configure, and manage Deep Discovery Web Inspector, and provides explanations on Deep Discovery Web Inspector concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide discusses requirements and procedures for installing and deploying Deep Discovery Web Inspector.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide contains information on event logging formats supported by Deep Discovery Web Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Web Inspector to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Web Inspector management console. The Online Help contains explanations of Deep Discovery Web Inspector components and features, as well as procedures needed to configure Deep Discovery Web Inspector.

Document	Description
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

View and download Deep Discovery Web Inspector documentation from the Trend Micro Documentation Center:

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

Audience

The Deep Discovery Web Inspector documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Policy management and enforcement

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

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

CONVENTION	DESCRIPTION
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
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

Introduction

Topics include:

- *Overview of Deep Discovery Web Inspector on page 1-2*
- *Features and Benefits on page 1-2*
- *New Features and Enhancements on page 1-8*

Overview of Deep Discovery Web Inspector

Deep Discovery Web Inspector inspects and eliminates cyber threats and attacks that could threaten your network. Designed to be integrated into your existing network topology to monitor your network traffic, Deep Discovery Web Inspector acts as either a transparent bridge or a forward proxy.

Features and Benefits

The following section describes Deep Discovery Web Inspector features and benefits.

Flexible Deployment

Deep Discovery Web Inspector integrates into your existing network topology by acting as either a transparent bridge or a forward proxy.

In forward proxy mode, Deep Discovery Web Inspector is configured as a proxy server for network clients. Clients have to configure the web proxy to redirect web traffic to Deep Discovery Web Inspector.

In transparent bridge mode, Deep Discovery Web Inspector acts as a layer 2 bridge between network devices (switches, routers, or firewalls) and is transparent in the network.

Visibility, Analysis, and Action

Deep Discovery Web Inspector provides real-time threat visibility and analysis in an intuitive, multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.

Easy-to-Use Policy Management

Deep Discovery Web Inspector provides easy-to-use, but powerful policy management.

- Create policies that specify which network and domain objects and which file types to scan.
- Create network or domain objects to use when creating policies.
- Use a pre-defined list of file types when configuring policies.
- Choose whether to allow, block, or scan objects that are a policy match.
- If matching objects are scanned, further refine actions taken by specifying whether to monitor or block the object depending on the risk level.
- Provide advanced malware protection by enabling Provide Patient Zero Protection.

  If an object is send to Virtual Analyzer for sandbox analysis, Patient Zero Protection temporarily holds objects until analysis is complete instead of passing the object to the endpoint even before analysis determines the risk level for the object.
- Configure multiple policies and prioritize by moving them up or down in the policy order.
- Customize email notifications sent to users for policy violations.
- Create HTTPS inspection rules to decrypt and inspect HTTPS traffic.
- Configure the Approved/Blocked lists to allow or block traffic without need for scanning.

Advanced Detection

Deep Discovery Web Inspector advanced detection technology discovers targeted threats based on network objects, domain objects, URLs, and file types.

Deep Discovery Web Inspector uses multiple detection methods to ensure the highest level of protection, including:

- Approved/Blocked list to determine which URLs, domains, or file (SHA1) objects to allow or block without needing to scan
- Untrusted server certificate analysis to detect whether the URL or domain has an untrusted SSL server certificate

- Web Reputation Services database to block users from URLs that are known malicious sites
- True file types that you select for inclusion in a policy to trigger a detection and then can take action based on the configured policy
- Static Intelligence Engine's known pattern for detecting malware
- Script Analyzer Lineup to detect malicious scripts
- Advanced Threat Scan Engine for advanced detection of malware
- Predictive Machine Learning for intelligent analysis of unknown threats
- Virtual Analyzer sandbox for custom threat simulation analysis

HTTP/2 Scanning

Deep Discovery Web Inspector advanced detection technology can scan HTTP/2 traffic.

HTTPS Inspection

The traffic over SSL/TLS is encrypted and signed to ensure security. Because encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections, HTTPS traffic should be inspected just as HTTP traffic is. Deep Discovery Web Inspector advanced detection technology can decrypt and inspect HTTPS traffic based on criteria that you specify.

Custom Threat Simulation Sandbox

The Virtual Analyzer sandbox environment opens suspicious files submitted to test for malicious behavior. Virtual Analyzer is able to find exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

Patient Zero Protection

Patient Zero Protection provides advanced malware protection from suspicious objects that have been sent to Virtual Analyzer for sandbox analysis.

If Patient Zero Protection is enabled, Deep Discovery Web Inspector temporarily holds the suspicious object while analysis is performed. Once analysis is complete, depending on the outcome of the analysis, the appropriate action is taken. Deep Discovery Web Inspector delivers the object to the endpoint if it is riskless. If sandbox analysis determines that the risk level for that object is low, medium, or high, the malicious object is blocked or monitored, according to the actions configured for the policy that triggered the analysis.

Access Log Offload to a Syslog Server

Deep Discovery Web Inspector supports an access log. You can configure syslog settings to offload the access logs to an external syslog server. Additionally, you can customize which access log entries are sent so that you send only the data that is useful to your business environment.

Integration with Microsoft Active Directory

Deep Discovery Web Inspector Active Directory Services supports integration with Microsoft Active Directory to provides authentication services.

You can configure Active Directory Services to use one or more domains for authentication. Additionally, you can customize your authentication strategy by configuring Active Directory Services authentication policies.

Deep Discovery Web Inspector can use Active Directory users and groups for the following purposes:

- For authentication when end-users access web resources through the Deep Discovery Web Inspector appliance or when they log on through Captive Portal
- To match policy traffic using the traffic source criteria
- To match HTTPS inspection policy traffic using the decryption source criteria

- Deep Discovery Web Inspector can insert Active Directory user or group names into the %USER% and %USER_GROUP % tokens used in applicable notification templates.
- When creating an account that can log into the web console, including a user with full administrative rights

Integration with Deep Discovery Analyzer

Deep Discovery Web Inspector supports integration with Deep Discovery Analyzer.

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration to augment or centralize the sandbox analysis of other Trend Micro products. The custom sandboxing environments created within Deep Discovery Analyzer precisely match target desktop software configurations, resulting in more accurate detections and fewer false positives.

For details, refer to the documentation available at:

http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx

Integration With Deep Discovery Director

Deep Discovery Web Inspector supports integration with Deep Discovery Director.

Deep Discovery Director is an on-premises management solution that enables centralized deployment of product updates, hotfixes, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication for Deep Discovery products.

Additionally, by registering Deep Discovery Web Inspector to Deep Discovery Director, you can enable the bi-directional synchronization of synchronized suspicious objects and suspicious object exceptions.

To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

For details, refer to the documentation available at: Deep Discovery Director.

Integration With Trend Micro Apex Central

Deep Discovery Web Inspector supports integration with Trend Micro Apex Central.

Apex Central is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Apex Central web-based management console provides a single monitoring point for managed products and services throughout the network.

In a network topology containing multiple Deep Discovery Web Inspector appliances, Apex Central can aggregate suspicious objects data.

Deep Discovery Web Inspector appliances support the synchronization of two types of suspicious objects: Virtual Analyzer suspicious objects and user-defined suspicious objects. The appliances also support the synchronization of the suspicious objects exceptions list.

With Apex Central integration, Deep Discovery Web Inspector appliances can defend from threats happening in the world in real time by blocking the traffic if matched in the synchronized high-risk suspicious objects list. Deep Discovery Web Inspector supports uploading the sandbox blacklist (Virtual Analyzer suspicious objects) to Apex Central for central management.

Other Apex Central functions including component and pattern deployment and suspicious object filtering detection logs are not supported.

Note

1. To download suspicious objects and user-defied suspicious objects from Apex Central, you must register to Apex Central from the Deep Discovery Web Inspector web console first.

2. To upload Deep Discovery Web Inspector suspicious objects and the suspicious object detection logs to Apex Central or to get the Apex Central exception list, you must use the Apex Central console to register Deep Discovery Web Inspector to Apex Central.

For details, refer to the documentation available at Apex Central.

New Features and Enhancements

Enhancement to HTTPS Inspection

Adds enhancements to HTTPS Inspection functionality. The Policy menu has been expanded with new sub-menus for HTTPS Inspection:

- Decryption Rules

  Menu item formerly known as HTTPS Inspection where you can configure decryption rules.

- Digital Certificates

  Manage digital certificates in Trusted, Untrusted, Invalid certificates stores and manage the exception list.

- HTTPS Tunnels

  Manage HTTPS tunnels, which allow the tunneling of HTTPS traffic without decryption.

- Intelligent Decryption

  Manage fingerprint patterns used to determine whether traffic should be decrypted or not decrypted based on the fingerprint signature of the browser.

Configure Whether to Bypass Scanning Of Traffic From iOS and Android Mobile Devices

Deep Discovery Web Inspector has adopted the Trend Micro DPI Turnkey Solution to classify network traffic from iOS or Android devices. The default is to scan traffic from these devices. You can now configure Deep Discovery Web Inspector to bypass scanning of traffic from iOS and Android devices.

Enhancement to Apex Central Integration

Adds support for synchronization of suspicious objects and suspicious object exceptions between Deep Discovery Web Inspector and Apex Central (formerly known as Trend Micro Control Manager).

You can upload suspicious objects and view synchronized suspicious objects from the **Detections** > **Suspicious Objects** screen. Deep Discovery Web Inspectorr can be registered from the Apex Central web console. Deep Discovery Web Inspector can upload suspicious objects and suspicious object detection logs to Apex Central.

Adds Support for Integration with Deep Discovery Director

Trend Micro Deep Discovery Director is an on-premises management solution that enables centralized management of certain Deep Discovery Web Inspector tasks, as well as configuration replication for Deep Discovery Web Inspector appliances.

By registering the appliance to Deep Discovery Director, you can enable the bi-directional synchronization of synchronized suspicious objects and suspicious object exceptions.

Additionally, Deep Discovery Director synchronization scheduling tasks provides synchronization services to Deep Discovery Web Inspector node pairs operating in Transparent HA mode.

Support for Transparent HA Mode

Transparent HA mode supports a multi-Internet connection network environment with asymmetric routing. For each connection link, there will be one Deep Discovery Web Inspector node. The difference between Transparent HA mode and Transparent Bridge mode is that under Transparent HA mode, each Deep Discovery Web Inspector appliance sets an IP address on the bridge egress interface (br0), and each appliance rewrites the source IP address to access real web servers, which solves the asymmetric routing issue.

You can use Transparent HA mode in network environments with asymmetric routing. If there is no asymmetric routing scenario in the network, you do not need to use this mode.

You can implement a Transparent HA deployment with or without LACP trunks.

Support for LACP

Deep Discovery Web Inspector supports LACP (Link Aggregation Control Protocol, 802.3ad standard) for configuring trunked data egress/data ingress interfaces in Transparent Bridge and Transparent HA modes. When LACP is enabled, Deep Discovery Web Inspector automatically creates a two-port aggregate for data ingress and a two-port aggregate for data egress.

LACP trunk links provide link redundancy.

Enhancement to Transparent Bridge Mode

Transparent Bridge mode has been enhanced to include support for LACP link aggregation.

As part of the deployment, you can enable LACP and use trunked interfaces for data ingress and data egress.

Support for Multi-Bridge Mode

Multi-Bridge mode is variation of Transparent Bridge mode where Deep Discovery Web Inspector is equipped with two bypass cards and connects to the Internet through two WAN lines. The appliance acts as a layer 2 bridge between network devices (core switches and routers) and is transparent on the network.

Enhancements to the Approved/Blocked List

Deep Discovery Web Inspector supports adding a new type, Server IP address, to the Approved/Blocked list.

Additionally, you can use the automatic method to add entries for all object types (Domain, URL, Server IP address, or File SHA1) to the Approved/Blocked List and Deep Discovery Web Inspector will automatically determine the entry type as the entry is added to a list.

Note

If desired, under advanced settings you can still specify whether you want an entry to be added as a domain, a URL, a Server IP address, or a file SHA1.

Support for Synchronized Suspicious Objects

Adds support for displaying detections for synchronized suspicious objects acquired from either Deep Discovery Director or Apex Central (formerly known as Control Manager).

Supported synchronized suspicious object types include: Domain, URL, IP address, and File SHA1.

You can conveniently select one or more synchronized suspicious objects from the detection page and add them to either the Approved List or Blocked List.

Support for TLS 1.3

Adds support to decrypt HTTPS traffic with TLS 1.3.

Enhanced X-Header Handling

Options have been added to the Deep Discovery Web Inspector web console to enable or disable parsing XFF headers. When Deep Discovery Web Inspector receives an HTTP request with an XFF header, it parses the XFF header to obtain the original client IP address and use the IP address when evaluating whether traffic matches a policy.

Note

Deep Discovery Web Inspector does not support parsing XFF headers for HTTPS traffic if the traffic is not decrypted.

Support for the Mitre Report

Deep Discovery Web Inspector supports displaying the Mitre report from the sandbox in the Virtual Analyzer report.

Chapter 2

Preparing for Deployment

Topics include:

- *Pre-deployment Tasks on page 2-2*
- *Network Deployment Mode Overview on page 2-3*
- *Adding a Second Bypass Adapter to the Appliance on page 2-21*
- *Recommended Network Environment on page 2-27*
- *System Requirements on page 2-27*
- *Ports Used by the Appliance on page 2-29*
- *Items to Prepare on page 2-32*
- *Apex Central Deployment on page 2-38*

Pre-deployment Tasks

The following procedure provides an overview of items to consider and tasks to perform before deploying Deep Discovery Web Inspector.

Procedure

1. Decide which deployment mode to use.

   See *Network Deployment Mode Overview on page 2-3*.

2. (Optional) If you are deploying a configuration that requires two bypass cards (Multi-Bridge Mode or LACP-enabled Transparent Bridge or Transparent HA Modes), add the second bypass card to your Deep Discovery Web Inspector appliance.

   See *Adding a Second Bypass Adapter to the Appliance on page 2-21*.

3. Review the recommended network environment information.

   See *Recommended Network Environment on page 2-27*.

4. Review the system requirements.

   See *System Requirements on page 2-27*.

5. Review the information about ports used by the appliance and open ports as needed.

   See *Ports Used by the Appliance on page 2-29*.

6. Prepare the items for deployment.

   See *Items to Prepare on page 2-32*.

7. Prepare Apex Central or Deep Discovery Director if used as part of the deployment.

   See *Apex Central Deployment on page 2-38* or *Deep Discovery Director on page 4-42*.

Network Deployment Mode Overview

You can configure Deep Discovery Web Inspector in one of several network topology modes.

If desired, you can deploy solutions that use LACP for link aggregation for Transparent Bridge and Transparent HA modes.

- *Forward Proxy Mode on page 2-3*
- *Transparent Bridge Mode on page 2-4*
  - *Topology: Transparent Bridge Mode on page 2-5*
  - *Topology: Transparent Bridge Mode With Trunks on page 2-6*
- *Transparent HA Mode on page 2-8*
  - *Topology and Requirements: Transparent HA Mode on page 2-9*
  - *Topology and Requirements: Transparent HA Mode With Trunks on page 2-11*
- *Multi-Bridge Mode on page 2-14*
- *LACP Deployments on page 2-16*
  - *How LACP Works With Deep Discovery Web Inspector on page 2-19*

Forward Proxy Mode

With Forward Proxy mode, Deep Discovery Web Inspector is configured as a proxy server for network clients. Client browser settings must be configured to redirect traffic to Deep Discovery Web Inspector.

Deep Discovery Web Inspector policies are compared against both incoming and outgoing traffic. Deep Discovery Web Inspector performs security scans and takes action if there is a traffic match according to configured policies. Deep Discovery Web Inspector can bypass scanning and forward the traffic straight to the endpoints, block traffic without scanning it, or scan the traffic and then either block or monitor traffic, depending on actions configured in policies.

Forward Proxy mode also provides the additional capability to forward all traffic to another upstream proxy server.

Transparent Bridge Mode

With Transparent Bridge mode, Deep Discovery Web Inspector (the appliance) acts as a layer 2 bridge between network devices (core switch, router, or firewall) and is transparent on the network.

Deep Discovery Web Inspector performs security scans on HTTP/HTTPS traffic that passes through the ingress and egress ports and takes action if there is a traffic match according to configured policies. The appliance can bypass scanning and let the traffic pass straight through the appliance, block the traffic without scanning, or scan the traffic and then either block or monitor the traffic, depending on actions configured in policies.

Transparent Bridge mode is suitable when you want to use Deep Discovery Web Inspector as an inline device and there is only one network path that you want to monitor. If you set up the appliance in Transparent Bridge mode, you do not need to reconfigure your network as you need only place the appliance in the network path that you want to secure.

Note

Deep Discovery Web Inspector does not support security scans for QUIC protocol traffic.

Support For Trunks Using LACP Link Aggregation

For environments where higher bandwidth is required for data ingress and data egress, you can implement a Transparent Bridge deployment with trunks using LACP link aggregation.

- LACP is available only on appliances equipped with two bypass cards.
- You must acquire and install the second bypass card before you can configure an LACP-enabled deployment.
- See *Adding a Second Bypass Adapter to the Appliance on page 2-21*.

Topology Diagrams

- *Topology: Transparent Bridge Mode on page 2-5*
- *Topology: Transparent Bridge Mode With Trunks on page 2-6*

Topology: Transparent Bridge Mode

The following graphic depicts the topology for Transparent Bridge mode.

Topology

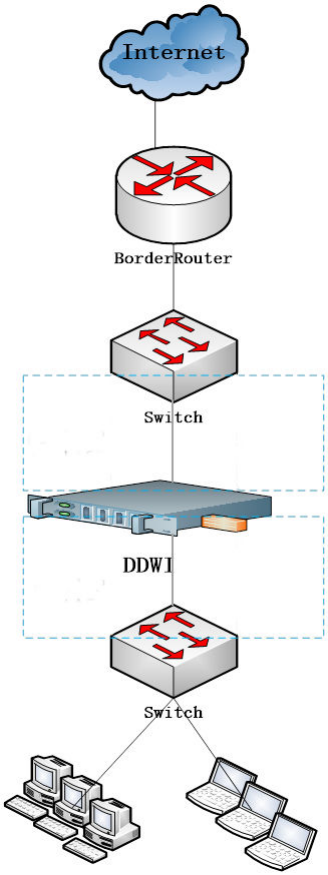


FIGURE 2-1. Transparent Bridge mode

Topology: Transparent Bridge Mode With Trunks

You can use LACP port aggregation in environments where higher bandwidth for data ingress and data egress is required. When LACP is enabled, Deep Discovery Web Inspector automatically creates a two-port aggregate for data ingress and a two-port aggregate for data egress.

The following graphic depicts the topology for Transparent Bridge mode with LACP trunks.

Topology

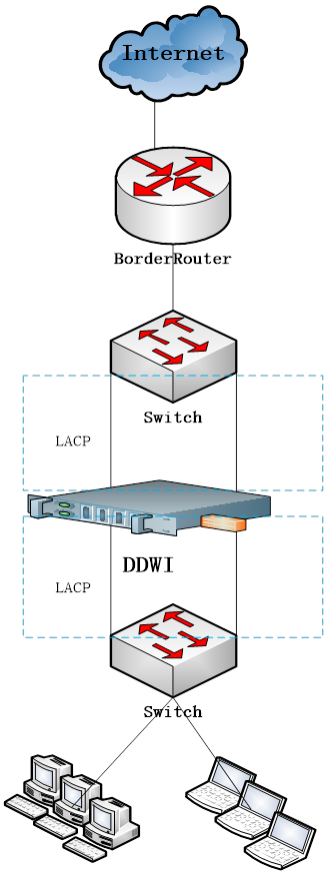


FIGURE 2-2. Transparent Bridge mode with trunks

Related information

↪ *LACP Deployments*

↳ *How LACP Works With Deep Discovery Web Inspector*

Transparent HA Mode

For enterprise networking, there is normally more than one Internet connection for reliability reasons; each connects to a different ISP. These Internet connections work in a load balancing or active-standby manner. With this configuration, asymmetric routing might occur. This raises challenges for a Deep Discovery Web Inspector deployment because Deep Discovery Web Inspector (the appliance) is a connection-oriented security gateway; it must have all data for a connection to perform scan tasks.

To solve asymmetric routing issue, Deep Discovery Web Inspector can be deployed in Transparent HA mode. If there is no asymmetric routing scenario in your network, you do not need to use this mode.

The appliance performs security scans on HTTP/HTTPS traffic that passes through the ingress and egress ports and takes action if there is a traffic match according to configured policies. The appliance can bypass scanning and let the traffic pass straight through the appliance, block the traffic without scanning, or scan the traffic and then either block or monitor the traffic, depending on actions configured in policies.

Difference Between Transparent Bridge and Transparent HA Modes

The difference between Transparent Bridge mode and Transparent HA mode is that under Transparent HA mode, each appliance sets an IP address on the bridge egress interface (br0), and each appliance rewrites the source IP address to access real web servers, which solves the asymmetric routing issue.

Support For Trunks Using LACP Link Aggregation

For environments where higher bandwidth is required for data ingress and data egress, you can implement a Transparent HA deployment with trunks using LACP link aggregation.

- LACP is available only on appliances equipped with two bypass cards.
- You must acquire and install the second bypass card before you can configure an LACP-enabled deployment.
- See *Adding a Second Bypass Adapter to the Appliance on page 2-21*.

Synchronization Between the Two Nodes:

Configuration and policy settings are synchronized between the two Deep Discovery Web Inspector HA nodes. This synchronization is not implemented by the Deep Discovery Web Inspector itself, but by the Deep Discovery Director appliance to which the Deep Discovery Web Inspector nodes are registered. The synchronization is accomplished by configuring the Deep Discovery Director synchronization scheduling task.

Therefore, to implement a Transparent HA mode deployment, you must integrate and register each of the Deep Discovery Web Inspector HA nodes to Deep Discovery Director.

Topology Diagrams and Implementation Requirements

- *Topology and Requirements: Transparent HA Mode on page 2-9*
- *Topology and Requirements: Transparent HA Mode With Trunks on page 2-11*

Topology and Requirements: Transparent HA Mode

You should be aware of certain requirements and the topology for the Transparent HA mode deployment.

Topology

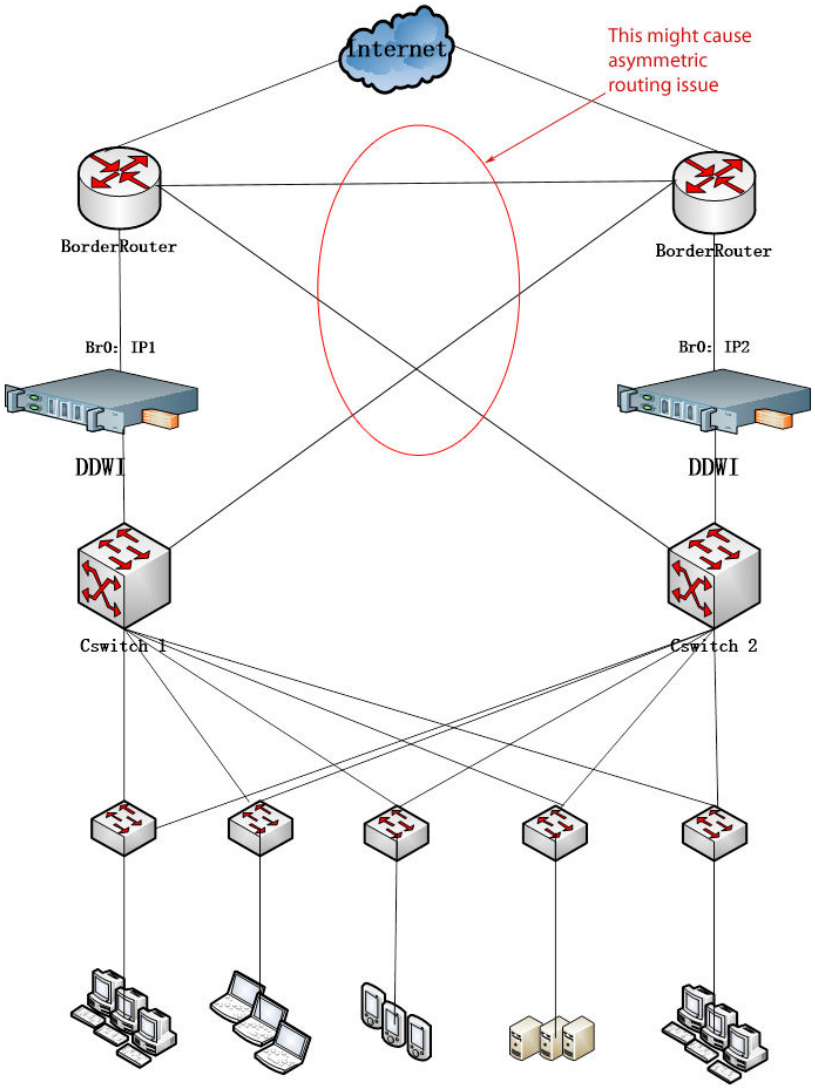


FIGURE 2-3. Transparent HA mode

Requirements

When performing the initial deployment, you should disable the VLAN ID on the egress port of each Deep Discovery Web Inspector node, and traffic through the appliances should not take VLAN tags.

Important

You must ensure that the IP address of the Deep Discovery Web Inspector bridge egress interface (br0) can access the Internet.

Topology and Requirements: Transparent HA Mode With Trunks

You can configure Transparent HA mode with trunk links. You should be aware of certain requirements and the topology for this deployment mode.

You can create trunk links using LACP port aggregation in environments where higher bandwidth for data ingress and data egress is required. When LACP is enabled, Deep Discovery Web Inspector automatically creates a two-port trunk for data ingress and a two-port trunk for data egress on each of the two HA nodes.

Topology

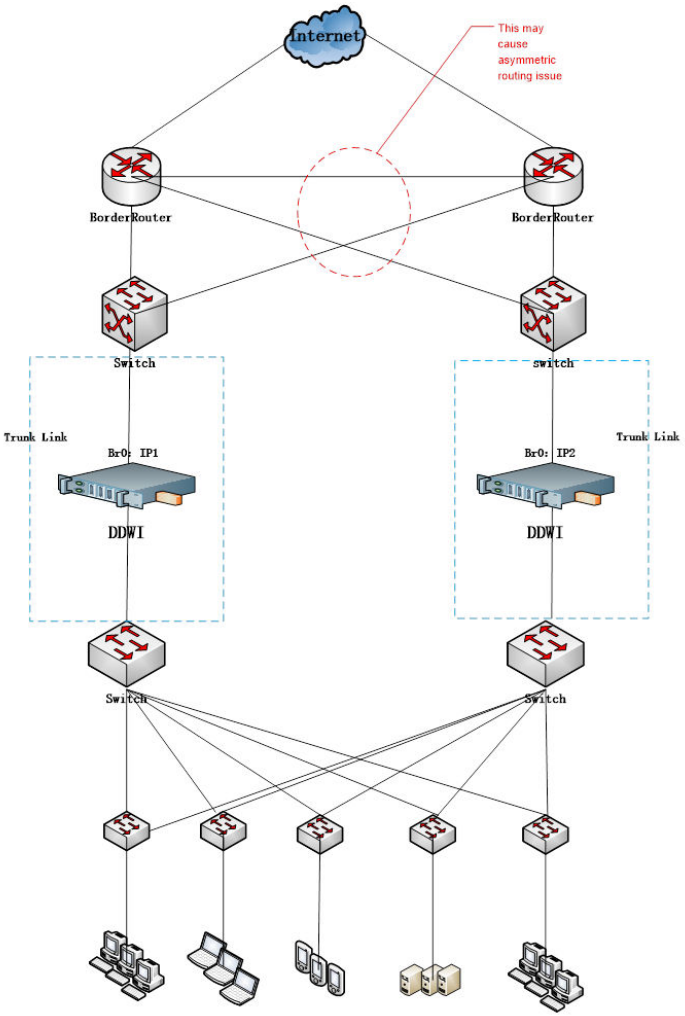


FIGURE 2-4. Transparent HA with trunk links

Requirements

You should understand the following requirements that are dependent on how Deep Discovery Web Inspector IP addressing works under various scenarios for VLAN trunk links including the following:

1. How IP addressing works under the native VLAN of the trunk link:

   Case 1: Traffic under the native VLAN going out of the switch to Deep Discovery Web Inspector does not carry the native VLAN ID.

   Requirement: When performing the initial deployment, you should disable the VLAN ID on the egress port.

   Case 2: Traffic under the native VLAN going out of the switch to Deep Discovery Web Inspector carries the native VLAN ID.

   Requirement: When performing the initial deployment, you should enable the VLAN ID on the egress port, and the VLAN ID must set to the native VLAN ID.

2. How IP addressing works under a normal trunk VLAN.

   Requirement: When performing the initial deployment, you should enable the VLAN ID on the egress port, and the VLAN ID must set to the normal trunk VLAN ID.

Important

- You must ensure that the IP address of the Deep Discovery Web Inspector bridge egress interface (br0) can access the Internet.
- If some clients and the internal web servers are deployed in the same VLAN and the IP address of the egress port of the appliance is not in the same VLAN, clients might not be able to access the internal HTTP server after the VLAN converges to the egress port VLAN.
- In a trunk link, all traffic from ingress can carry different VLAN tags. All these VLAN tags will converge to the one VLAN (native VLAN/normal VLAN) of the egress port to access to the Internet.

Related information

➥ *LACP Deployments*

➥ *How LACP Works With Deep Discovery Web Inspector*

Multi-Bridge Mode

Multi-Bridge mode is variation of Transparent Bridge mode where Deep Discovery Web Inspector is equipped with two bypass cards and connects to the Internet through two WAN lines. The appliance acts as a layer 2 bridge between network devices (core switches and routers) and is transparent on the network.

Deep Discovery Web Inspector performs security scans on HTTP/HTTPS traffic that passes through the ingress and egress ports and takes action if there is a traffic match according to configured policies. The appliance can bypass scanning and let the traffic pass straight through the appliance, block the traffic without scanning, or scan the traffic and then either block or monitor the traffic, depending on actions configured in policies.

Multi-Bridge mode is suitable when you want to use Deep Discovery Web Inspector as an inline device and there are two network paths to the Internet and two separated internal networks that you want to monitor and secure.

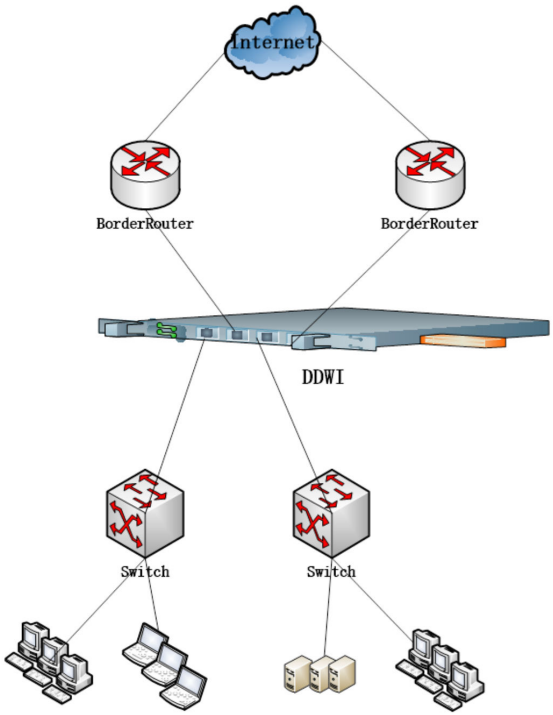


FIGURE 2-5. Multi-Bridge mode deployment

To deploy Multi-Bridge mode:

- The appliance must be equipped with two bypass cards, one for each line.
  - You must acquire and install the second bypass card before you can configure a Multi-Bridge Mode deployment.
  - See *Adding a Second Bypass Adapter to the Appliance on page 2-21*.

- LACP cannot be enabled.
- There can be no device interference between the lines.

LACP Deployments

In your enterprise environment, you might have requirements for increased reliability for network links. Deep Discovery Web Inspector can provide this increased reliability by supporting LACP link aggregation, which provides increased reliability through link redundancy. In addition, LACP supports two-way load balancing.

- For environments where you want to enable LACP:
  - When LACP is enabled, Deep Discovery Web Inspector automatically creates a two-port aggregate for data ingress and a two-port aggregate for data egress on the appliance.
  - You can implement LACP under Transparent Bridge mode and Transparent HA mode.
- LACP is available only on appliances equipped with two bypass cards.
  - You must acquire and install the second bypass card before you can configure an LACP-enabled deployment.
  - See *Adding a Second Bypass Adapter to the Appliance on page 2-21*.

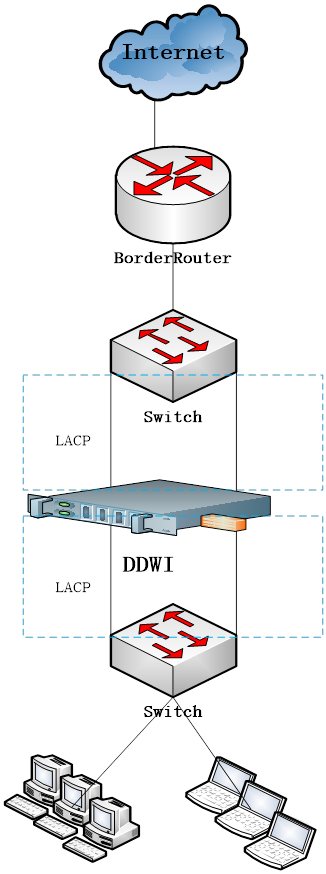


FIGURE 2-6. Transparent Bridge mode with LACP

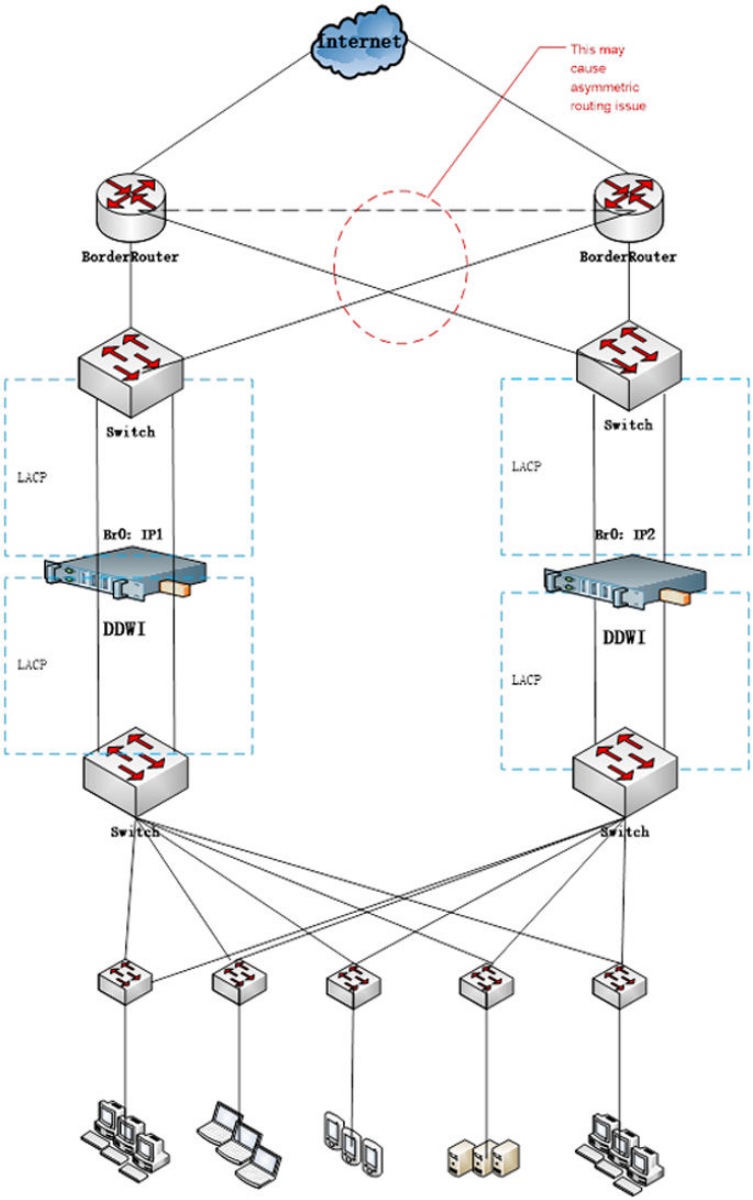


FIGURE 2-7. Transparent HA mode with LACP

Important

- Deep Discovery Web Inspector only supports LACP passive mode; therefore, LACP on the peer device must work under active mode.
- Deep Discovery Web Inspector does not support dynamic LACP mode link aggregation.
- LACP cannot be enabled with Multi-Bridge deployments (a variation of Transparent Bridge mode).

For more, see *How LACP Works With Deep Discovery Web Inspector on page 2-19*.

How LACP Works With Deep Discovery Web Inspector

Customers often need greater than 1 GB bandwidth for traffic traversing a Deep Discovery Web Inspector appliance. To provide increased bandwidth to meet customer needs, Deep Discovery Web Inspector supports LACP (Link Aggregation Control Protocol, 802.3ad standard) for configuring Ethernet interfaces. LACP is a layer 2 protocol that provides functionality when aggregating one or more Ethernet interfaces to form a single logical link (link aggregation groups).

Use the following table to determine LACP support for each deployment mode.

MODE	LACP SUPPORTED
Forward Proxy	No
Transparent Bridge	Yes
Multi-Bridge (a variation of Transparent Bridge mode)	No
Transparent HA	Yes

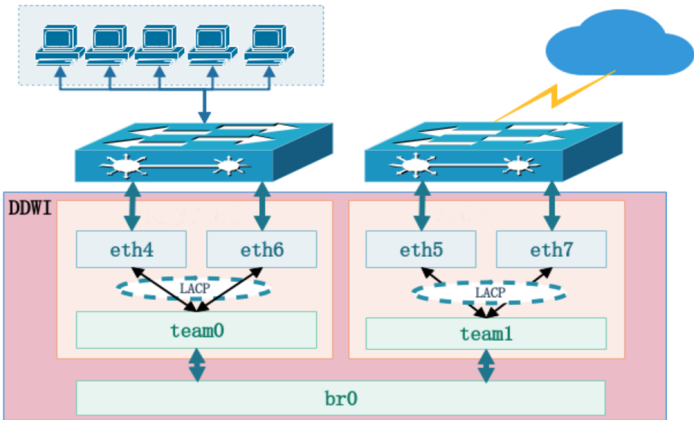


FIGURE 2-8. LACP enabled on Transparent Bridge mode

General Information

You should keep the following information in mind:

- LACP is available only on appliances equipped with two bypass cards.
- The switches to which Deep Discovery Web Inspector connects must support LACP and LACP ports must be configured for active mode.

  Deep Discovery Web Inspector automatically configures LACP on the appliance for passive mode.
- When LACP is enabled, Deep Discovery Web Inspector automatically creates the following two-link aggregates.
  - **team0**: **eth4** and **eth6**
  - **team1**: **eth5** and **eth7**
- You must configure active LACP link aggregation on the switch to match the appliance's LACP configuration.

  The speed of all network ports used for LACP must be the same.
- After enabling LACP, Deep Discovery Web Inspector provides two-way load balancing.

Information for Transparent Bridge with LACP

- Transparent Bridge interfaces:
  - **eth0**: Used as the management interface
  - **team0**/**team1**: Used for data ingress and data egress respectively

    If one of the links in a trunk is down, then the other link continues to support data.

Information for Transparent HA with LACP

Transparent HA interfaces:

- **eth0**: Used as the management interface
- **team0**/**team1**: Used for data ingress and data egress respectively

  If one of the links in a trunk is down, then the other link continues to support data.
- **br0**: Virtual L3 interface used to manage data ingress/egress for the LACP trunk links.

  If one of the links in a trunk is down, the **br0** virtual interface continues to work.

  Each node of the HA pair maintains separate connectivity to the Internet and internal network and uses a unique br0 IP address.

Adding a Second Bypass Adapter to the Appliance

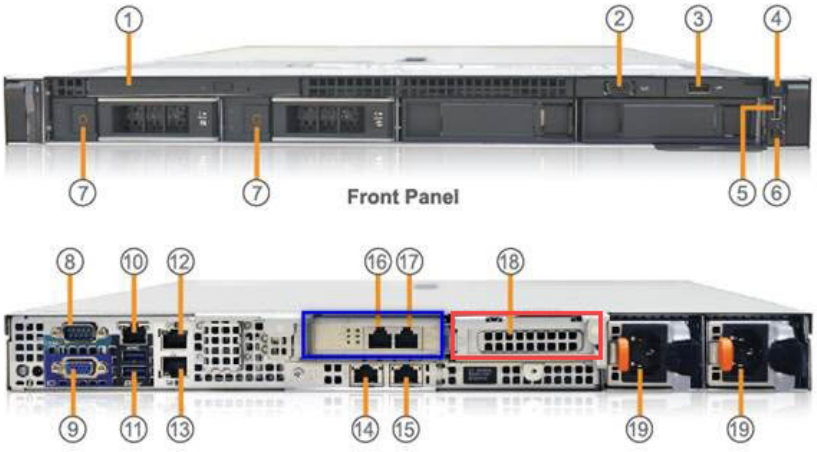
When deploying Multi-Bridge mode or LACP-enabled configurations on your Deep Discovery Web Inspector appliance, the appliance configures data ingress/egress using the eth4/eth5 (bypass card 1), eth6/eth7 (bypass card 2) interfaces.

Deep Discovery Web Inspector uses an external NIC adapter (Silicom: Dual Port LAN Bypass Adapter (PE2G2BPI80)) that is plugged into the first Fiber NIC slot (labeled as 16, 17 below) to support Bridge Mode and bypass mode. To deploy Multi-Bridge or LACP-enabled deployments, you must plug a second Dual Port LAN Bypass Adapter into your appliance using the second Fiber NIC slot (18).

Use the following procedure to insert the second bypass adapter into the appliance.

Procedure

1. Identify the location of the empty Fiber NIC slot (18) using the following diagram:



(1) Optical drive
(2) Front video connector
(3) USB Connector
(4) Power-on indicator
(5) USB connector
(6) IDRAC Direct (Micro-AB USB)
(7) Hard drives
(8) Serial connector
(9) Back video connector
(10) IDRAC port
(11) USB connector
(12) Management port (M) eth0
(13) NIC eth1
(14) NIC eth2 (not used)
(15) NIC eth3 (not used)
(16) Transparent Bridge Egress eth5 (E)
(17) Transparent Bridge Ingress eth4 (I)
(18) Fiber NIC slot
(19) Power supply connector

2. Open the package and inspect the Silicom Dual Port LAN Bypass Adapter.

   The model and specification are at the following link: Silicom Dual Port LAN Bypass Adapter (PE2G2BPI80) specifications

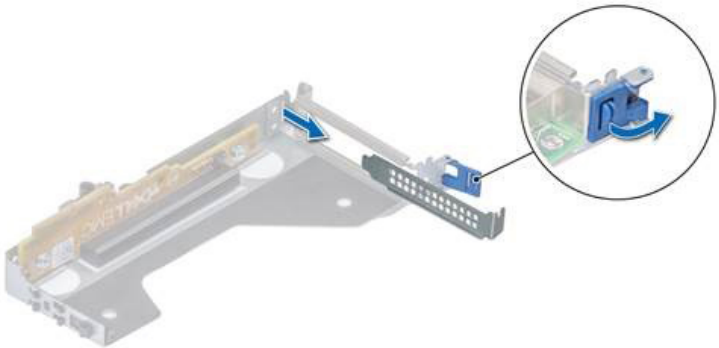
P/N	DESCRIPTION	NOTES
PE2G2PBI80-SD-R	Dual Port Copper Gigabit PCI Ethernet PCI Express Bypass Server Adapter	x4, Based on Intel 82580DB, PCI-E Gen 2.0, RoHS compliant

3. Add the Dual Port LAN Bypass Adapter using the Fiber NIC slot.

   a. Perform a system shut down by pressing the Deep Discovery Web Inspector appliance's power button.

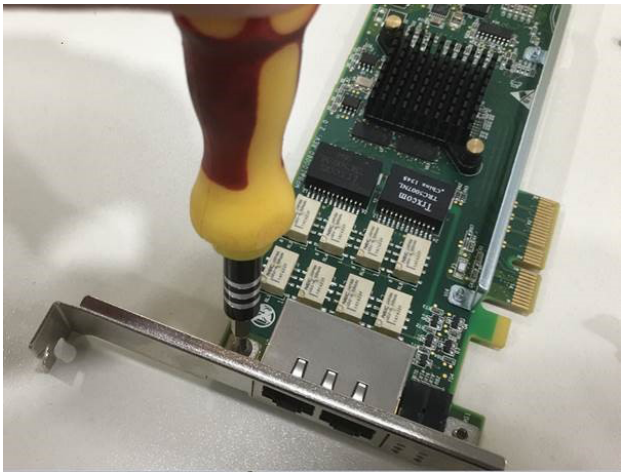
   b. Disconnect the appliance from the power supplies.

   c. Open the appliance chassis and pull the PCIe adapter holder latch, then remove the filler bracket.

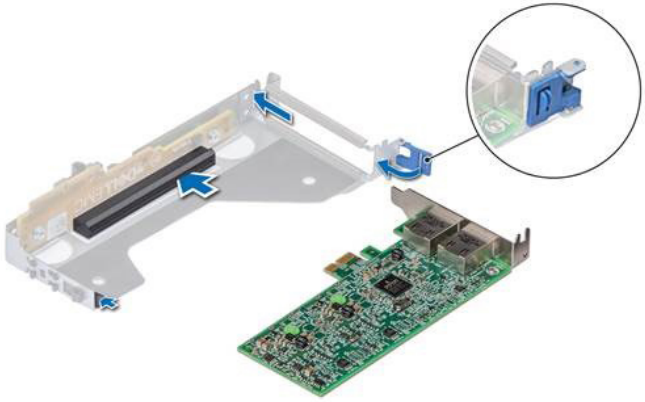


   d. Replace the standard adapter riser with the provided low-profile riser using the following images for guidance.

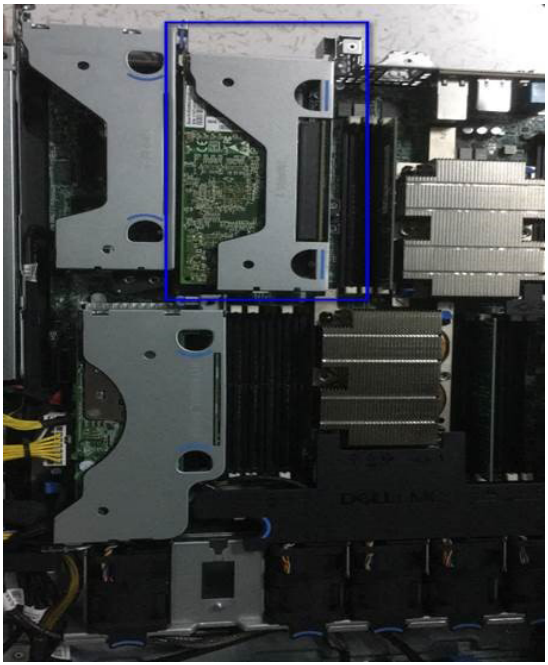
The Deep Discovery Web Inspector appliance supports only a low profile PCI adapter riser (also known as LPPCI or half-height adapters), but the Silicom Dual Port LAN Bypass Adapter is a standard (full height) PCI adapter by default. So you must replace the bracket on the LAN Bypass Adapter with the low-profile riser.



e. Hold the adapter by its edges and align the adapter edge connector with the adapter connector on the riser. Insert the adapter edge connector firmly into the adapter connector until the adapter is fully seated. Then close the adapter retention latch.



f. Fix the adapter holder latch into the appliance's chassis.



g. Close the appliance chassis and power on machine.

The LED per port of the bypass adapter turns on bypass (green), which means the bypass adapters are inserted correctly.

Recommended Network Environment

Deep Discovery Web Inspector requires connection to a management network. After deployment, administrators can perform configuration tasks from any computer on the management network.

The appliance model determines what the maximum expected throughput and maximum concurrent connections are in your network environment. You can use the following table when deciding on which model to deploy:

Appliance Model	Maximum Throughput	Maximum HTTPS Throughput	Maximum Concurrent Connections
1100	1 Gbps	700 Mbps	40,000
510	500 Mbps	350 Mbps	20,000

System Requirements

Deep Discovery Web Inspector is a hardware appliance with all software pre-installed. It is ready to deploy on your network as shipped from the manufacturer.

The following table lists the minimum software requirements to access the command line interface and the web management console that are used to manage Deep

Discovery Web Inspector. Before deployment, you should review the list and ensure that you can meet the browser and SSH client software requirements.

TABLE 2-1. Minimum Software Requirements

APPLICATION	REQUIREMENTS	DETAILS
SSH client	SSH protocol version 2	Set the Command Line Interface terminal window size to 80 columns and 24 rows.
Microsoft Internet Explorer	Version 11	Use only a supported browser to access the management console. Using the data port IP address you set during the initial configuration, specify the following URL: `https://[Appliance_IP_Address]`
Microsoft Edge	Windows 10	
Mozilla® Firefox®	Version 70 or later	
Google Chrome™	Version 78 or later	
Mac® Safari®	Mac OS 12.0.3 or later	

- Trend Micro recommends viewing the console using a monitor that supports 1280 x 1024 resolution or greater.
- By default, the SSH service is disabled and is not started when enabled. To use SSH, you must first enable and then start the SSH service.
- Make sure that the management interface eth0 (on the back of the appliance) is accessible via TCP port 22 for the Command Line Interface (SSH) and TCP port 443 for the management console (HTTPS).

Related information

↪ *Enabling and Starting the SSH Service*

Enabling and Starting the SSH Service

By default, the SSH service is disabled and is not started when enabled. You must use the command line interface to first enable and then start the SSH service.

Procedure

1. To enable and start the SSH service, first enter the CLI.

   Entering the CLI on page 8-2.

2. Enable the SSH service.

   ```
   configure service ssh enable
   ```

3. Start the SSH service.

   ```
   start service ssh
   ```

Ports Used by the Appliance

The following table shows the ports that are used with Deep Discovery Web Inspector and why they are used.

TABLE 2-2. Ports used by Deep Discovery Web Inspector

PORT	PROTOCOL	FUNCTION	PURPOSE
22*	TCP	Listening	Endpoints connect to Deep Discovery Web Inspector through SSH. *Because SSH is disabled by default, this port is not used by default. If you enable and start SSH, Deep Discovery Web Inspector then listens on this port.
53	TCP/UDP	Outbound	Deep Discovery Web Inspector uses this port for DNS resolution.
80*	TCP	Listening and outbound	Deep Discovery Web Inspector listens on this port when uploading Virtual Analyzer images. *All other access to Deep Discovery Web Inspector is secured by SSL, which uses 443.

PORT	PROTOCOL	FUNCTION	PURPOSE
123	UDP	Outbound	Deep Discovery Web Inspector connects to the NTP server to synchronize time.
161	UDP	Listening	Deep Discovery Web Inspector uses this port to listen for requests from SNMP managers.
162	UDP	Outbound	Deep Discovery Web Inspector connects to SNMP managers to send SNMP trap messages.
389	TCP	Outbound	Deep Discovery Web Inspector uses this port to do LDAP connections to Active Directory domain controller servers and to handle LDAP authentication.

PORT	PROTOCOL	FUNCTION	PURPOSE
443	TCP	Listening and outbound	Deep Discovery Web Inspector uses this port to: • Query the Predictive Machine Learning engine • Access the management console with a computer through HTTPS • Communicate with Trend Micro Apex Central • Communicate with Deep Discovery Director • Connect to the Smart Protection Network and query Web Reputation Services • Connect to Trend Micro Threat Connect • Send anonymous threat information to Smart Feedback • Update components by connecting to the ActiveUpdate server • Send product usage information to Trend Micro feedback servers • Share threat intelligence information and exception list with other products
443	TCP	Listening	Deep Discovery Web Inspector uses this port when authenticating and to redirect customers' web traffic to Captive Portal to do Kerberos/NTLM/ Basic Captive Portal authentication.

PORT	PROTOCOL	FUNCTION	PURPOSE
3268	TCP	Outbound	Deep Discovery Web Inspector uses this port when authenticating and to redirect customers' web traffic to Captive Portal to do Kerberos/NTLM/ Basic Captive Portal authentication.
User-defined	N/A	Outbound	Deep Discovery Web Inspector uses specified ports to: • Send logs to syslog servers • Share threat intelligence with integrated products/services • Send emails by SMTP

Items to Prepare

Before beginning the deployment, ensure that the following preparations are complete.

General Requirements

REQUIREMENT	DETAILS
Activation Code	Obtain from Trend Micro
Monitor and VGA cable	Connect to the VGA port of the appliance
USB keyboard	Connect to a USB port of the appliance
Internet-enabled computer	Access to the management console from a computer with the following software installed: A supported web browser: • Microsoft Internet Explorer 11 • Microsoft Edge Windows 10 • Mozilla® Firefox® 70 or later • Google Chrome™ 78 or later

Requirement	Details
	• Mac® Safari® Mac OS 12.0.3 or later
Third party software licenses	Licenses for all third-party software installed on sandbox images

Forward Proxy Mode

Requirement	Details
Ethernet cable (1 cable)	• **eth0** This is the data interface, used for both management and data.
IPv4 address (1 address)	• Assigned to the **eth0** data interface.

Transparent Bridge Mode

Topology: Transparent Bridge Mode on page 2-5

Requirement	Details
Ethernet cables (3 cables)	• **eth0** The management interface — connects to management network. • **eth4** Data ingress interface — connects to **upstream switch**. • **eth5** Data egress interface — connects to **downstream switch**.
IPv4 address (1 address)	• Assigned to the **eth0** management interface.

REQUIREMENT	DETAILS
	Note In Transparent Bridge mode, **eth4** and **eth5** act as layer 2 interfaces and are not assigned IP addresses.

Transparent Bridge Mode With Trunks

Topology: Transparent Bridge Mode With Trunks on page 2-6

REQUIREMENT	DETAILS
Ethernet cables (5 cables)	• **eth0** The management interface - connects to management network. • **eth4** / **eth6** Deep Discovery Web Inspector automatically creates the **team0** trunk for data ingress. Data ingress: **team0** connects to LACP aggregated ports on **upstream switch1**. • **eth5** / **eth7** Deep Discovery Web Inspector automatically creates the **team1** trunk for data egress. Data egress: **team1** connects to LACP aggregated ports on **downstream switch1**.
IPv4 addresses (2 addresses)	• One assigned to the **eth0** management interface. One assigned to the **br0** virtual data interface. **Note** In Transparent Bridge mode with LACP, **team0** and **team1** act as layer 2 interfaces and are not assigned IP addresses. However, **br0** , the virtual data interface is assigned an IPv4 address.

Transparent HA Mode

There are two nodes in Transparent HA mode implementations.

Topology diagram: *Topology and Requirements: Transparent HA Mode on page 2-9*

REQUIREMENT	DETAILS
Ethernet cables (3 cables per node)	**Node 1** requires the following cabling: • **eth0** The management interface — connects to management network. • **eth4** Data ingress interface — connects to **upstream switch1**. • **eth5** Data egress interface — connects to **downstream switch1**. **Node 2** requires the following cabling: • **eth0** The management interface — connects to management network. • **eth4** Data ingress interface — connects to **upstream switch2**. • **eth5** Data egress interface — connects to **downstream switch2**.
IPv4 addresses (1 address per node)	• For each node, assign an IP address to the **eth0** management interface.

REQUIREMENT	DETAILS
	Note In Transparent HA mode, **eth4** and **eth5** act as layer 2 interfaces and are not assigned IP addresses.

Transparent HA Mode With Trunks

There are two nodes in Transparent HA mode implementations.

Topology and Requirements: Transparent HA Mode With Trunks on page 2-11

REQUIREMENT	DETAILS
Ethernet cables (5 cables per node)	**Node 1** requires the following cabling: • **eth0** The management interface — connects to management network. • **eth4** / **eth6** Deep Discovery Web Inspector automatically creates the **team0** trunk for data ingress. Data ingress: **team0** connects to LACP aggregated ports on **upstream switch1**. • **eth5** / **eth7** Deep Discovery Web Inspector automatically creates the **team1** trunk for data egress. Data egress: **team1** connects to LACP aggregated ports on **downstream switch1**. **Node 2** requires the following cabling: • **eth0** The management interface — connects to management network. • **eth4** / **eth6**

REQUIREMENT	DETAILS
	Deep Discovery Web Inspector automatically creates the **team0** trunk for data ingress. Data ingress: **team0** connects to LACP aggregated ports on **upstream switch2**. • **eth5** / **eth7** Deep Discovery Web Inspector automatically creates the **team1** trunk for data egress. Data egress: **team1** connects to LACP aggregated ports on **downstream switch2**.
IPv4 addresses (2 IP addresses per node)	• For each node, assign an address to the **eth0** management interface. For each node, assign an address to the **br0** virtual data interface. **Note** In Transparent HA mode with LACP, **team0** and **team1** act as layer 2 interfaces and are not assigned IP addresses. However, **br0** , the virtual data interface is assigned an IPv4 address on each node.

Multi-Bridge Mode (A Variation of Transparent Bridge Mode)

Multi-Bridge Mode on page 2-14

REQUIREMENT	DETAILS
Ethernet cables (5 cables)	• **eth0** The management interface — connects to management network. • **eth4** / **eth5** Data ingress: **eth4** — connects to **upstream switch 1**. Data egress: **eth5** — connects to **upstream switch 2**.

REQUIREMENT	DETAILS
	• **eth6** / **eth7** Data ingress: **eth6** — connects to **downstream switch 1**. Data egress: **eth7** — connects to **downstream switch 2**. **Note** You cannot enabled LACP on a Multi-Bridge deployment.
IPv4 address (1 address)	• Assigned to the **eth0** management interface. **Note** In Multi-Bridge mode, **eth4**/**eth5** and **eth6**/**eth7** act as layer 2 interfaces and are not assigned IP addresses.

Apex Central Deployment

In a network topology containing multiple Deep Discovery Web Inspector appliances, Trend Micro Apex Central can aggregate suspicious objects data.

With Trend Micro Apex Central integration, Deep Discovery Web Inspector appliances can defend from threats happening in the world in real time. Deep Discovery Web Inspector supports bi-directional synchronization of two types of suspicious objects between Apex Central and Deep Discovery Web Inspector: Virtual Analyzer suspicious objects and user-defined suspicious objects. Deep Discovery Web Inspector can block the traffic if matched in the synchronized high-risk suspicious objects list.

In addition, the exceptions list is bi-directionally synchronized between Apex Central and Deep Discovery Web Inspector.

See *Registering to Apex Central From Deep Discovery Web Inspector Console on page 4-40* for details about configuring the Apex Central setting.

Note

You can register the Deep Discovery Web Inspector appliance to only one of either Apex Central or Deep Discovery Director at any given time. You cannot register the appliance with both products at the same time.

If the appliance is already registered with Deep Discovery Director, you cannot register with Apex Central until you unregister Deep Discovery Director.

Chapter 3

Deployment

Topics include:

- *Setting up the Hardware on page 3-2*
- *Configuring Management Console Access on page 3-2*
- *Opening the Management Console on page 3-5*
  - *Changing Your Password on page 3-6*
- *Activating the License on page 3-6*
- *Performing the Initial Deployment on page 3-9*
  - *Initial Deployment for Forward Proxy Mode on page 3-9*
  - *Initial Deployment for Transparent Bridge Mode on page 3-12*
  - *Initial Deployment for Transparent HA Mode on page 3-15*
  - *Initial Deployment for Multi-Bridge Mode on page 3-19*
  - *Initial Deployment for LACP on page 3-22*

Setting up the Hardware

Your appliance shipped with the software installed and licensed. Before you can deploy and configure Deep Discovery Web Inspector, you must set up the hardware.

Procedure

1. Use the Deep Discovery Web Inspector *Quick Start Card* that came with your appliance to set up the hardware and cable the appliance to the network.
2. Connect a USB keyboard and monitor to the appliance.
3. Power on the Deep Discovery Web Inspector appliance.

What to do next

After, power on is complete, you can log in to the command line interface (CLI) to configure management console access.

Configuring Management Console Access

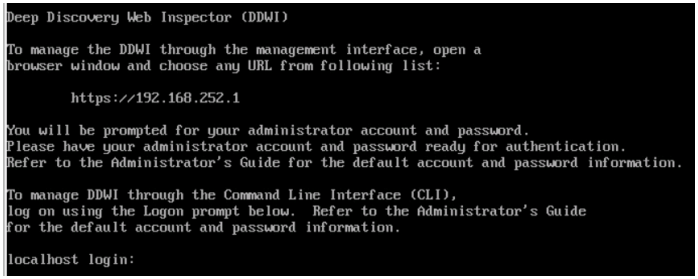
Before you can perform the initial deployment of Deep Discovery Web Inspector, you must log on to the Command Line Interface (CLI) and configure access to the Deep Discovery Web Inspector management console.

The following procedure explains how to log on to the CLI and configure the required network settings:

Procedure

1. Power up the appliance if it is not already up.
2. To make a direct connection, connect a monitor and keyboard to the Deep Discovery Web Inspector appliance.

The appliance's command line interface is displayed on the monitor. You can log in to the CLI and perform basic tasks.



3. Log in to the CLI with the default credentials.

   - User name: `admin`
   - Password: `ddwi`

4. At the prompt, type `enable` and press Enter to enter privileged mode.

5. Type the default password, `trend#1`, and then press Enter.

   The prompt changes from > to #.

6. Configure network settings with the following command:

   ```
   configure network basic
   ```

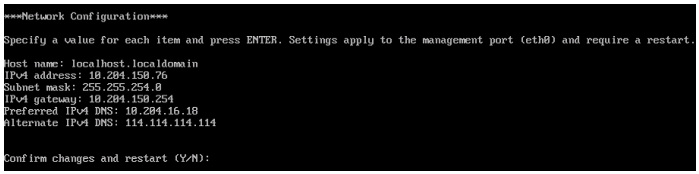
7. Configure the following network settings and press Enter after typing each setting.

Note

The default management IP address / subnet mask is `192.168.252.1` / `255.255.0.0`.

You should reserve the IP address `192.168.252.1` for Deep Discovery Web Inspector use only to prevent conflicts and possible configuration failures because of duplicate IP addresses on the network.

- Host name
- IPv4 address
- Subnet mask
- IPv4 gateway
- Preferred IPv4 DNS
- Alternate IPv4 DNS



8. Type `Y` to confirm settings and restart.

Deep Discovery Web Inspector implements the specified network settings and then restarts network services.

You can now access the Deep Discovery Web Inspector management console using a supported Web browser by accessing `https://<management_IP_address>`.

Note

You can log on to the CLI later to perform additional configuration, troubleshooting, or maintenance tasks:

Using the Command Line Interface on page 8-1.

Opening the Management Console

Deep Discovery Web Inspector provides a built-in management console that you can use to configure and manage the product.

You can connect to the management console using any supported web browser.

See *System Requirements on page 2-27*.

Procedure

1. In a web browser, type the IP address of the Deep Discovery Web Inspector server.

   `https://<management_IP_address>`

   The default URL is `https://192.168.252.1`.

   You should reserve the IP address `192.168.252.1` for Deep Discovery Web Inspector use only to prevent conflicts and possible configuration failures because of duplicate IP addresses on the network.

   The log on screen appears.

2. Specify the log on credentials (user name and password).

Note

Use the default administrator log on credentials when logging on for the first time:

- User name: `admin`
- Password: `ddwi`

3. Click **Log On**.

   The **Dashboard** screen opens.

   Important

   Trend Micro recommends changing the password to prevent unauthorized changes to the management console.

Related information

↪ *Changing Your Password*

Changing Your Password

You can change your password when you are logged on to the management console.

Procedure

1. On the management console banner, click your account name and then click **Change password**.

   The **Change Password** screen appears.

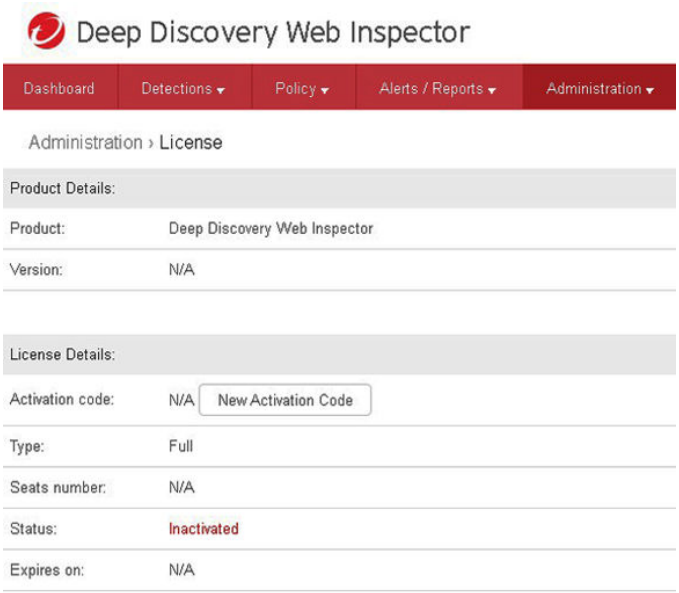
2. Specify password settings.
   - **Old password**
   - **New password**
   - **Confirm password**
3. Click **Save**.

Activating the License

You must activate the Deep Discovery Web Inspector license before performing the initial deployment.

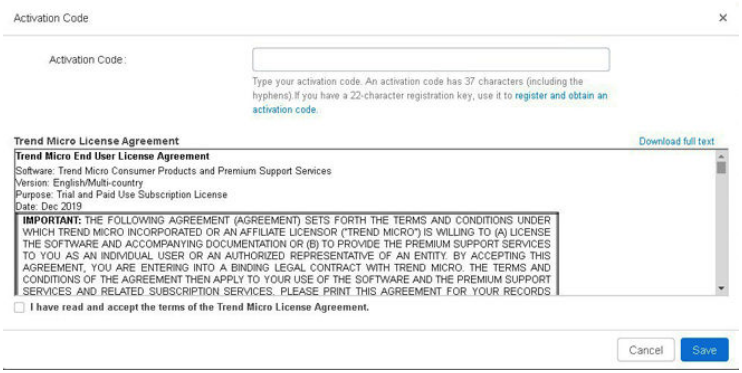
Procedure

1. Go to **Administration** > **License**.



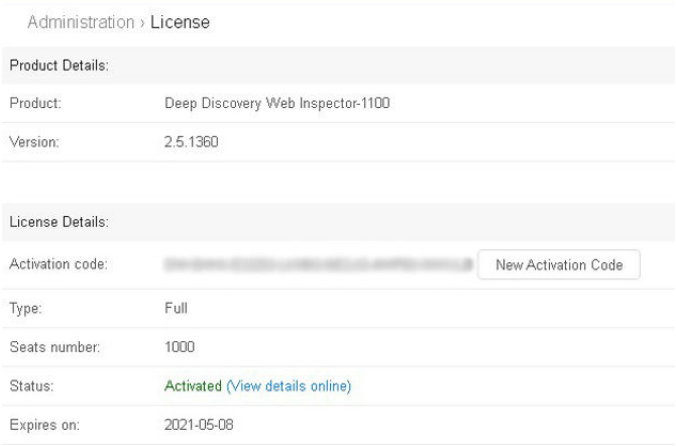
2. Click **New Activation Code**.

The **Activation Code** screen displays.



3. Specify the new activation code.
4. Read the license agreement and select **I have read and accept the terms of the Trend Micro License Agreement**.
5. Click **Save**.

   The Deep Discovery Web Inspector activates.



Performing the Initial Deployment

After activating the Deep Discovery Web Inspector license, you can use the **Deployment Wizard** to configure your Deep Discovery Web Inspector appliance's basic settings.

Perform one of the following initial deployments, depending on the desired deployment mode.

- *Initial Deployment for Forward Proxy Mode on page 3-9*
- *Initial Deployment for Transparent Bridge Mode on page 3-12*
- *Initial Deployment for Transparent HA Mode on page 3-15*
- *Initial Deployment for Multi-Bridge Mode on page 3-19*
- *Initial Deployment for LACP on page 3-22*

Related information

↪ *Network Deployment Mode Overview*

Initial Deployment for Forward Proxy Mode

You can use the **Deployment Wizard** to configure the basic settings for forward proxy mode on your Deep Discovery Web Inspector appliance.

Note

You can exit the **Deployment Wizard** at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to **Administration** > **Deployment Wizard**.

   The **Welcome** page opens.

2. In the **Deployment Mode** section, select **Forward proxy**.
3. Click **Next**.
4. In the **Working Mode Settings** page, specify the following details.

HTTP listening port	Specify the port that the proxy server uses to listen.
Enable upstream proxy	Select this option if the network uses an upstream proxy server and specify the IPv4 address and port number in **Proxy server** and **Port number**.

5. Click **Next**.
6. In the **Network** page, specify the following details:

OPTION	DESCRIPTION
Host name	Specify a host name.
Primary DNS server	Specify the IP address of the DNS server. This is a required setting.
Secondary DNS server	Optionally, specify the IP address for a secondary DNS server.
Data interface	This is a read-only field and is pre-set to **eth0**. This interface is also used for management.
Mode	This is a read-only field and is pre-set to **static**.
IPv4 address, **IPv4 mask**, and **Default IPv4 gateway**	Specify the IPv4 network settings.

7. Click **Next**.

   The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

OPTION	DESCRIPTION
NTP server	Enter the NTP server IP address.
System time zone	Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select `Etc` and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.

9. Click **Next**.

   The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Previous** and modify settings as required.

    b. If the settings are verified, click on **Done** to save the configuration.

Note

After you click **Done**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

Important

If you exit the wizard before saving settings, the configuration is not saved.

What to do next

To configure how Deep Discovery Web Inspector manages X-Header settings for the X-Forwarded-For and X-Authenticated-User fields, see *Configuring X-Header Handling Settings on page 4-44*.

Initial Deployment for Transparent Bridge Mode

You can use the **Deployment Wizard** to configure the basic settings for transparent bridge mode on your Deep Discovery Web Inspector appliance.

Prerequisite When Using LACP Trunk Links

As part of the configuration, you can enable LACP and use trunked interfaces for data ingress and data egress. To deploy LACP link aggregation for Transparent Bridge mode, the appliance must be equipped with two bypass cards. You must configure the connected switches with the corresponding LACP configuration.

See *How LACP Works With Deep Discovery Web Inspector on page 2-19*.

You can exit the **Deployment Wizard** at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to **Administration** > **Deployment Wizard**.

   The **Welcome** page opens.

2. In the **Deployment Mode** section, select **Transparent bridge**.

3. Click **Next**.

4. In the **Working Mode Settings** page, specify the following:

OPTION	DESCRIPTION
HTTP port	Scan for HTTP traffic on this port. Default is 80.

Option	Description
HTTPS port	Scan for HTTPS traffic on this port. Default is 443.

5. Click **Next**.

6. In the **Network** page, specify the following details:

Option	Description
Host name	Specify a host name.
Primary DNS server	Specify the IP address of the DNS server. This is a required setting.
Secondary DNS server	Optionally, specify the IP address for a secondary DNS server.
Enable LACP	Select if using LACP to aggregate network bandwidth. Interfaces **eth4/eth6** and **eth5/eth7** will be teamed to become **team0** and **team1** respectively. **Note** This field is visible only the appliance is equipped with two bypass cards. The eth4-eth7 ports must be connected to a switch with LACP enabled. Additionally, the switch ports connected to eth4/eth6 must be teamed and the switch ports connected to eth5/eth7 must be teamed.
LACP bond interface	This option is visible only if LACP is enabled. A read-only field, preset to **eth4/eth5/eth6/eth7**.
Data ingress / egress interface	This is a read-only field and is pre-set. • LACP not enabled: Field is pre-set to **eth4/eth5** • LACP enabled: Field is pre-set to **team0/team1**
Management interface	This is a read-only field and is pre-set to **eth0**.

OPTION	DESCRIPTION
Mode	This is a read-only field and is pre-set to **static**.
IPv4 address, **IPv4 mask**, and **Default IPv4 gateway**	Specify the IPv4 network settings.

7. Click **Next**.

   The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

OPTION	DESCRIPTION
NTP server	Enter the NTP server IP address.
System time zone	Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select `Etc` and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.

9. Click **Next**.

   The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Previous** and modify settings as required.

    b. If the settings are verified, click on **Done** to save the configuration.

Note

After you click **Done**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

Important

If you exit the wizard before saving settings, the configuration is not saved.

Initial Deployment for Transparent HA Mode

You can use the **Deployment Wizard** to configure the basic settings for Transparent HA mode on your Deep Discovery Web Inspector appliances. Transparent HA mode is a two-node solution. Perform the following procedure on each node.

Prerequisite: Deep Discovery Director Integration

Configuration and policy settings are synchronized between the two Deep Discovery Web Inspector HA nodes. This synchronization is not implemented by the Deep Discovery Web Inspector itself, but by the Deep Discovery Director appliance to which the Deep Discovery Web Inspector nodes are registered. The synchronization is accomplished by configuring the Deep Discovery Director synchronization scheduling task.

Therefore, to implement a Transparent HA mode deployment, you must integrate and register each of the Deep Discovery Web Inspector HA nodes to Deep Discovery Director.

Prerequisite When Using LACP Trunk Links

As part of the configuration, you can enable LACP and use trunked interfaces for data ingress and data egress. To deploy LACP link aggregation for Transparent HA mode, the appliance must be equipped with two bypass cards. You must configure the connected switches with the corresponding LACP configuration.

See *How LACP Works With Deep Discovery Web Inspector on page 2-19*.

You can exit the **Deployment Wizard** at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to **Administration** > **Deployment Wizard**.

   The **Welcome** page opens.

2. In the **Deployment Mode** section, select **Transparent HA**.

3. Click **Next**.

4. In the **Working Mode Settings** page, specify the following:

OPTION	DESCRIPTION
HTTP port	Scan for HTTP traffic on this port. Default is 80.
HTTPS port	Scan for HTTPS traffic on this port. Default is 443.

5. Click **Next**.

6. In the **Network** page, specify the following details:

OPTION	DESCRIPTION
Host name	Specify a host name.
Primary DNS server	Specify the IP address of the DNS server. This is a required setting.
Secondary DNS server	Optionally, specify the IP address for a secondary DNS server.

OPTION	DESCRIPTION
Enable LACP	Select if using LACP to aggregate network bandwidth. Interfaces **eth4/eth6** and **eth5/eth7** will be teamed to become **team0** and **team1** respectively. **Note** This field is visible only the appliance is equipped with two bypass cards. The eth4-eth7 ports must be connected to a switch with LACP enabled. Additionally, the switch ports connected to eth4/eth6 must be teamed and the switch ports connected to eth5/eth7 must be teamed.
LACP bond interface	This option is visible only if LACP is enabled. A read-only field, preset to **eth4/eth5/eth6/eth7**.
Data ingress / egress interface	Specify the data ingress/egress interface. • LACP not enabled: Field is pre-set to **eth4/eth5** • LACP enabled: Field is pre-set to **team0/team1**
Data interface	This is a read-only field and is pre-set to **br0**.
Enable VLAN ID	Select whether to enable the VLAN tag for the data interface and enter the VLAN ID number (1-4094).
IPv4 address, **IPv4 mask**, and **IPv4 gateway**	Specify the IPv4 network settings for the **br0** data interface.
Management interface	This is a read-only field and is pre-set to **eth0**.
Mode	This is a read-only field and is pre-set to **static**.
IPv4 address, **IPv4 mask**, and **Default IPv4 gateway**	Specify the IPv4 network settings for the management interface.

7. Click **Next**.

   The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

OPTION	DESCRIPTION
NTP server	Enter the NTP server IP address.
System time zone	Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select `Etc` and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.

9. Click **Next**.

   The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Previous** and modify settings as required.

    b. If the settings are verified, click on **Done** to save the configuration.

Note

After you click **Done**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

Important

If you exit the wizard before saving settings, the configuration is not saved.

What to do next

Configure synchronization between the two Deep Discovery Web Inspector nodes on the Deep Discovery Director appliance to which Deep Discovery Web Inspector is registered. The synchronization is accomplished by configuring the Deep Discovery Director synchronization scheduling task.

Please refer to the Deep Discovery Director documentation for procedures about configuring synchronization.

Important

1. Synchronization supports the replication of the following configuration list:

Dashboard	Detections	Policy
Alerts/Reports	Component updates	System settings
Active Directory Services	Virtual Analyzer	Integrated Products/ Services
Product Updates	System Maintenance	Accounts/Contacts
Audit Log/	License	Help…

2. This type of task does not support periodic tasks.
3. This type of task does not support synchronization between two Deep Discovery Web Inspector appliances. It only support synchronization from one Deep Discovery Web Inspector appliance to another Deep Discovery Web Inspector appliance.

Related information

↪ *Network Deployment Mode Overview*

Initial Deployment for Multi-Bridge Mode

You can use the **Deployment Wizard** to configure the basic settings for a Multi-Bridge deployment on your Deep Discovery Web Inspector appliance.

Important

To deploy a Multi-Bridge configuration, the appliance must be equipped with two bypass cards and LACP must be disabled.

You can exit the **Deployment Wizard** at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to **Administration** > **Deployment Wizard**.

   The **Welcome** page opens.

2. In the **Deployment Mode** section, select **Transparent bridge**.

3. Click **Next**.

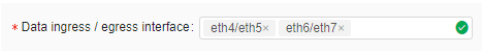
4. In the **Working Mode Settings** page, specify the following:

OPTION	DESCRIPTION
HTTP port	Scan for HTTP traffic on this port. Default is 80.
HTTPS port	Scan for HTTPS traffic on this port. Default is 443.

5. Click **Next**.

6. In the **Network** page, specify the following details:

OPTION	DESCRIPTION
Host name	Specify a host name.
Primary DNS server	Specify the IP address of the DNS server. This is a required setting.
Secondary DNS server	Optionally, specify the IP address for a secondary DNS server.

OPTION	DESCRIPTION
Enable LACP	Ensure that LACP is not enabled. This configuration only appears when the device is configured with two bypass cards. When deployed in a Multi-Bridge configuration, LACP must be disabled.
LACP bond interface	This option is visible only if LACP is enabled.
Data ingress / egress interface	Specify the data ingress/egress interface. When deployed in a Multi-Bridge configuration, select two pairs of network cards as **eth4/eth5 eth6/eth7**. 
Management interface	This is a read-only field and is pre-set to **eth0**.
Mode	This is a read-only field and is pre-set to **static**.
IPv4 address, **IPv4 mask**, and **Default IPv4 gateway**	Specify the IPv4 network settings.

7. Click **Next**.

   The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

OPTION	DESCRIPTION
NTP server	Enter the NTP server IP address.
System time zone	Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select `Etc` and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.

9. Click **Next**.

   The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Previous** and modify settings as required.

    b. If the settings are verified, click on **Done** to save the configuration.

Note

After you click **Done**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

Important

If you exit the wizard before saving settings, the configuration is not saved.

Initial Deployment for LACP

You can use the **Deployment Wizard** to configure the basic settings Transparent Bridge or Transparent HA mode deployments with LACP enabled.

As part of the configuration, you can enable LACP and use trunked interfaces for data ingress and data egress. To deploy LACP link aggregation for Transparent Bridge or Transparent HA modes, the appliance must be equipped with two bypass cards. You must configure the connected switches with the corresponding LACP configuration.

See *How LACP Works With Deep Discovery Web Inspector on page 2-19*.

Important

Keep the following in mind if configuring Transparent HA mode with LACP:

Configuration and policy settings are synchronized between the two Deep Discovery Web Inspector HA nodes. This synchronization is not implemented by the Deep Discovery Web Inspector itself, but by the Deep Discovery Director appliance to which the Deep Discovery Web Inspector nodes are registered. The synchronization is accomplished by configuring the Deep Discovery Director synchronization scheduling task.

Therefore, to implement a Transparent HA mode deployment, you must integrate and register each of the Deep Discovery Web Inspector HA nodes to Deep Discovery Director.

You can exit the **Deployment Wizard** at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to **Administration** > **Deployment Wizard**.

   The **Welcome** page opens.

2. In the **Deployment Mode** section, select **Transparent bridge** or **Transparent HA** according to your business needs.

3. Click **Next**.

4. In the **Working Mode Settings** page, specify the following:

OPTION	DESCRIPTION
HTTP port	Scan for HTTP traffic on this port. Default is 80.
HTTPS port	Scan for HTTPS traffic on this port. Default is 443.

5. Click **Next**.

6. In the **Network** page, specify the following details:

OPTION	DESCRIPTION
Host name	Specify a host name.
Primary DNS server	Specify the IP address of the DNS server. This is a required setting.
Secondary DNS server	Optionally, specify the IP address for a secondary DNS server.
Enable LACP	This configuration field only appears when the device is configured with two bypass cards. Enable LACP. Interfaces **eth4/eth6** and **eth5/eth7** will be teamed to become **team0** and **team1** respectively.
LACP bond interface	This option is visible only if LACP is enabled. A read-only field, preset to **eth4/eth5/eth6/eth7**.
Data ingress / egress interface	When LACP is enabled, this is a read-only field that is pre-set to **team0/team1**.
Data interface	Appears only under Transparent HA mode. This is a read-only field and is pre-set to **br0**.
Enable VLAN ID	Appears only under Transparent HA mode. Configuration is based on requirements.
IPv4 address, **IPv4 mask**, and **IPv4 gateway**	Appears only under Transparent HA mode. Configuration is based on requirements.
Management interface	This is a read-only field and is pre-set to **eth0**.
Mode	This is a read-only field and is pre-set to **static**.
IPv4 address, **IPv4 mask**, and **Default IPv4 gateway**	Specify the IPv4 network settings for the management interface.

7. Click **Next**.

   The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

OPTION	DESCRIPTION
NTP server	Enter the NTP server IP address.
System time zone	Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select `Etc` and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.

9. Click **Next**.

   The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Previous** and modify settings as required.

    b. If the settings are verified, click on **Done** to save the configuration.

Note

After you click **Done**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

Important

If you exit the wizard before saving settings, the configuration is not saved.

Related information

↪ *Network Deployment Mode Overview*

Chapter 4

Getting Started

This chapter describes how to get started with Deep Discovery Web Inspector after initial deployment is complete.

Topics include:

- *Management Console Navigation on page 4-2*
- *Getting Started Tasks on page 4-2*
- *Performing Additional Configuration Tasks on page 4-43*

Management Console Navigation

The management console consists of the following elements:

TABLE 4-1. Management Console Elements

SECTION	DETAILS
Banner	The management console banner contains: • Product logo and name: For details, see the Dashboard section of the *Deep Discovery Web Inspector Administrator's Guide*. • Name of the user currently logged on: Click and select **Change password** to change the account password (see *Changing Your Password on page 3-6*) or select **Log off** to log out of the management console. • System time: Displays the current system date and time. • Appliance IP address: Displays the IP address of the Deep Discovery Web Inspector appliance. • Network traffic: Displays the incoming and outgoing network throughput.
Main Menu Bar	The main menu bar contains several menu items that allow you to configure product settings. For some menu items, such as **Dashboard**, clicking the item opens the corresponding screen. For other menu items, sub-menu items appear when you click or mouse over the menu item. Clicking a sub-menu item opens the corresponding screen.
Context-sensitive Help	Use **Help** ( ) to find more information about the screen that is currently displayed.

Getting Started Tasks

After you complete the initial deployment, there are additional tasks you must perform to get Deep Discovery Web Inspector up and running as quickly as possible. Getting Started Tasks provides a high-level overview of these additional tasks. Each step links to more detailed instructions later in the document.

Procedure

1. Open the management console.

   For details, see *Opening the Management Console on page 3-5*.

2. Manage your Deep Discovery Web Inspector product license as needed.

   For details, see *Managing Your Product License on page 4-5*.

3. Configure additional network settings as needed.

   For details, see *Configuring Network Settings on page 4-5*.

4. Configure the notification SMTP server.

   For details, see *Configuring the Notification SMTP Server on page 4-8*.

5. Configure the desired Virtual Analyzer solution:

   You can configure Deep Discovery Web Inspector to use either the internal Virtual Analyzer server or to use Deep Discovery Analyzer as an integrated Virtual Analyzer solution to perform suspicious object analysis.

INTERNAL OR EXTERNAL	PERFORM THE FOLLOWING...
Internal	a. Import Virtual Analyzer Images For details, see *Importing Virtual Analyzer Images on page 4-9*. **Important** At least one Virtual Analyzer image is required to perform analysis. b. Configure a network connection for Virtual Analyzer sandbox instances. For details, see *Virtual Analyzer Network on page 4-13*. No network access is the default.
External	a. Record the Deep Discovery Analyzer API key.

INTERNAL OR EXTERNAL	PERFORM THE FOLLOWING...
	See Deep Discovery Analyzer documentation for more information. b. Configure Deep Discovery Analyzer integration. For details see, *Virtual Analyzer Integration with Deep Discovery Analyzer on page 4-16*.

6. (Optional) Configure proxy settings if your network uses proxy servers.

   For details, see *Configuring Proxy Settings on page 4-17*.

7. Add at least one notification recipient to all critical and important alerts.

   For details, see *Alerts on page 4-19*.

8. Configure policies used to determine how objects are scanned and what actions to take with policy matches.

   For details, see *Managing Policies on page 4-26* and *Managing User-Defined Settings on page 4-21*.

9. (Optional) Configure HTTPS decryption rules.

   For details, see *Managing HTTPS Decryption Rules on page 4-31*.

10. ((Optional) Register with Apex Central or Deep Discovery Director to download synchronized suspicious objects and the suspicious objects exception list.

    For details, see *Apex Central on page 4-39* or *Deep Discovery Director on page 4-42*.

Important

If you deployed the Deep Discovery Web Inspector appliances as a Transparent HA 2-node pair, you must register the appliances to Deep Discovery Director because Deep Discovery Director synchronization tasks are used to synchronize the Transparent HA pair.

Managing Your Product License

Procedure

1. Go to **Administration** > **License**.
2. Click **New Activation Code**.

   The **Activation Code** screen displays.
3. Specify the new activation code.
4. Read the Trend Micro license agreement and then click **I have read and accept the terms of the Trend Micro License Agreement**.
5. Click **Save**.

   The Deep Discovery Web Inspector activates.
6. View your product license.

   See *Viewing Your Product License on page 4-5*.

Viewing Your Product License

Procedure

1. Go to **Administration** > **License**.
2. Under **License Details**, click **View details online** to display product licensing details.

Configuring Network Settings

You can use the management console to make changes to the network interface settings after the initial deployment.

You can configure the host name, the IPv4 addresses of the Deep Discovery Web Inspector appliance, and other network settings.

Note

As part of the configuration, you can enable LACP and use trunked interfaces for data ingress and data egress. To deploy LACP link aggregation for Transparent Bridge or Transparent HA modes, the appliance must be equipped with two bypass cards. You must configure the connected switches with the corresponding LACP configuration.

See *How LACP Works With Deep Discovery Web Inspector on page 2-19*.

Procedure

1. Go to **Administration** > **System Settings** > **Network**.
2. Specify the general network settings that affect all interfaces.

OPTION	DESCRIPTION
Host name	Specify the host name.
Gateway	Specify the IPv4 address of the gateway.
Primary DNS server and **Secondary DNS server**	Specify the IPv4 addresses of the primary DNS server and optionally, the secondary DNS server.

3. Specify the IPv4 address and subnet mask for the `eth0` port:

   The `eth0` interface handles management console traffic, SSH connections, Trend Micro updates, and other related Trend Micro traffic.

   `eth0` is known as the:

   - **Data interface** for the **Forward Proxy** deployment mode
   - **Management interface** for the **Transparent Bridge** deployment mode
   - **Management interface** for the **Transparent HA** deployment mode

4. Specify the IPv4 address and subnet mask for the `eth1` port if you plan on using a custom network for Virtual Analyzer sandbox instances to connect to the Internet.

   The `eth1` interface is known as the dirty line port for Virtual Analyzer custom network connections. If **Custom network** is selected when configuring Virtual Analyzer network connections, Virtual Analyzer connects to the Internet using `eth1`, which is isolated from the management network.

5. Specify the IPv4 address and subnet mask for other Ethernet interface ports that you will use in your deployment.

   The available ports will vary depending on the deployment mode and your particular deployment.

Deployment Mode	Port Information
Forward proxy	`eth2` – `eth5`: L3 interfaces You can configure these ports with static IP addresses.
Transparent Bridge :	• `eth4`: Designated as **eth4 — Data Ingress Port** • `eth5`: Designated as **eth5 — Data Egress Port** You cannot assign IP addresses to these ports.
Transparent HA:	• `eth4`: Designated as **eth4 — Data Ingress Port** • `eth5`: Designated as **eth5 — Data Egress Port** You cannot assign IP addresses to these ports. For Transparent HA, you can modify the `br0` IP address and VLAN tag.
Transparent Bridge with LACP trunks	• `eth4`/`eth6`: Teamed to become the **team0** interface • `eth5`/`eth7`: Teamed to become the **team1** interface The teamed interfaces are used for data ingress/data egress. You cannot assign IP addresses to these ports.

Deployment Mode	Port Information
Transparent HA with LACP trunks	• `eth4`/`eth6`: Teamed to become the **team0** interface • `eth5`/`eth7`: Teamed to become the **team1** interface The teamed interfaces are used for data ingress/data egress. You cannot assign IP addresses to these ports. You can modify the `br0` IP address and VLAN tag.

6. Click **Save**.

   When you save network changes, network services are restarted. After the restart, you must log on to the console again.

Configuring the Notification SMTP Server

Deep Discovery Web Inspector uses the SMTP server to send alert notifications and reports to configured recipients.

Procedure

1. Go to **Administration** > **System Settings** > **SMTP**.
2. Specify the SMTP server settings.

Option	Description
Sender email address	This is the email address used to send notifications and reports.
Server address	Type the external SMTP server host name (FQDN) or IPv4 address.
Port	Type the external SMTP server port number.

OPTION	DESCRIPTION
Connection security	Select a security protocol if required for the connection. Options are `StartTLS` or `SSL/TLS`.
SMTP server requires authentication	Select this option if the connection to the SMTP server requires authentication and then configure the user name and password. **Note** Make sure that you configure the user name and password correctly. An external SMTP server may refuse connection from Deep Discovery Web Inspector after the maximum number of unsuccessful authentication attempts has been reached.

3. Click **Save**.

Importing Virtual Analyzer Images

If you are using the internal Virtual Analyzer, you must import a minimum of one virtual image.

Virtual Analyzer supports OVA files between 1GB and 30 GB in size.

You can import an image to Deep Discovery Web Inspector using one of the following methods:

- The Deep Discovery Web Inspector management console.
- Image deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

  You can use this method if Deep Discovery Web Inspector is registered to Deep Discovery Director.

Note

Virtual Analyzer stops analysis and keeps all samples in the queue whenever an image is added or deleted, or when instances are modified.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Images**.
2. Click **Import**.

   The **Import Image** screen appears.
3. Specify a name in the **Image** field.
4. Specify the number of instances for this image.
5. Select an image source and configure the applicable settings.
   - **Local or network folder**

     See *Importing an Image from a Local or Network Folder on page 4-11*.
   - **HTTP or FTP server**

     See *Importing an Image from an HTTP or FTP Server on page 4-12*.

Virtual Analyzer Image Preparation

Virtual Analyzer does not contain any images by default. To analyze samples, you must prepare and import at least one image in the Open Virtual Appliance (OVA) format.

You can use existing VirtualBox or VMware images, or create new images using VirtualBox. For details, see Chapters 2 and 3 of the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Before importing, validate and configure images using the Virtual Analyzer Image Preparation Tool. For details, see Chapter 4 of the *Virtual Analyzer Image Preparation User's Guide*.

Deep Discovery Web Inspector supports a maximum of three images at a time.

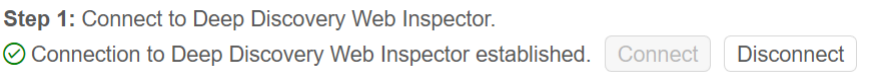
Importing an Image from a Local or Network Folder

The following procedure explains how to import an image into Virtual Analyzer from a local or network folder. Before you can import an image, your computer must be able to establish a connection to Deep Discovery Web Inspector.

Procedure

1. Select **Local or network folder**.
2. Specify an image name with a maximum of 260 characters/bytes.
3. Click **Connect**.

   From the connection status under **Step 1** of the **Images** screen, the status message verifies that the connection has been established.

4. Once connected, import the image using the Virtual Analyzer Image Import Tool.
   a. Click **Download Image Import Tool**.
   b. Open the file `VirtualAnalyzerImageImportTool.exe`.
   c. Specify the Deep Discovery Web Inspector management IP address.

      Note

      For information about configuring the Deep Discovery Web Inspector management IP address, see *Configuring Network Settings on page 4-5*.

   d. Click **Browse** and select the image file.
   e. Click **Import**.

      The import process will stop if:

- The connection to the device was interrupted
- Memory allocation was unsuccessful
- Windows socket initialization was unsuccessful
- The image file is corrupt

5. Wait for import to complete.

Note

Virtual Analyzer deploys the imported image to sandbox instances immediately after the image uploads.

Importing an Image from an HTTP or FTP Server

The following procedure explains how to import an image into Virtual Analyzer from an HTTP or FTP server.

Procedure

1. Select **HTTP or FTP server**.
2. Specify the HTTP or FTP URL settings.

OPTION	DESCRIPTION
URL	Specify the HTTP or FTP URL. Example: `ftp://custom_ftp:1080/tmp/test.ova`
User name	Optional: Specify the user name if authentication is required.
Password	Optional: Specify the password if authentication is required.
Anonymous Login	Optional: Select to disable the user name and password, and authenticate anonymously.

3. Click **Import**.

4. Wait for deployment to complete.

Note

Virtual Analyzer deploys instances immediately.

Virtual Analyzer Network

When Deep Discovery Web Inspector is using an internal Virtual Analyzer, you can configure how Virtual Analyzer instances connect to external destinations, including the Internet. You can configure no network access, access using the management port, or access using a custom port.

Note

Object analysis is paused and settings are disabled whenever Virtual Analyzer is being configured.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Network Connection**.
2. From the **Network type** drop-down list, select how Virtual Analyzer connects to the network.
   - No network access
   - Management network
   - Custom network

   For information about network types, see *Types of Virtual Analyzer Networks on page 4-15*.
3. Specify network connection settings, depending on the network type specified.

OPTION	DESCRIPTION
No network access	There are no configurable settings for this network type. This is the default selection.

Management network	**Proxy settings**
	• If a proxy server is not required for the internal Virtual Analyzer to connect to the Internet, select **Do not use a proxy server** from the drop-down list.
	• If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select **Use a dedicated proxy server** from the drop-down list and provide the following information:
	  • **Server address**
	  • **Port**
	  • **Proxy server requires authentication**: If authentication is required, select this check box and type the user name and password.

Custom Network	**Sandbox port**
	• If eth1 is not already configured, click **Configure IPv4 settings** to configure network settings.
	Proxy settings
	• If a proxy server is not required for the internal Virtual Analyzer to connect to the Internet, select **Do not use a proxy server** from the drop-down list.
	• If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select **Use a dedicated proxy server** from the drop-down list and provide the following information:
	  • **Server address**
	  • **Port**
	  • **Proxy server requires authentication**: If authentication is required, select this check box and type the user name and password.

4. Click **Save**.

5. After configuring the network connection, click **Test Internet Connectivity** to verify that Virtual Analyzer can connect to the Internet.

Note

If **No network access** is selected, a connection cannot be established. The default setting is **No network access**.

Types of Virtual Analyzer Networks

When simulating file behavior, Virtual Analyzer uses its own analysis engine to determine the risk of an object. The selected network type also determines whether submitted objects can connect to the Internet, and if so, which network is used to connect.

Note

Internet access improves analysis by allowing samples to access C&C callback addresses or other external links.

NETWORK TYPE	DESCRIPTION
No network access	Isolates Virtual Analyzer traffic within the sandbox environment. The environment has no connection to an outside network. **Note** Virtual Analyzer has no Internet connection and relies only on its analysis engine.

NETWORK TYPE	DESCRIPTION
Management network	Directs Virtual Analyzer traffic through the management port. **Important** Enabling connections to the management network may result in malware propagation and other malicious activity in the network. Trend Micro recommends using an environment isolated from the management network, such as a test network with Internet connection but without connection restrictions.
Custom network	Virtual Analyzer connects to the Internet using the eth1 port.

Virtual Analyzer Integration with Deep Discovery Analyzer

You can configure Deep Discovery Web Inspector to integrate with Deep Discovery Analyzer to perform suspicious object analysis.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **External Integration**.
2. In the **Source** drop-down, select **External**.
3. In the **Server address** field, provide the IP address or FQDN of the Deep Discovery Analyzer server.
4. If your company uses a proxy server, select **Connect using a proxy server**.

   For information about configuring proxy settings, see *Configuring Proxy Settings on page 4-17*.
5. Type the Deep Discovery Analyzer API key.
6. Click **Test Connection** to verify the server settings.
7. Click **Save**.

The status changes to registered. You can unregister from Deep Discovery Analyzer at any time and perform virtual analysis locally by choosing **Internal** as the source and then saving the configuration.

Configuring Proxy Settings

Configuring proxy settings affects:

- Certified Safe Software Service
- Community File Reputation
- Component updates (pattern files and scan engines)
- Product license registration
- Script Analyzer Engine
- Web Reputation queries
- Web Inspection Service
- Predictive Machine Learning
- Virtual Analyzer integration with Deep Discovery Analyzer

Procedure

1. Go to **Administration** > **System Settings** > **Proxy**.

   The **Proxy** screen appears.

2. Specify the proxy server settings.

OPTION	DESCRIPTION
Use a proxy server for Trend Micro services	Select to use a proxy server.
Proxy server	Specify the proxy server host name or IP address.

OPTION	DESCRIPTION
Port	Specify the port that the proxy server uses to connect to the Internet.
Proxy server requires authentication	Select if your proxy server requires authentication and then specify **User ID** and **Password**.

3. Click **Save**.

Note

Some Trend Micro services only support **Basic** authentication via system proxy. If **Basic** authentication is disabled in system proxy, these services will not work. The recommendation is to enable **Basic** authentication in system proxy, or put the external services into the white list of the system proxy.

For more information about external services FQDNs, see *Testing Network Connections on page 4-18*

Testing Network Connections

You can use the **Network Services Diagnostics** screen to test network connections using network tools such as ping and to test connectivity to other network services such as the ActiveUpdate and Web Reputation Service servers.

Procedure

1. Go to **Administration** > **System Maintenance** > **Network Services Diagnostics**.

2. Select one or more enabled services and click **Test**.

   Wait for the connection test to complete. The time required depends on the network environment and the number of services selected. View the connection test result in the **Result** column.

Important

Deep Discovery Web Inspector uses HTTPS to communicate with cloud services. If the Deep Discovery Web Inspector upstream devices have the HTTPS decryption feature enabled, it is recommended that you ensure that the following domains and URLs are not decrypted by the upstream devices. Otherwise, cloud query can fail and some Deep Discovery Web Inspector features might not work correctly.

- https://ddwi25-p.activeupdate.trendmicro.com/activeupdate
- https://ddwi25-wrs-p.activeupdate.trendmicro.com/activeupdate
- https://olr.trendmicro.com/redirect/product_register.aspx
- ddwi25-en-f.trx.trendmicro.com
- grid-global.trendmicro.com
- ddwi2-5-wis.trendmicro.com
- ubr-testing.trendmicro.com
- ddwi25-threatconnect.trendmicro.com
- ddwi25.icrc.trendmicro.com

Alerts

Alerts provide immediate intelligence about the state of Deep Discovery Web Inspector.

Alerts are classified into two categories:

- Critical alerts are triggered by events that require immediate attention.
- Important and informational alerts are triggered by events that require observation.

You can view or export information about triggered alerts.

Alert notifications are predefined and cannot be deleted; however, using alert notification rules you can make modifications to the predefined notifications to meet

your needs. The rules define what the conditions are for triggering an alert as well as defining what content to include within the notification.

Configuring Alert Notifications

Each alert notification has a default configuration that is defined in alert notification rules. You can modify the parameters for each alert notification rule.

Important

You must configure an SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 4-8*.

Procedure

1. Go to **Alerts / Reports** > **Alerts** > **Rules**.
2. Click the name of an alert under the **Rule** column.

   The alert rule configuration screen appears.
3. Configure the alert parameters.

   The list of message tokens that are valid for a specific notification is shown to the right of the message body.
4. Click **Save**.
5. Click **Back** to return to the **Rules** screen.

Alert Notification Parameters

You can modify the parameters for each rule such as the notification message header and body, alert frequency, and other parameters. You can also enable or disable the notification.

The default recipient setting is to send the alert notifications to all contacts. If you want to send an alert notification to specific recipients, you must add recipients to the corresponding notification alert rule.

If using the default recipient setting and you want to configure the list of contacts, see *Managing Contacts on page 4-21*.

For some notifications, you can configure the parameter that triggers the alert notification and the network objects to which the rule applies.

Managing Contacts

You can add or remove the email addresses of contacts. Contacts added to this list are sent email if the default option `Send to all contacts` is selected when configuring alerts and reports.

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Contacts**.
2. Type the email addresses of recipients who will receive notifications and reports.

   Use a semicolon to separate multiple recipients.
3. Remove any recipients who should no longer receive notifications and reports.
4. Click **Save**.

Managing User-Defined Settings

Go to **Policy** > **User Defined Settings** to perform any of the following tasks to manage user-defined settings.

Procedure

- Click on the **Network Objects** tab to configure network objects used when defining policies, HTTPS decryption rules, Security Alert rules, and Authentication Policy.
- Click on the **Domain Objects** tab to configure domain objects used when defining policies and HTTPS decryption rules.

- Click on the **Approved/Blocked Lists** tab to configure which Server IP addresses, domains, URLs, and file (SHA1s) to add to the approved list or the blocked list.
- Click on the **Notifications** tab to customize notifications sent to end-users that are requesting network resources and violations occur.

Managing Network Objects

Go to **Policy** > **User Defined Settings** > **Network Objects** to perform any of the following tasks to manage network objects.

Procedure

- View summary information about existing objects.
- Click **Add** to create a new object.
- Click an objects name to view or modify settings.
- Select a object and then click **Remove** to remove the object.
- Click **Import/Export** to export a copy of the defined objects.

Network Objects

Network objects are used when defining policies, HTTPS decryption rules, Security Alert rules, and Authentication Policy.

- Select the networks on which to apply a policy
- Select the networks on which to perform decryption for HTTPS inspection
- Select the networks to add to a policy's exceptions list.

  Policy actions are not applied to networks in the exceptions list, even if they otherwise would meet the criteria for a configured policy action.
- Select the networks to add to an HTTPS decryption policy's exceptions list.

- Select the networks to use as a parameter in an alert notification rule.

  The following notification rules can use network objects as a parameter:

  - Security: Multiple Advanced Threat Detections in Specified Network Groups
  - Security: Multiple Ransomware Detections in Specified Network Groups
  - Security: Multiple C&C Callback Detections in Specified Network Groups
  - Security: Multiple Coin Miner Detections in Specified Network Groups

Adding/Editing Network Objects

Network objects contain configurable parameters and are used by policies and HTTPS inspections rules.

Procedure

1. Go to **Policy** > **User Defined Settings** > **Network Objects**.
2. Click **Add** or click the item to edit.

   The **Add/Edit Network Object** screen opens.
3. Specify a name that describes the network object.
4. Optionally, enter a description.
5. Specify **IP addresses** as a single entry or comma-delimited list of IP addresses, Class InterDomain Routing (CIDR) networks, or IP address ranges.

   Example:

   - `10.0.0.8/23`
   - `192.168.0.1, 10.0.0.1-10.0.0.4, 10.0.0.8/23`
6. Click **Save**.

Related information

↳ *Network Objects*

Managing Domain Objects

Go to **Policy** > **User Defined Settings** > **Domain Objects** to perform any of the following tasks to manage domain objects.

Procedure

- View summary information about existing objects.
- Click **Add** to create a new object.
- Click an objects name to view or modify settings.
- Select a object and then click **Remove** to remove the object.
- Click **Import/Export** to export a copy of the defined objects.

Domain Objects

Domain objects contain configurable parameters and are used by policies and HTTPS inspections rules. Domain objects are used to:

- Select the domains on which to apply a policy
- Select the domains on which to perform decryption for HTTPS inspection

Adding/Editing Domain Objects

Domain objects are used when creating policies or HTTPS inspection rules.

- You can add multiple domain objects at the same time by using a delimiter between each domain entry.
- Valid delimiters are semicolon (;), comma (,), or linefeed (\r, \n, or \n).

Procedure

1. Go to **Policy** > **User Defined Settings** > **Domain Objects**.
2. Click **Add** or click the item to edit.

   The **Add/Edit Domain Object** screen opens.
3. Specify a name that describes the domain object.
4. Optionally, enter a description.
5. Note that the **Domain type** is **Domain** and is the only available domain type.
6. Specify one or more domains to add (using supported delimiters when specifying multiple domain entries).

   A match is found if the site domain for the traffic matches the input domain name.

RULES	EXAMPLES
• If the input entry does not contain a wild card, Deep Discovery Web Inspector matches the entire domain only.	• `www.test.com` matches the domain site “www.test.com” only.
• The domain input string is case-insensitive.	• `www.test.com` and `WWW.TEST.COM` are equivalent.
• Traffic matches are protocol sensitive if the input record contains the protocol. If the input entry does not contain the protocol, traffic matches include both HTTP and HTTPS traffic.	• `https://www.test.com` matches the domain site “https://www.test.com” but not “http://www.test.com”. • `www.test.com` matches both “https://www.test.com” and “http://www.test.com”.

RULES	EXAMPLES
• Wild cards can be used to do prefix, intermediate, or suffix position matches. The asterisk (*) and question mark (?) are supported wild cards. The "?" only matches one string. The "*" matches any length string.	• `*www.test.com` matches any domain that ends with "www.test.com". • `www.test.com*` matches any domain that starts with "www.test.com". • `www.t*est.com` matches the domain"www.ttest.com" and "www.test.com" • `www.test.c?m` matches "www.test.com".
• An IP address is a valid entry for a domain match.	• `192.168.2.1` matches only that single IP address.

7. Click **Add**.
8. Add additional domain entries as needed.
9. Click **Save**.

Related information

↪ *Domain Objects*

Managing Policies

Go to **Policy** > **Policy** to perform any of the following tasks to manage policies.

Note

The default policy is predefined and is always the last one in the policy list. You cannot select the default policy and cannot perform any action on it (move, duplicate, remove). You can only enable or disable the default policy.

Procedure

- View summary information about existing policies.
- Click **Add** to create a new policy.
- Click a policy's name to view or modify settings, including enabling or disabling the policy.
- Configure iOS/Android device scan bypass.
- For a selected policy, click on the **Drag and Drop** icon (✣) and drag it to the position to which you want to move that policy.

  Note

  You cannot drag a policy to a position below the default policy.

- Select a policy and then click **Move Up**, **Move Down**, or **Move Top** to change the policy order.
- Select a policy and then click **Duplicate** to make a copy of the policy.
- Select a policy and then click **Remove** to remove the policy.

Adding Policies

Policies are composed of policy objects that contain specified parameters.

Procedure

1. Go to **Policy** > **Policy**.
2. Click **Add**.
3. Specify a policy name between 1 and 64 characters.
4. Optionally, specify a description between 1 and 128 characters.
5. Enable or disable the policy.

6. Configure **Traffic source** by selecting one of the following:

   - **Any**

     The policy applies to all networks, Active Directory users/groups, and guest users.

   - **Selected users and groups**

     The policy applies only to specific Active Directory users or groups.

     Under the **All users and groups** section, search for and add the users/groups to include as a traffic source. You can choose users and groups only if Active Directory Services is configured and only from domains that are included in the Active Directory Services configuration.

     Note

     Deep Discovery Web Inspector uses CommonName (CN) to perform user/group searches when selecting users/groups as a traffic source.

   - **Selected network objects**

     The policy applies only to specific network objects.

     Select and then move one or more objects from the available network objects list to the selected network objects list. You can create a new network object to include in the policy by clicking **Add New Network Object**.

     See *Adding/Editing Network Objects on page 4-23*.

   - **Guest users**

     The policy applies only to users that authenticate on the network using a designated guest account.

     Note

     You can configure exceptions if you chose **Selected users and groups** or **Selected network objects** as the traffic source.

     See *How Exception Lists Are Used on page 4-30*.

7. Configure **Domain objects** by selecting one of the following:

   - **Any**

     The policy applies to all domain objects.

   - **Selected domain objects**

     The policy applies only to specific domain objects.

     Move one or more objects from the available domain objects box to the selected domain objects box. You can create a new domain object to include in the policy by clicking on **Add New Domain Object**.

     See *Adding/Editing Domain Objects on page 4-24*.

8. Configure **File types** by selecting one of the following:

   - **Any**

     The policy applies to all defined file types.

   - **Selected file types**

     The policy applies to only specific file types.

     Move one or more file types from the available file types box to the selected file types box. The available file types are predefined and cannot be configured.

9. Select the **Action**.

   - **Allow**

     If the traffic matches the policy, allow the traffic while bypassing scanning.

   - **Block**

     If the traffic matches the policy, block the traffic.

   - **Scan**

     If the traffic matches the policy, scan the traffic and perform the appropriate action configured for each risk level.

10. If you configured **Scan** as the action, perform the following:

    a. Configure which action to take (**Block** or **Monitor**) for each risk level if this policy is matched.

    b. Enable or disable **Patient-Zero**.

       If Patient Zero Protection is enabled, objects that are sent to the Virtual Analyzer sandbox for analysis are temporarily held (neither delivered to the endpoint nor blocked) while waiting for sandbox analysis to complete. Once analysis is complete, depending on the outcome of the analysis, the appropriate action is taken.

11. Click **Save**.

What to do next

Move the policy to the desired location within the policy list.

How Exception Lists Are Used

When you configure policies, you can configure policy scanning exceptions if you have selected either **Selected users and groups** or **Selected network objects** for the traffic source.

Entries in an exception list will not be scanned even if they are a match to other criteria in the policy.

- **Selected users and groups**

  If a user or group is included in both the selected users and groups list and the users and group exceptions list, the presence in the exceptions list has higher priority.

- **Selected network objects**

  If an IP address is included in both the selected network objects list and the network objects exceptions list, the presence in the exceptions list has higher priority.

If the client's IP address is part of a network object in the exception list of a policy, this policy will not be matched. Instead, Deep Discovery Web Inspector will look at the next policy to search for a match to this client's IP address.

Managing HTTPS Decryption Rules

Encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections. To maintain security, Deep Discovery Web Inspector can decrypt and scan selected HTTPS traffic for potential risks and threats. Before Deep Discovery Web Inspector can apply scanning and filtering policies on encrypted content, you must configure HTTPS decryption rules that define what to decrypt.

Go to **Policy** > **Decryption Rules** to perform any of the following tasks to manage HTTPS decryption rules.

Note

The default HTTPS decryption rule is predefined and is always the last one in the list.

Procedure

- View summary information about existing HTTPS decryption rules.
- Click **Add** to create a new rule.
- Click a rule's name to view or modify settings, including enabling or disabling the rule.
- Click a rule's name to import a certificate or reset the rule to use the default certificate.

  On first installation, Deep Discovery Web Inspector creates a self-signed certificate that will be used to resign decrypted HTTPS traffic. In doing so, Deep Discovery Web Inspector also acts as its own CA. Users who wish to adopt their own organizations' CA can import a certificate signed by that CA to Deep Discovery Web Inspector.
- For a selected decryption rule, click on the **Drag and Drop** icon (✣) and drag it to the position to which you want to move that rule.

Note

You cannot drag a rule to a position below the default rule.

- Select a rule and then click **Move Up**, **Move Down**, or **Move Top** to change the rule order and to prioritize rules as needed.
- Select a rule and then click **Duplicate** to copy the selected rule.
- Select one or more rules and then click **Remove** to remove the rules.
- Generate a CSR to request a certificate from the Certificate Authority. You can import this certificate into an HTTPS decryption rule.

HTTPS Decryption Rules

Because encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections, you can configure Deep Discovery Web Inspector to decrypt and scan selected HTTPS traffic for potential risks and threats.

You can deploy HTTPS decryption rules to enable decryption and inspection of specific HTTPS network traffic based on the following criteria:

- Decryption source

  Sources include: **Any**, **Selected users and groups**, **Selected network objects**, and **Guest users**

  Note

  You can add exceptions if you configure **Selected users and groups** or **Selected network objects** as the decryption source.

- Decryption categories
- Decryption domain objects

  To scan HTTPS traffic, Deep Discovery Web Inspector identifies the SSL connection at the first packet of the SSL handshake, acquires the client IP address information from the session, and identifies the URL categories of the target domain.

- If the client IP is included in the selected network objects for **Decryption source** and the target domain is in the configured **Decryption Domain Objects**, then the traffic will match this policy and will be decrypted.
- If certain traffic matches multiple policies, the policy with the highest priority will take effect, and the traffic will be re-signed using the certificate configured in that policy. Deep Discovery Web Inspector will not decrypt the connection if it does not match any network objects (from decryption source field), URL categories, or domain objects specified in the HTTPS decryption rules.
- After the HTTPS traffic to be inspected and the policy to use is identified, Deep Discovery Web Inspector re-signs the website certificate using that policy's CA certificate and decrypts and inspects the traffic and then determines the appropriate actions for traffic based on configured policies.

Viewing HTTPS Decryption Rules

Procedure

1. Go to **Policy** > **Decryption Rules**.
2. View summary information about existing rules including:
   - The name of the rule.
   - The decryption source, decryption domain objects, and decryption categories included in the rule.

     The decryption source can be one of the following: **Any**, **Selected network objects**, **Selected users and groups**, or **Guest users**.
   - Whether the rule is enabled.
   - Information about the subject and issuer of the Certificate Authority (CA) used to re-sign the website certificate.
3. Click on the name of an HTTPS decryption rule to view more details about that rule.

Adding/Editing HTTPS Decryption Rules

HTTPS decryption rules are composed of decryption sources, decryption domain objects, and decryption categories that contain specified parameters. When Deep Discovery Web Inspector determines that network traffic matches an HTTPS decryption rule, the HTTPS traffic is decrypted and inspected and action taken according to the configured policy rules. To further define how HTTPS traffic is handled, you can enable auto tunneling and intelligent decryption. HTTPS decryption rules also provide the means to import and save CA certificates used to re-sign the website certificate.

Procedure

1. Go to **Policy** > **Decryption Rules**.
2. Click **Add** or click the item to edit.
3. Specify a policy name between 1 and 64 characters.
4. Optionally, specify a description between 1 and 128 characters.
5. Enable or disable the rule.
6. Enable or disable auto tunneling.

   When auto tunneling is enabled, Deep Discovery Web Inspector maintains a list of trusted domains or URLs, whose HTTPS traffic will not be subject to HTTPS decryption rules, and will always be accessible by end users without being decrypted and inspected by Deep Discovery Web Inspector.

   See the *Deep Discovery Web Inspector Administrator's Guide* for more information about configuring the auto tunnel list.
7. Enable or disable **Intelligent Decryption**.

   Intelligent Decryption is designed to bypass HTTPS decryption for application-based HTTPS traffic.

Note

If you disable **Intelligent Decryption**, all HTTPS traffic will be decrypted, which can impact some applications and affect business continuity. Trend Micro recommends enabling **Intelligent Decryption** for HTTPS decryption policies.

See the *Deep Discovery Web Inspector Administrator's Guide* for more information about configuring the **Intelligent Decryption** list.

8. Configure **Decryption sources** by selecting one of the following:

- **Any**

  The rule to applies to all networks, users/groups, and guest users.

- **Selected users and groups**

  The rule applies only to specific Active Directory users or groups

  Search for and select the users/groups to include as decryption sources. You can choose users and groups only if Active Directory Services is configured and only from domains that are included in the Active Directory Services configuration.

  Note

  Deep Discovery Web Inspector uses CommonName (CN) to perform user/group searches when selecting users/groups as a decryption source.

- **Selected network objects**

  The rule applies only to specific network objects.

  Move one or more objects from the available network objects list to the selected network objects list. You can create a new network object to include in the HTTPS decryption rule.

  See *Adding/Editing Network Objects on page 4-23*.

- **Guest users**

  The rule applies to users that authenticate on the network using a designated guest account.

Note

You can configure exceptions if you chose **Selected users and groups** or **Selected network objects** as the decryption source. Entries in an exception list will not be decrypted even if they are a match to other criteria in the HTTP decryption rule.

9. Configure **Decryption Categories**:

   a. Click on the **Decryption Categories** box to open the list of URL categories.

   b. Select or deselect URL categories on which to apply the HTTPS decryption rule.

      The available categories are predefined and cannot be configured. The categories are organized in a hierarchical structure with main categories and subcategories. Click the arrow by a main category to view the sub-categories. You can choose entire categories or only sub-categories to add to the list.

10. Configure **Decryption Domain Objects** by moving one or more objects from the available domain objects list to the selected domain objects list.

    You can create a new domain object to include in the HTTPS decryption rule.

    See *Adding/Editing Domain Objects on page 4-24*.

11. If you do not want to use the default Deep Discovery Web Inspector CA, you can use a private CA by doing one of the following under the certificate section:

    a. If the certificate is not based on the CSR generated by Deep Discovery Web Inspector:

       i. Under **Certificate type**, make sure that **Certificate with CSR generated by Deep Discovery Web Inspector** is not selected.

       ii. Under **Import type**, select the appropriate certificate file type:

           Valid options are **PEM/DER**, **PKCS7**, and **PKCS12**.

       iii. In **Certificate**, browse and choose the certificate file.

       iv. In **Private key**, browse and choose the private key file for the certificate file.

v. Enter the password of the private key and then confirm it.

vi. Click on **Verify Certificate** to verify that the certificate is valid.

b. If the certificate is based on the CSR generated by Deep Discovery Web Inspector:

i. Select **Certificate with CSR generated by Deep Discovery Web Inspector**.

ii. Under **Import type**, select the appropriate certificate file type:

Valid options are **PEM/DER**, **PKCS7**, and **PKCS12**.

iii. In **Certificate**, browse and choose the certificate file.

iv. Click on **Verify Certificate** to verify that the certificate is valid.

Note

Deep Discovery Web Inspector uses the certificate to re-sign the website certificate and decrypt the traffic for inspection. You can use your own private CA certificate; however, you cannot use a CA certificate that is signed by a public certificate authority.

You can configure Active Directory Services to use the HTTPS decryption rule certificate when creating authentication policies for authenticating Active Directory users. For more information, see *Integration with Microsoft Active Directory on page 1-5*

12. Click **Save**.

Note

You can also restore the certificate settings to the default Trend Micro Deep Discovery Web Inspector CA, from the certificate section by clicking on **Restore to Default**.

What to do next

If you are using the default Trend Micro Deep Discovery Web Inspector CA, end-users can go to the following link or use the code to download the default CA:

http://files.trendmicro.com/products/network/Deep%20Discovery%20Web%20Inspector/2.0/ddwi-default.cer

Trend Micro provides a tool that Windows users can use to directly install and trust the Deep Discovery Web Inspector default CA. To download the tool go to the following link:

http://files.trendmicro.com/products/network/Deep%20Discovery%20Web%20Inspector/2.0/ddwi_rootca_tool.zip

The file is password protected with the password: `ddwi`.

Generating a CSR

When Deep Discovery Web Inspector determines that network traffic matches an HTTPS decryption rule, the HTTPS traffic is decrypted and inspected and action taken according to the configured policy rules. You can generate a CSR to request a certificate from a Certificate Authority. You can import this certificate into an HTTPS decryption rule. The certificate is used to re-sign the website certificate.

Procedure

1. Go to **Policy** > **Decryption Rules**.
2. Click **Generate CSR** to generate the CSR file.

   The **Generate CSR** window opens.

3. Specify the following parameters:

OPTION	DESCRIPTION
Common Name	The Common Name (CN) is typically composed of Host + Domain Name. It can also be the name of the server.
Country Code	The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.
State/Province	Name of the state or province where your organization is located. Do not abbreviate.
Locality	Name of the city where your organization is registered or located. Do not abbreviate.
Organization	The legally-registered name for your business.
Organizational Unit	The name of the department or organization unit making the request.
(Optional) **Email Address**	Email address of the submitter.

4. Click **Generate CSR**.

   The following message is displayed: "CSR generated successfully, please click to download".

5. Click **Download** to download the CSR to your local computer.

Note

Deep Discovery Web Inspector only archives one CSR and Private Key. If multiple certificates are needed, generate a CSR after the previous certificate has been imported successfully. Otherwise, the previous CSR and Private Key are replaced.

Apex Central

Trend Micro Apex Central is a software management solution that gives you the ability to control antivirus and content security programs from a central location, regardless of

the program's physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

In a network topology containing multiple Deep Discovery Web Inspector appliances, Apex Central can aggregate suspicious objects data.

Deep Discovery Web Inspector supports synchronizing two types of suspicious objects from Apex Central: Virtual Analyzer suspicious objects and user-defined suspicious objects. Deep Discovery Web Inspector can block the traffic if a match is found in the synchronized high-risk suspicious objects list.

On Deep Discovery Web Inspector, use the **Administration** > **Integrated Products/ Services** > **Apex Central** tab to perform the following tasks:

- Register to an Apex Central server.
- Check the connection status between Deep Discovery Web Inspector and Apex Central.
- Unregister from an Apex Central server.
- Synchronize suspicious objects with Apex Central.

For more information about configuring Deep Discovery Web Inspector to use Apex Central, see the *Deep Discovery Web Inspector Administrator's Guide*.

Registering to Apex Central From Deep Discovery Web Inspector Console

Before you can synchronize suspicious objects with Apex Central, you must complete the integration using the Deep Discovery Web Inspector console.

Note

You can register the Deep Discovery Web Inspector appliance to only one of either Apex Central or Deep Discovery Director at any given time. You cannot register the appliance with both products at the same time.

If the appliance is already registered with Deep Discovery Director, you cannot register with Apex Central until you unregister Deep Discovery Director.

Procedure

1. On the Deep Discovery Web Inspector console, go to **Administration** > **Integrated Products/Services** > **Apex Central**.
2. Under the **General** section, view the registration status.
3. Configure **Server Settings**.

OPTION	DESCRIPTION
Server address	Type the Apex Central server FQDN or IP address.
Port	This is a read-only field. Deep Discovery Web Inspector uses port 443 to communicate with Apex Central via the web service.

4. (Optional) Under **Suspicious Object Synchronization**, do the following:
   a. Select **Synchronize suspicious objects from Apex Central**.
   b. Type the API key from Apex Central.

   Note
   Log on to Apex Central and go to the **Help** menu to obtain the API key.
5. Click **Save**.

Deep Discovery Web Inspector connects to Apex Central.

What to do next

After you register to Apex Central from the Deep Discovery Web Inspector console, you must continue to register Deep Discovery Web Inspector from the Apex Central web console.

Use the Apex Central web console to perform the following steps to complete registration of Deep Discovery Web Inspector to Apex Central:

1. Open the Apex Central web console, go to **Administration** > **Managed Servers** > **Server Registration**, select **Add**, and input the necessary information.

Select **Deep Discovery Web Inspector** as the product while registering.

2. Click **Save**.

After registration, Deep Discovery Web Inspector can be found in the Apex Central **Managed Servers** page. Deep Discovery Web Inspector can upload the virtual analyzer suspicious object and suspicious object detection logs to Apex Central.

Deep Discovery Web Inspector synchronizes suspicious object lists from Apex Central every 20 seconds, and displays the time of the last synchronization.

Note

You need to follow the above registration steps. If the registration order is reversed (login Apex Central web console to register to Deep Discovery Web Inspector and then register to Apex Central from the Deep Discovery Web Inspector console), exceptions to Virtual Analyzer Suspicious Objects synchronized from Apex Center will be cleared. Deep Discovery Web Inspector cannot set these exception objects to the internal virtual analyzer's white list until adding a new exception object.

Deep Discovery Director

Trend Micro Deep Discovery Director is an on-premises management solution that enables centralized management of certain Deep Discovery Web Inspector tasks, as well as configuration replication for Deep Discovery Web Inspector appliances.

Additionally, by registering Deep Discovery Web Inspector to Deep Discovery Director, you can enable the bi-directional synchronization of synchronized suspicious objects and suspicious object exceptions.

Deep Discovery Web Inspector supports integration with Deep Discovery Director 5.1 and later versions.

- After registration is successful, the following capabilities are enabled:
  - Upload the appliance's system information to Deep Discovery Director.
  - Upgrade appliance firmware and apply hotfixes and patches using a Deep Discovery Director plan.

- Import Virtual Analyzer images to an appliance using a Deep Discovery Director plan.
- Replicate a selected Deep Discovery Web Inspector appliance's configuration across several appliances using a Deep Discovery Director plan.
- Configure bi-directional synchronization of synchronized suspicious objects and suspicious object exceptions.

For more information, see the **Deep Discovery Director Administrator's Guide**.

Performing Additional Configuration Tasks

You can perform additional configuration steps to meet your business requirements, including the following:

- Configuring Active Directory services that allow you to use Active Directory users and groups when creating policies, HTTPS inspection rules, and accounts, and for authentication when users access web resources.
- Creating the Approved List and Blocked List.
- Managing and customizing the notifications sent to end users when there are violations.
- Managing reports that are sent to configured recipients.
- Configuring additional system settings such as static routes, proxy settings, NTP servers, authentication certificates, and X-Header handling settings.
- Configuring additional integrated products and services such as Deep Discovery Director integration, threat intelligence sharing, and configuring a syslog server.
- Managing settings that determines how long to save log data.
- Backing up certain settings.
- Creating new accounts and contacts.

For information about how to perform additional configuration tasks, see the *Deep Discovery Web Inspector Administrator's Guide*.

Configuring X-Header Handling Settings

You can configure how Deep Discovery Web Inspector manages X-Header settings for the X-Forwarded-For and X-Authenticated-User fields.

Note

X-Header settings are supported for all deployment modes.

Procedure

1. Go to **Administration** > **System Settings** > **X-Header Handling**.
2. Enable or disable **X-Forwarded-For Parsing** .

   If this option is enabled, when Deep Discovery Web Inspector gets the X-Forwarded-For from the user request, Deep Discovery Web Inspector uses the first address of the resolved X-Forwarded-For instead of the IP address of the TCP connection to do authentication, decryption, scanning, and logging.
3. Specify the X-Header handling settings for **X-Forwarded-For** and **X-Authenticated-User**.

OPTION	DESCRIPTION
Keep	Retain the information found in the X-Forwarded-For or X-Authenticated-User fields.
Remove	Remove the specified field.

OPTION	DESCRIPTION
Add	Retain the specified field and additionally: • For X-Forwarded-For, append the proxy IP to the field. • For X-Authenticated-User, append the user info to the field. **Note** The appended user information is added in the following format: [DOMAIN]\[USERNAME]

4. Click **Save**.

Chapter 5

Updating Deep Discovery Web Inspector

Topics include:

- *Hotfixes and Patches Overview on page 5-2*
- *Managing Patches on page 5-2*
- *Upgrading Firmware on page 5-3*

Hotfixes and Patches Overview

After an official product release, Trend Micro releases hotfixes, security patches, and patches to address issues, enhance product performance, or add new features.

TABLE 5-1. Hotfixes and Patches

HOTFIXES AND PATCHES	DESCRIPTION
Hotfix	A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers. **Note** A new hotfix might include previous hotfixes until Trend Micro releases a patch.
Security patch	A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.
Patch	A patch is a group of hotfixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hotfix, patch, and service pack releases:

http://downloadcenter.trendmicro.com

Managing Patches

From time to time, Trend Micro releases a patch for a reported known issue or an upgrade that applies to the product. Find available patches at http://downloadcenter.trendmicro.com.

You can install a patch file on Deep Discovery Web Inspector using one of the following methods:

- The Deep Discovery Web Inspector management console.
- Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

  You can use this method if Deep Discovery Web Inspector is registered to Deep Discovery Director.

Use the following method to install a patch file on Deep Discovery Web Inspector:

Procedure

1. Go to **Administration** > **Product Updates** > **Hotfixes / Patches**.
2. Under **History**, verify the firmware version number.
3. Manage the product patch.
   - Upload a patch by browsing to the patch file provided by Trend Micro Support and then clicking **Install** under **Install Hotfix / Patch**.
   - Roll back a patch by clicking **Roll Back** under **History**.

     After rollback, Deep Discovery Web Inspector uses the most recent previous configuration. For example, rolling back patch 3 returns Deep Discovery Web Inspector to a patch 2 state.

Upgrading Firmware

From time to time, Trend Micro releases a firmware upgrade that applies to the product. Find available firmware upgrades at http://downloadcenter.trendmicro.com.

Updating the firmware ensures that Deep Discovery Web Inspector has access to new and improved security features when they become available.

You can upgrade the firmware on Deep Discovery Web Inspector using one of the following methods:

- The Deep Discovery Web Inspector management console.
- Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

  You can use this method if Deep Discovery Web Inspector is registered to Deep Discovery Director.

Upgrade the firmware on Deep Discovery Web Inspector using the following method:

Note

Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete. Trend Micro recommends starting the upgrade during off-peak office hours. Installing the update restarts Deep Discovery Web Inspector.

Procedure

1. Obtain the firmware image.
   - Download the Deep Discovery Web Inspector firmware package from the Trend Micro Download Center at:

     http://downloadcenter.trendmicro.com
   - Obtain the firmware package from your Trend Micro reseller or support provider.
2. Save the package to any folder on a local computer.
3. Go to **Administration** > **Product Updates** > **Firmware**.
4. Next to **Firmware version**, verify your firmware version.
5. Browse for the firmware update package.
6. Click **Install**.

Tip

You can access the command line interface to view the installation process.

After the installation has completed, Deep Discovery Web Inspector automatically restarts and the web console log on page appears.

7. Perform the following post-installation steps:

   - Clear the browser cache.
   - Manually log on to the web console.
   - If Deep Discovery Web Inspector is using an internal Virtual Analyzer that connects to the Internet through a proxy server, reconfigure the proxy settings for the internal Virtual Analyzer.

Chapter 6

Backing Up or Restoring a Configuration

You can back up or restore certain Deep Discovery Web Inspector configuration settings by exporting or importing those settings using the management console.

Trend Micro recommends exporting your settings to:

- Keep a backup

  If Deep Discovery Web Inspector cannot recover from a critical problem, import your configuration backup after restoring the device to automatically implement the pre-failure configuration.

  Or you can create a backup on a running appliance before making changes to the configuration. Having a backup provides you with the option of quickly and conveniently reverting to the original settings saved in the backup at a later time.

- Replicate settings across several devices

  If you have several devices on your network, you do not need to separately configure most settings. You can replicate a configuration across several Deep Discovery Web Inspector appliances by restoring the configuration file into each appliance.

Important

Deep Discovery Web Inspector only supports restoring configurations from other Deep Discovery Web Inspector appliances running the same version. When restoring different versions, Deep Discovery Web Inspector now only supports restoring the Deep Discovery Web Inspector 2.2 to the Deep Discovery Web Inspector 2.5 version.

When exporting/importing your settings, the database is locked. Therefore, all Deep Discovery Web Inspector actions that depend on database access will not function.

Trend Micro recommends:

- Backing up the current configuration before each import operation.
- Performing the operation when Deep Discovery Web Inspector is idle. Importing and exporting affects Deep Discovery Web Inspector performance.

Settings That Are Backed Up or Restored

You can back up settings from the screens and tabs listed in the following table.

TABLE 6-1. Backed up configuration settings

SCREEN	TAB
Dashboard	Not applicable
Policy > **Policy**	All policies
Policy > **Decryption Rules**	All HTTPS decryption rules (formerly known as HTTPS Inspection rules)
Policy > **Digital Certificates**	All certificates in the trusted, untrusted, and invalid certificate stores and certificate exceptions
Policy > **HTTPS Tunnels**	All domain tunnels
Policy > **Intelligent Decryption**	All custom patterns and exceptions
Policy > **User Defined Settings**	Network objects
	Domain objects
	Approved list and blocked list
	All notification pages
Alerts / Reports > **Alerts**	Rules
Alerts / Reports > **Reports**	Schedules
Administration > **Component Updates**	Enable scheduled update
	Schedule time
Administration > **System Settings**	X-Header Handling

SCREEN	TAB
Administration > **Active Directory Services**	Active Directory
	Authentication Policy
	Configure Global Authentication Settings **Note** The Kerberos keytable information is not backed up.

Backing Up a Configuration

During export, do not:

- Access other management console screens or modify any settings
- Perform any database operations
- Start/stop any services on the device or in the group to which the device belongs
- Launch other export or import tasks

Note

For information on the settings that are backed up, see *Settings That Are Backed Up or Restored on page 6-3*.

Procedure

1. Go to **Administration** > **System Maintenance** > **Configure BackUp / Restore**.
2. Next to **Back Up Configuration Settings**, click **Export**.

   A confirmation dialog box appears.

3. Click **OK** to continue with the export.

Note

If you click **Cancel**, the export is canceled.

A **File Download** window appears.

4. Click **OK** to save the configuration file to local storage.

Restoring a Configuration

Restoring Deep Discovery Web Inspector settings replaces the original settings and rules, such as policy settings, with the imported configuration.

During the restore, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Launch other export or import tasks.

Note

For information on the settings that you can restore, see *Settings That Are Backed Up or Restored on page 6-3*.

Procedure

1. Go to **Administration** > **System Maintenance** > **Configure BackUp / Restore**.
2. Next to **Restore Configuration Settings**, click **Select File** and locate the backup file to use for the restore.

If you have selected a file and want to remove the file and select another file, do the following:

a. Move your mouse over the file name to find the dismiss icon.

b. Click the icon.
The file is deleted.

c. You can choose another file to use for restore.

3. Click **Import**.

A message displays saying the import was successful.

4. Click **Restore**.

A confirmation dialog box appears.

5. Click **OK** to continue with the restore.

Note

If you click **Cancel**, the restore is canceled.

After clicking **OK**, the **Restarting DDWI Service** page appears.

If the restore is successful, after a few minutes, the page displays information about the successful restore. The management console page then opens.

If the restore fails, after a few minutes, the page displays information about the failed restore. The management console page then opens.

Chapter 7

Reinstalling Deep Discovery Web Inspector

Topics include:

- *Before Reinstalling on page 7-2*
- *Performing a Fresh Install of Deep Discovery Web Inspector on page 7-2*

Before Reinstalling

The following procedure provides a list of task to consider performing before reinstalling Deep Discovery Web Inspector.

Procedure

1. Review the recommended network information.

   See *Recommended Network Environment on page 2-27*.

2. Review the information about ports used by the appliance.

   See *Ports Used by the Appliance on page 2-29*.

3. Prepare the items for the installation.

   See *Items to Prepare on page 2-32*.

4. Review the system requirements.

   See *System Requirements on page 2-27*.

Performing a Fresh Install of Deep Discovery Web Inspector

Important

The Deep Discovery Web Inspector appliance comes with the appliance software installed. The following procedure provides a reference for fresh installs only.

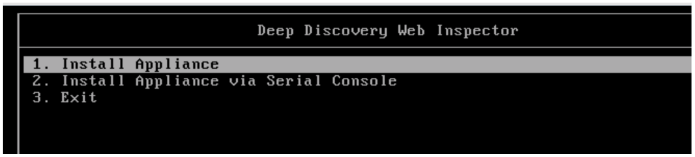
Trend Micro provides the Deep Discovery Web Inspector appliance hardware. No other hardware is supported.

WARNING!

The installation deletes any existing data or partitions on the selected disk. Back up existing data before installing Deep Discovery Web Inspector.

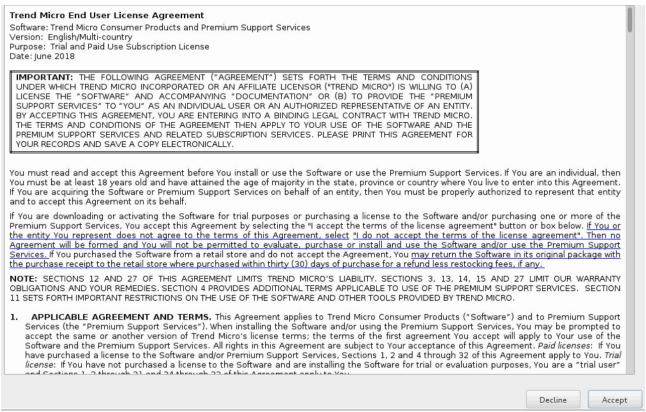
Procedure

1. Connect a keyboard and monitor to the server.
2. Power on the server.
3. Insert the Deep Discovery Web Inspector Installation DVD into the optical disc drive.
4. Restart the server.
5. The server boots from the Deep Discovery Web Inspector Installation DVD and the installation begins. Select **Install Appliance**.



After the setup initializes, the **License Agreement** screen appears.

6. Click **Accept**.



7. Select the device to install Deep Discovery Web Inspector.

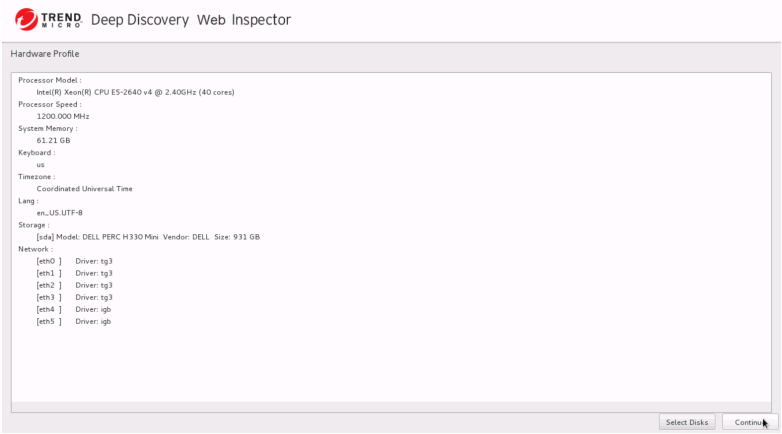
8. Click **Continue**.

9. At the warning message, click **Yes** to continue.

   The Deep Discovery Web Inspector installer scans the hardware to determine that it meets the minimum specifications.

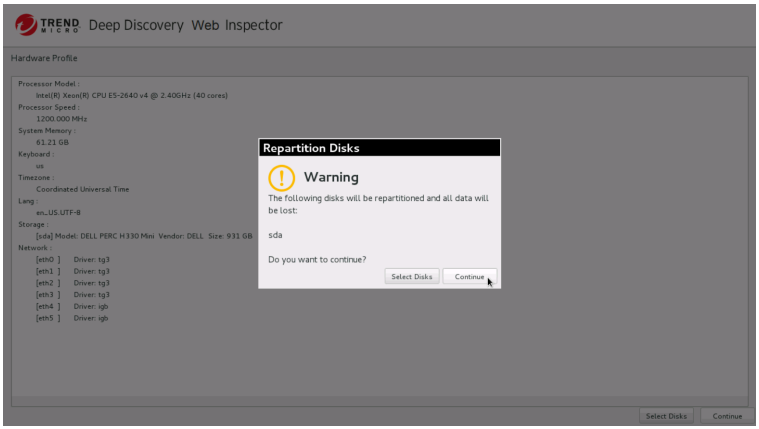
10. Click **Next**.

    The **Summary** screen appears.



11. Click **Continue** to begin the installation.

12. At the warning message, click **Continue**.



After formatting the disk, the program installs the operating system. The Deep Discovery Web Inspector appliance installs after the appliance restarts.

13. Remove the Installation DVD from the optical disc drive to prevent reinstallation.

14. Installation begins.

After installation completes, the appliance will restart and enter CLI mode.

Chapter 8

Using the Command Line Interface

You can use the Command Line Interface (CLI) to perform tasks, including the following tasks:

- Configure initial settings, such as the device IP address and host name
- Start, stop, and restart services
- View device status and statistics
- Debug and troubleshoot the device

Related information

↳ *Entering the CLI*
↳ *Normal and Privileged Commands*
↳ *Entering Privileged Mode*
↳ *CLI Command Reference*

Entering the CLI

To log on to the CLI, either connect directly to the Deep Discovery Web Inspector appliance or connect using SSH.

Procedure

- To make a direct connection, connect a monitor and keyboard to the Deep Discovery Web Inspector appliance.

  The appliance's command line interface is displayed on the monitor. You can log in to the CLI and perform basic tasks.

- If the SSH service is enabled, do the following to connect using SSH:

  a. Verify the computer you are using can ping Deep Discovery Web Inspector's IP address.

  b. Use an SSH client to connect to Deep Discovery Web Inspector's IP address and TCP port 22.

  Note

  The default IP address / subnet mask is `192.168.252.1` / `255.255.0.0`.

- Log in to the CLI with the default credentials.

  - User name: `admin`
  - Password: `ddwi`

  Note

  Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

Normal and Privileged Commands

The Deep Discovery Web Inspector CLI commands are separated into two categories: normal and privileged commands. Normal commands are basic commands to obtain system information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by the **`enable`** command and password.

Entering Privileged Mode

WARNING!

Enter the shell environment only if your support provider instructs you to perform debugging operations.

Procedure

1. Log on to the CLI.

   See *Entering the CLI on page 8-2*.

2. At the prompt, type `enable` and press ENTER to enter privileged mode.

3. Type the default password, `trend#1`, and then press ENTER.

   The prompt changes from > to #.

CLI Command Reference

The following tables explain the CLI commands.

Note

Some CLI commands require privileged mode. For details, see *Entering Privileged Mode on page 8-3*.

configure deploy reset

TABLE 8-1. configure deploy reset

Reboots the system and changes deploy mode back to the default mode while other settings remain the same on the Deep Discovery Web Inspector appliance.	
Syntax: `configure deploy reset`	
View	Privileged
Parameters	None
Examples:	

Reboots the system and changes deploy mode back to the default mode while other settings remain the same:
`configure deploy reset`
`configure deploy reset`
`Reset the deploy mode.`	

configure module

TABLE 8-2. configure module

Command family configures module settings for the Deep Discovery Web Inspector appliance.	
Syntax: `configure module`	
View	Privileged

configure module non-http(s) block

TABLE 8-3. configure module non-http(s) block

Configures the IP addresses of non-http(s) module block clients and servers on the Deep Discovery Web Inspector appliance.	
Syntax: `configure module non-http(s) block`	
View	Privileged
Parameters	None
Examples:	

To configure the IP addresses of non-http(s) module block clients and servers on the Deep Discovery Web Inspector appliance:
`configure module non-http(s) block`
`Input Client IPs and Server IPs. Enter multiple IPs separated by commas.`
`***Configure Module Non-http(s) Block***`
`Please input the ClientIPs , such as 192.168.137.1,10.64.55.0/24`
`ClientIP:`
 	
`Please input the Server IPs, such as 192.168.137.1,10.64.55.0/24`
`Server IP:`	

configure module non-http(s) block delete

TABLE 8-4. configure module non-http(s) block delete

Clears the non-http(s) module block configuration on the Deep Discovery Web Inspector appliance.

Syntax: `configure module non-http(s) block delete`	
View	Privileged
Parameters	None
Examples:	

Clears the non-http(s) module block configuration on the Deep Discovery Web Inspector appliance:
`configure module non-http(s) block delete`
`#configure module non-http(s) block delete`
`Clear configure for non-http(s) block success`	

configure module webscanner pmtu_discover disable

TABLE 8-5. configure module webscanner pmtu_discover disable

Disables the webscanner pmtu_discover module on the Deep Discovery Web Inspector appliance.	
Syntax: `configure module webscanner pmtu_discover disable`	
View	Privileged
Parameters	None
Examples:	

Disables the webscanner pmtu_discover module on the Deep Discovery Web Inspector appliance:

```
configure module webscanner pmtu_discover disable
```

```
Please wait while the InterScan Web Security Suite daemon is being
checked...ok

Shutting down the InterScan HTTP daemon...
stop ...
prepare dtas in /var/iwss/log
prepare dtas/usandbox_report in /var/iwss/log
prepare dtas/usandbox_summary in /var/iwss/log
prepare iwssd_cache in /var/iwss/log
prepare dump_files in /var/iwss/log
prepare syslog in /var/iwss/log
prepare tmfbe in /var/iwss/log
No need to update /var/iwss/intscan.ini
Starting the InterScan HTTP daemon...
Please wait while the InterScan Web Security Suite daemon is being
checked.............ok
```

configure module webscanner pmtu_discover enable

TABLE 8-6. configure module webscanner pmtu_discover enable

Enables the webscanner pmtu_discover module on the Deep Discovery Web Inspector appliance.	
Syntax: `configure module webscanner pmtu_discover enable`	
View	Privileged
Parameters	None
Examples:	

Enables the webscanner pmtu_discover module on the Deep Discovery Web Inspector appliance:

```
configure module webscanner pmtu_discover enable
```

```
Please wait while the InterScan Web Security Suite daemon is being
checked...ok

Shutting down the InterScan HTTP daemon...
stop ...
prepare dtas in /var/iwss/log
prepare dtas/usandbox_report in /var/iwss/log
prepare dtas/usandbox_summary in /var/iwss/log
prepare iwssd_cache in /var/iwss/log
prepare dump_files in /var/iwss/log
prepare syslog in /var/iwss/log
prepare tmfbe in /var/iwss/log
No need to update /var/iwss/intscan.ini
Starting the InterScan HTTP daemon...
Please wait while the InterScan Web Security Suite daemon is being
checked.............ok
```

configure network

TABLE 8-7. configure network

Command family configures network settings for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network`	
View	Privileged

configure network basic

TABLE 8-8. configure network basic

Configures basic network settings, including host name, IP address, subnet mask, gateway, and DNS.

Syntax: `configure network basic`	
View	Privileged
Parameters	None
Examples:	

`***Network Configuration***`
`Specify value for each item and press ENTER. Settings apply to the management port (eth0) and require a restart.`
`Host name: ddwi2.example.com`
`IPv4 address: 10.64.70.151`
`Subnet mask: 255.255.254.0`
`IPv4 gateway: 10.64.70.1`
`Preferred IPv4 DNS: 10.64.1.55`
`Alternate IPv4 DNS: 10.64.1.54`
`Confirm changes and restart (Y/N):`	

configure network bypass

TABLE 8-9. configure network bypass

Sets the bypass mode for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network bypass`	
View	Privileged
Parameters	**<mode>**: Sets the bypass mode: `on` | `auto`
Examples:	

To set the network bypass mode for the Deep Discovery Web Inspector appliance to “on”

```
configure network bypass on
```

configure network dns ipv4

TABLE 8-10. configure network dns ipv4

Configures IPv4 DNS settings for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network dns ipv4 <dns1> [dns2]`	
View	Privileged
Parameters	**<dns1>**: Primary DNS server **[dns2]**: Optional secondary DNS server **Note** Use a space to separate the primary and optional secondary DNS value.
Examples:	
To configure the primary DNS with an IP address of 192.168.10.21: `configure network dns ipv4 192.168.10.21`	
To configure the primary and optional secondary DNS with the following values: • Primary DNS: `192.168.10.21` • Secondary DNS: `192.168.10.22` `configure network dns ipv4 192.168.10.21 192.168.10.22`	

configure network hostname

TABLE 8-11. configure network hostname

Configures the host name for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network hostname <hostname>`	
View	Privileged
Parameters	**<hostname>**: Host name or fully qualified domain name (FQDN) for the Deep Discovery Web Inspector appliance
Examples:	
To change the host name of the Deep Discovery Web Inspector appliance to test.example.com: `configure network hostname test.example.com`	

configure network interface ipv4

TABLE 8-12. configure network interface ipv4

Configures the IPv4 static IP address and network mask for a network interface.	
Syntax: `configure network interface ipv4 <interface> <ip> <mask>`	
View	Privileged
Parameters	**<interface>**: Network interface name **<ip>**: IP address for the interface **<mask>**: Network mask for the interface
Example:	

To configure a network interface with the following values:

- Interface: `eth0`
- IPv4 address: `192.168.10.10`
- IPv4 network mask: `255.255.255.0`

```
configure network interface ipv4 eth0 192.168.10.10 255.255.255.0
```

configure network interface mtu

TABLE 8-13. configure network interface mtu

Configures the MTU size for a network interface.	
Syntax: `configure network interface mtu <interface> <mtu>`	
View	Privileged
Parameters	**<interface>**: Network interface name **<mtu>**: Network interface MTU size
Example:	
To configure a network interface MTU with the following values: • Interface: `eth0` • MTU size: 1580 `configure network interface mtu eth0 1580`	

configure network redirect

TABLE 8-14. configure network redirect

Command family configures policies to use when redirecting traffic for the Deep Discovery Web Inspector appliance.

Syntax: `configure network redirect`	
View	Privileged

configure network redirect bypass ip

TABLE 8-15. configure network redirect bypass ip

Command family configures a redirect bypass policy for the Deep Discovery Web Inspector appliance by specifying an IP address or IP network range.	
Syntax: `configure network redirect bypass ip`	
View	Privileged

configure network redirect bypass ip source add

TABLE 8-16. configure network redirect bypass ip source add

Adds a redirect bypass policy by specifying a source IP address or network ID.	
Syntax: `configure network redirect bypass ip source add <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Source IP address or network ID **<mask>**: Network mask
Example:	

To add a new redirect bypass policy entry using a source IP address:

```
configure network redirect bypass ip source add 10.10.10.150
255.255.255.255
```

To add a new redirect bypass policy entry using a source network ID:

```
configure network redirect bypass ip source add 10.10.10.0
255.255.255.128
```

configure network redirect bypass ip source del

TABLE 8-17. configure network redirect bypass ip source del

Deletes a redirect bypass policy by specifying a source IP address or network ID.	
Syntax: `configure network redirect bypass ip source del <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Source IP address or network ID **<mask>**: Network mask
Example:	

To delete a redirect bypass policy entry using a source IP address:
`configure network redirect bypass ip source del 192.168.1.1 255.255.255.255`
To delete a redirect bypass policy entry using a source network ID:
`configure network redirect bypass ip source del 192.168.1.0 255.255.255.128`	

configure network redirect bypass ip destination add

TABLE 8-18. configure network redirect bypass ip destination add

Adds a redirect bypass policy by specifying a destination IP address or network ID.

Syntax: `configure network redirect bypass ip destination add <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Destination IP address or network ID **<mask>**: Network mask
Example:	

To add a new redirect bypass policy entry using a destination IP address:
`configure network redirect bypass ip destination add 10.10.20.150 255.255.255.255`
To add a new redirect bypass policy entry using a destination network ID:
`configure network redirect bypass ip destination add 10.10.20.0 255.255.255.128`	

configure network redirect bypass ip destination del

TABLE 8-19. configure network redirect bypass ip destination del

Deletes a redirect bypass policy by specifying a destination IP address or network ID.	
Syntax: `configure network redirect bypass ip destination del <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Destination IP address or network ID **<mask>**: Network mask
Example:	

To delete a redirect bypass policy entry using a destination IP address:

```
configure network redirect bypass ip destination del 192.168.2.1
255.255.255.255
```

To delete a redirect bypass policy entry using a destination network ID:

```
configure network redirect bypass ip destination del 192.168.2.0
255.255.255.128
```

configure network redirect scan ip

TABLE 8-20. configure network redirect scan ip

Command family configures a redirect scan policy for the Deep Discovery Web Inspector appliance by specifying an IP address or IP network range.	
Syntax: `configure network redirect scan ip`	
View	Privileged

configure network redirect scan ip source add

TABLE 8-21. configure network redirect scan ip source add

Adds a redirect scan policy by specifying a source IP address or network ID.	
Syntax: `configure network redirect scan ip source add <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Source IP address or network ID **<mask>**: Network mask
Example:	

To add a new redirect scan policy entry using a source IP address:

```
configure network redirect scan ip source add 10.10.10.150
255.255.255.255
```

To add a new redirect scan policy entry using a source network ID:

```
configure network redirect scan ip source add 10.10.10.0 255.255.255.128
```

configure network redirect scan ip source del

TABLE 8-22. configure network redirect scan ip source del

Deletes a redirect scan policy by specifying a source IP address or network ID.	
Syntax: `configure network redirect scan ip source del <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Source IP address or network ID **<mask>**: Network mask
Example:	

To delete a redirect scan policy entry using a source IP address:
`configure network redirect scan ip source del 192.168.1.1 255.255.255.255`
To delete a redirect scan policy entry using a source network ID:
`configure network redirect scan ip source del 192.168.1.0 255.255.255.128`	

configure network redirect scan ip destination add

TABLE 8-23. configure network redirect scan ip destination add

Adds a redirect scan policy by specifying a destination IP address or network ID.
Syntax: `configure network redirect scan ip destination add <ip> <mask>`

View	Privileged
Parameters	**<ip>**: Destination IP address or network ID **<mask>**: Network mask
Example:	

To add a new redirect scan policy entry using a destination IP address:
`configure network redirect scan ip destination add 10.10.20.150 255.255.255.255`
To add a new redirect scan policy entry using a destination network ID:
`configure network redirect scan ip destination add 10.10.20.0 255.255.255.128`	

configure network redirect scan ip destination del

TABLE 8-24. configure network redirect scan ip destination del

Deletes a redirect scan policy by specifying a destination IP address or network ID.	
Syntax: `configure network redirect scan ip destination del <ip> <mask>`	
View	Privileged
Parameters	**<ip>**: Destination IP address or network ID **<mask>**: Network mask
Example:	

To delete a redirect scan policy entry using a destination IP address:
`configure network redirect scan ip destination del 192.168.2.1 255.255.255.255`
To delete a redirect scan policy entry using a destination network ID:
`configure network redirect scan ip destination del 192.168.2.0 255.255.255.128`	

configure network redirect scan mac

TABLE 8-25. configure network redirect scan mac

Command family configures a redirect scan policy for the Deep Discovery Web Inspector appliance by specifying a MAC address.	
Syntax: `configure network redirect scan mac`	
View	Privileged

configure network redirect scan mac source add

TABLE 8-26. configure network redirect scan mac source add

Adds a redirect scan policy by specifying a source MAC address.	
Syntax: `configure network redirect scan mac source add <mac_addr>`	
View	Privileged
Parameters	**<mac_addr>**: Source MAC address
Example:	
To add a new redirect scan policy entry using a source MAC address: `configure network redirect scan mac source add 02:00:00:00:00:00`	

configure network redirect scan mac source del

TABLE 8-27. configure network redirect scan mac source del

Deletes a redirect scan policy by specifying a source MAC address.	
Syntax: `configure network redirect scan mac source del <mac_addr>`	
View	Privileged
Parameters	**<mac_addr>**: Source MAC address

Example:
To delete a redirect scan policy entry using a source MAC address: `configure network redirect scan mac source del 02:00:00:00:00:00`

configure network redirect scan mac destination add

TABLE 8-28. configure network redirect scan mac destination add

Adds a redirect scan policy by specifying a destination MAC address.	
Syntax: `configure network redirect scan mac destination add <mac_addr>`	
View	Privileged
Parameters	**<mac_addr>**: Destination MAC address
Example:	
To add a new redirect scan policy entry using a destination MAC address: `configure network redirect scan mac destination add 06:00:00:00:00:00`	

configure network redirect scan mac destination del

TABLE 8-29. configure network redirect scan mac destination del

Deletes a redirect scan policy by specifying a destination MAC address.	
Syntax: `configure network redirect scan mac destination del <mac_addr>`	
View	Privileged
Parameters	**<mac_addr>**: Destination MAC address
Example:	
To delete a redirect scan policy entry using a destination MAC address: `configure network redirect scan mac destination del 06:00:00:00:00:00`	

configure network redirect check-fdb

TABLE 8-30. configure network redirect check-fdb

Command family configures whether to check the MAC forwarding table when redirecting traffic for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network redirect check-fdb`	
View	Privileged

configure network redirect check-fdb enable

TABLE 8-31. configure network redirect check-fdb enable

Enables checking the MAC forwarding table when redirecting traffic.	
Syntax: `configure network redirect check-fdb enable`	
View	Privileged
Parameters	None
Example:	
To enable checking the MAC forwarding table when redirecting traffic: `configure network redirect check-fdb enable`	

configure network redirect check-fdb disable

TABLE 8-32. configure network redirect check-fdb disable

Disables checking the MAC forwarding table when redirecting traffic.	
Syntax: `configure network redirect check-fdb disable`	
View	Privileged
Parameters	None

Example:
To disable checking the MAC forwarding table when redirecting traffic: `configure network redirect check-fdb disable`

configure network route

TABLE 8-33. configure network route

Command family configures IP routes for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network route`	
View	Privileged

configure network route add ipv4

TABLE 8-34. configure network route add ipv4

Adds a new IPv4 route entry.	
Syntax: `configure network route add ipv4 <ip_prefixlen> <via> <dev>`	
View	Privileged
Parameters	**<ip_prefixlen>**: Destination network ID with format IP Address/Prefixlen **<via>**: IPv4 address of the next hop router **<dev>**: Name of the interface to use for the route
Example:	
To add a new IPv4 route entry: `configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route default ipv4

TABLE 8-35. configure network route default ipv4

Configures the IPv4 default gateway for the Deep Discovery Web Inspector appliance.	
Syntax: `configure network route default ipv4 <gateway> <device>`	
View	Privileged
Parameter	**<gateway>**: IPv4 address of default gateway **<device>**: Name of the interface to use to reach the IPv4 default gateway
Example:	
Configures the default route for the Deep Discovery Web Inspector appliance: `configure network route default ipv4 192.168.10.1 eth0`	

configure network route del ipv4

TABLE 8-36. configure network route del ipv4

Deletes an IPv4 route entry.	
Syntax: `configure network route del ipv4 <ip_prefixlen> <via> <dev>`	
View	Privileged
Parameters	**<ip_prefixlen>**: Destination network ID with format IP Address/ Prefixlen **<via>**: IPv4 address of the next hop router **<dev>**: Name of the interface used by the route
Example:	
To delete an IPv4 route for the Deep Discovery Web Inspector appliance: `configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure service

TABLE 8-37. configure service

Command family configures system services for the Deep Discovery Web Inspector appliance.	
Syntax: `configure service`	
View	Privileged

configure service ssh disable

TABLE 8-38. configure service ssh disable

Disables the SSH service.	
Syntax: `configure service ssh disable`	
View	Privileged
Parameters	None
Examples:	
To disable the SSH service: `configure service ssh disable`	

configure service ssh enable

TABLE 8-39. configure service ssh enable

Enables the SSH service.
Syntax: `configure service ssh enable`

View	Privileged
Parameters	None
Examples:	
To enable the SSH service: `configure service ssh enable`	

configure service ssh port

TABLE 8-40. configure service ssh port

Configures the TCP port to use for the SSH service.	
Syntax: `configure service ssh port <port>`	
View	Privileged
Parameters	**<port>**: TCP port to use for the SSH service
Example: To change the SSH service port to 56743: `configure service ssh port 56743`	

configure service ntp enable

TABLE 8-41. configure service ntp enable

Enables the NTP service on the Deep Discovery Web Inspector appliance.	
Syntax: `configure service ntp enable`	
View	Privileged
Parameters	None

Examples:
To enable the NTP service on the Deep Discovery Web Inspector appliance: `configure service ntp enable`

configure service ntp disable

TABLE 8-42. configure service ntp disable

Disables the NTP service on the Deep Discovery Web Inspector appliance.	
Syntax: `configure service ntp disable`	
View	Privileged
Parameters	None
Examples:	
To disable the NTP service on the Deep Discovery Web Inspector appliance: `configure service ntp disable`	

configure service ntp server-address

TABLE 8-43. configure service ntp server-address

Configures the NTP server address.	
Syntax: `configure service ntp server-address <address>`	
View	Privileged
Parameters	**<address>**: IP address or FQDN of the NTP server
Examples:	

To configure the NTP server address as 192.168.10.21: `configure service ntp server-address 192.168.10.21`

configure system

TABLE 8-44. configure system

Command family configures basic system settings for the Deep Discovery Web Inspector appliance.	
Syntax: `configure system`	
View	Privileged

configure system date

TABLE 8-45. configure system date

Configures the date and time and saves the data to CMOS.	
Syntax: `configure system date <date> <time>`	
View	Privileged
Parameters	**<date>**: Set the date using the following format: **yyyy-mm-dd** **<time>**: Set the time with the following format: **hh:mm:ss**
Example:	
To set the date to August 12, 2017 and the time to 3:40 PM: `configure system date 2017-08-12 15:40:00`	

configure system license

TABLE 8-46. configure system license

Set license activation code for fresh installs on Deep Discovery Web Inspector appliances or renew activation code on appliances with activated licenses.	
Syntax: `configure system license`	
View	Privileged
Parameters	None
Examples:	

Example: Activate license during fresh install

```
configure system license

Trend Micro End User License Agreement
Software : Trend Micro Consumer Products and Premium Support Services
Version: <version>
Purpose: <license type>
Date: <date>

<license agreement  - output truncated>

I have read and accept the terms of the Trend Micro License Agreement: [Y/N]Y
Activation Code:xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
Set activation code successfully.
```

Example: Renew license after license is already activated

```
configure system license

Existing Activation Code:xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
New Activation Code     :

Existing Activation Code:xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
New Activation Code     :yy-yyyy-yyyyy-yyyyy-yyyyy-yyyyy-yyyyy
Set activation code successfully.
```

configure system password enable

TABLE 8-47. configure system password enable

Changing the password can only be performed in Privileged mode.	
Syntax: `configure system password enable`	
View	Privileged
Parameters	None
Examples:	
To change the password by entering Privileged mode: `configure system password enable`	

enable

TABLE 8-48. enable

Enters privileged mode where privileged commands are run.	
Syntax: `enable`	
View	Normal
Parameters	None
Example:	
To enter privileged mode: `enable`	

exit

TABLE 8-49. exit

Exits privileged mode. Exits the session for those not in privileged mode.	
Syntax: `exit`	
View	Normal when exiting a session Privileged when exiting privileged mode
Parameters	None
Example:	
To exit privileged mode or to exit the session when not in privileged mode: `exit`	

help

TABLE 8-50. help

Displays an overview of the Command Line Interface (CLI) help information.	
Syntax: `help`	
View	Normal
Parameters	None
Example:	
To display the Command Line Interface (CLI) help information: `help`	

history

TABLE 8-51. history

Displays the current session's command line history.	
Syntax: `history [limit]`	
View	Normal
Parameters	**[limit]**: Sets the size of the history list for the current session Specifying "0" retains all commands for the session.
Example:	
To specify six commands for the size of the history list: `history 6`	

logout

TABLE 8-52. logout

Logs out of the current Command Line Interface (CLI) session.	
Syntax: `logout`	
View	Normal
Parameters	None
Example:	
To logout from the current session: `logout`	

ping

TABLE 8-53. ping

Pings a specified host.	
Syntax: `ping [num_echos] [interval] <dest>`	
View	Normal
Parameters	**[num_echos]**: Specifies the number of echo requests to send; default is 5 **[interval]**: Specifies the delay interval in seconds between each packet; the default is 1 second **<dest>**: Specifies the destination host name or IP address
Examples:	
To ping the IP address 192.168.1.1: `ping 192.168.1.1`	
To ping the host remote.host.com: `ping remote.host.com`	

reboot

TABLE 8-54. reboot

Reboots the Deep Discovery Web Inspector appliance immediately or after a specified delay.	
Syntax: `reboot [time]`	
View	Privileged
Parameters	**[time]**: Optional delay in minutes before rebooting the Deep Discovery Web Inspector appliance

Examples:
To reboot the Deep Discovery Web Inspector appliance immediately: `reboot`
To reboot the Deep Discovery Web Inspector appliance after 5 minutes: `reboot 5`

resolve

TABLE 8-55. resolve

Resolves an IPv4 address on the network.	
Syntax: `resolve <dest>`	
View	Privileged
Parameter	**<dest>**: Remote IP address to resolve
Examples:	
To resolve the host name from IP address 192.168.10.1: `resolve 192.168.10.1`	

restart service

TABLE 8-56. restart service

Command family restarts system services for the Deep Discovery Web Inspector appliance.	
Syntax: `restart service`	
View	Privileged

restart service product

TABLE 8-57. restart service product

Restarts the product service.	
Syntax: `restart service product`	
View	Privileged
Parameters	None
Example:	
To restart the product service: `restart service product`	

restart service ssh

TABLE 8-58. restart service ssh

Restarts the SSH service.	
Syntax: `restart service ssh`	
View	Privileged
Parameters	None
Example:	
To restart the SSH service: `restart ssh service`	

show kernel

TABLE 8-59. show kernel

Command family displays information about the currently running OS kernel for the Deep Discovery Web Inspector appliance.	
Syntax: `show kernel`	
View	Normal

show kernel iostat

TABLE 8-60. show kernel iostat

Displays CPU statistics and I/O statistics for devices and partitions for the Deep Discovery Web Inspector appliance.	
Syntax: `show kernel iostat`	
View	Normal
Parameters	None
Examples:	
To display CPU statistics and I/O statistics for the devices and partitions: `show kernel iostat`	

show kernel messages

TABLE 8-61. show kernel messages

Displays OS kernel messages for the Deep Discovery Web Inspector appliance.
Syntax: `show kernel messages`

View	Normal
Parameters	None
Examples:	
To display the OS kernel messages: `show kernel messages`	

show kernel modules

TABLE 8-62. show kernel modules

Displays the loaded OS kernel modules for the Deep Discovery Web Inspector appliance.	
Syntax: `show kernel modules`	
View	Normal
Parameters	None
Examples:	
To display the loaded OS kernel modules: `show kernel modules`	

show kernel parameters

TABLE 8-63. show kernel parameters

Displays the OS kernel parameters for the Deep Discovery Web Inspector appliance.	
Syntax: `show kernel parameters`	
View	Normal
Parameters	None

Examples:
To display the OS kernel parameters: `show kernel parameters`

show memory

TABLE 8-64. show memory

Command family displays the memory statistics for the Deep Discovery Web Inspector appliance.	
Syntax: `show memory`	
View	Normal

show memory statistic

TABLE 8-65. show memory statistic

Displays system memory statistics for the Deep Discovery Web Inspector.	
Syntax: `show memory statistic`	
View	Normal
Parameters	None
Examples:	
To display the system memory statistics: `show memory statistic`	

show memory vm

TABLE 8-66. show memory vm

Displays virtual memory statistics for the Deep Discovery Web Inspector.	
Syntax: `show memory vm`	
View	Normal
Parameters	None
Examples:	
To display the virtual memory statistics: `show memory vm`	

show module

TABLE 8-67. show module

Command family shows information about modules for the Deep Discovery Web Inspector appliance.	
Syntax: `show module [module name]`	
View	Normal

show module non-http(s) block

TABLE 8-68. show module non-http(s) block

Displays information about the IP addresses for non-http(s) module block clients and servers for the Deep Discovery Web Inspector appliance.
Syntax: `show module non-http(s) block`

View	Normal
Parameters	None
Example:	

To display information about the IP addresses for non-http(s) module block clients and servers for the Deep Discovery Web Inspector appliance:
`show module non-http(s) block`
`***Configure Module Non-http(s) Block***`
`Non-http(s) Block ClientIP: 127.0.0.1,10.64.0.0/24`
`Non-http(s) Block ServerIP: 192.168.137.1,10.64.55.0/24`	

show module webscanner

TABLE 8-69. show module webscanner

Displays information about the status of the webscanner pmtu_discover module for the Deep Discovery Web Inspector appliance.	
Syntax: `show module webscanner`	
View	Normal
Parameters	None
Example:	

To display information about the status of the webscanner pmtu_discover module for the Deep Discovery Web Inspector appliance:
Example with module enabled:
`show module webscanner`
`PMTU Discover: enabled`
Example with module disabled:
`show module webscanner`
`PMTU Discover: disabled`

show network

TABLE 8-70. show network

Command family displays various Deep Discovery Web Inspector network information.	
Syntax: `show network`	
View	Normal

show network arp

TABLE 8-71. show network arp

Displays the value returned from the Address Resolution Protocol (ARP) table for the given IP address.	
Syntax: `show network arp <dest>`	
View	Normal
Parameters	**<dest>**: IP address or FQDN
Examples:	

To display the ARP information for the address 10.2.23.41: `show network arp 10.2.23.41`

show network bypass

TABLE 8-72. show network bypass

Displays the current bypass mode for the Deep Discovery Web Inspector appliance.	
Syntax: `show network bypass`	
View	Normal
Parameters	None
Examples:	
To display the bypass mode for the Deep Discovery Web Inspector appliance: `show network bypass`	

show network connections

TABLE 8-73. show network connections

Displays the current network connections for the Deep Discovery Web Inspector appliance.	
Syntax: `show network connections`	
View	Normal
Parameters	None
Examples:	

To display the current network connections of the Deep Discovery Web Inspector appliance: `show network connections`

show network dns

TABLE 8-74. show network dns

Displays the DNS IPv4 configuration for the Deep Discovery Web Inspector appliance.	
Syntax: `show network dns`	
View	Normal
Parameters	None
Examples:	
To display the IPv4 DNS configuration: `show network dns`	

show network hostname

TABLE 8-75. show network hostname

Displays the host name of the Deep Discovery Web Inspector appliance.	
Syntax: `show network hostname`	
View	Normal
Parameters	None
Examples:	
To display the host name of the Deep Discovery Web Inspector appliance: `show network hostname`	

show network interface

TABLE 8-76. show network interface

Displays the network interface status and configuration for the Deep Discovery Web Inspector appliance.	
Syntax: `show network interface`	
View	Normal
Parameters	None
Examples:	
To display the network interface status and configuration: `show network interface`	

show network redirect

TABLE 8-77. show network redirect

Displays the current redirect policy for the Deep Discovery Web Inspector appliance.	
Syntax: `show network redirect`	
View	Normal
Parameters	None
Examples:	
To display the current redirect policy for the Deep Discovery Web Inspector appliance: `show network redirect`	

show network route

TABLE 8-78. show network route

Displays the IP address route table for the Deep Discovery Web Inspector appliance.	
Syntax: `show network route`	
View	Normal
Parameters	None
Examples:	
To display the IP address route table: `show network route`	

show network route default ipv4

TABLE 8-79. show network route default ipv4

Displays the default IPv4 gateway for the Deep Discovery Web Inspector appliance.	
Syntax: `show network route default ipv4`	
View	Normal
Parameters	None
Examples:	
To display system default IPv4 gateway: `show network route default ipv4`	

show network route ipv4

TABLE 8-80. show network route ipv4

Displays the IPv4 route table for the Deep Discovery Web Inspector appliance.	
Syntax: `show network route ipv4`	
View	Normal
Parameters	None
Examples:	
To display system IPv4 route table: `show network route ipv4`	

show process

TABLE 8-81. show process

Command family displays information about currently running processes on the Deep Discovery Web Inspector appliance. The parent command displays the status of the processes that are currently running.	
Syntax: `show process [target]`	
View	Normal
Parameters	**target**: Optionally specify a process name or ID; wildcards are supported
Examples:	
To display the status of the processes that are currently running: `show process`	

show process ltrace

TABLE 8-82. show process ltrace

Traces library calls of running processes.	
Syntax: `show process ltrace [pid]`	
View	Normal
Parameters	**pid**: The process ID number (pid)
Examples:	
To display the library call of process 1233: `show process ltrace 1233`	

show process stack

TABLE 8-83. show process stack

Prints a stack trace of a running process.	
Syntax: `show process stack [pid]`	
View	Normal
Parameters	**pid**: The process ID number (pid)
Examples:	
To display the stack trace of process 1233: `show process stack 1233`	

show process top

TABLE 8-84. show process top

Displays information about the top currently running processes. The processes with the most activity are at the top.	
Syntax: `show process top`	
View	Normal
Parameters	None
Examples:	
To display the status of the top processes that are currently running: `show process top`	

show process trace

TABLE 8-85. show process trace

Traces system calls and signals.	
Syntax: `show process trace [pid]`	
View	Normal
Parameters	**pid**: The process ID number (pid)
Examples:	
To display the system calls and signals of process 1233: `show process trace 1233`	

show kernel

TABLE 8-86. show product-info

Command family displays information about product settings for the Deep Discovery Web Inspector appliance.	
Syntax: `show product-info`	
View	Normal

show product-info management-port

TABLE 8-87. show product-info management-port

Displays the management port's IP address and subnet mask for the Deep Discovery Web Inspector appliance.	
Syntax: `show product-info management-port`	
View	Normal
Parameters	None
Examples:	
To display the management port's IP address and subnet mask: `show product-info management-port`	

show product-info operation-mode

TABLE 8-88. show product-info operation-mode

Displays the operation mode for the Deep Discovery Web Inspector appliance.
Syntax: `show product-info operation-mode`

View	Normal
Parameters	None
Examples:	
To display the operation mode: `show product-info operation-mode`	

show product-info service-status

TABLE 8-89. show product-info service-status

Displays the status of services for the Deep Discovery Web Inspector appliance.	
Syntax: `show product-info service-status`	
View	Normal
Parameters	None
Examples:	
To display the status of services: `show product-info service-status`	

show product-info version

TABLE 8-90. show product-info version

Displays the product version for the Deep Discovery Web Inspector appliance.	
Syntax: `show product-info version`	
View	Normal
Parameters	None

Examples:
To display the product version: `show product-info version`

show service

TABLE 8-91. show service

Command family displays the status and configuration information for Deep Discovery Web Inspector appliance services.	
Syntax: `show service`	
View	Normal

show service ntp

TABLE 8-92. show service ntp

Displays information about whether the NTP service is enabled and running for the Deep Discovery Web Inspector appliance.	
Syntax: `show service ntp`	
View	Normal
Parameters	None
Examples:	
To display the NTP service status: `show service ntp`	

show service ntp enabled

TABLE 8-93. show service ntp enabled

Displays information about whether the NTP service is enabled.	
Syntax: `show service ntp enabled`	
View	Normal
Parameters	None
Examples:	
To display whether the NTP service is enabled: `show service ntp enabled`	

show service ntp server-address

TABLE 8-94. show service ntp server-address

Displays the IP address for the NTP server.	
Syntax: `show service ntp server-address`	
View	Normal
Parameters	None
Examples:	
To display the IP address of the NTP server: `show service ntp server-address`	

show service ssh

TABLE 8-95. show service ssh

Displays information about whether the SSH service is enabled and running and, if enabled, what the listening port is for the service.	
Syntax: `show service ssh`	
View	Normal
Parameters	None
Examples:	
To display the SSH status: `show service ssh`	

show storage statistic

TABLE 8-96. show storage statistic

Displays statistics for file system disk space usage for the Deep Discovery Web Inspector appliance.	
Syntax: `show storage statistic [partition]`	
View	Normal
Parameters	**[partition]**: Optionally, specify a partition
Example:	
To display the file system disk space usage for the Deep Discovery Web Inspector appliance: `show storage statistic`	

show system

TABLE 8-97. show system

Command family displays system information for the Deep Discovery Web Inspector appliance.	
Syntax: `show system`	
View	Normal

show system date

TABLE 8-98. show system date

Displays the current date and time for the Deep Discovery Web Inspector appliance.	
Syntax: `show system date`	
View	Normal
Parameters	None
Examples:	
To display the current date and time of the Deep Discovery Web Inspector appliance: `show system date`	

show system license

TABLE 8-99. show system license

Displays information about the system license for the Deep Discovery Web Inspector appliance.
Syntax: `show system license`

View	Normal
Parameters	None
Examples:	

To display system license information for the Deep Discovery Web Inspector appliance:
`show system license`
`Product : Deep discovery Web Inspector-<model>`
`Version : <version>`
`Activation cdoe : xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx`
`Type : <license type>`
`Seats number : <seats>`
`Status : Activated`
`Expires on : <date>`	

show system timezone

TABLE 8-100. show system timezone

Displays the timezone settings for the Deep Discovery Web Inspector appliance.	
Syntax: `show system timezone`	
View	Normal
Parameters	None
Examples:	
To display the timezone settings: `show system timezone`	

show system timezone city

TABLE 8-101. show system timezone city

Displays the city configured in the timezone settings for the Deep Discovery Web Inspector appliance.

Syntax: `show system timezone city`	
View	Normal
Parameters	None
Examples:	
To display the city configured in the timezone settings for the Deep Discovery Web Inspector appliance:: `show system timezone city`	

show system timezone continent

TABLE 8-102. show system timezone continent

Displays the continent configured in the timezone settings for the Deep Discovery Web Inspector appliance.	
Syntax: `show system timezone continent`	
View	Normal
Parameters	None
Examples:	
To display the continent configured in the timezone settings for the Deep Discovery Web Inspector appliance: `show system timezone continent`	

show system timezone country

TABLE 8-103. show system timezone country

Displays the country configured in the timezone settings for the Deep Discovery Web Inspector appliance.

Syntax: `show system timezone country`	
View	Normal
Parameters	None
Examples:	
To display the country configured in the timezone settings for the Deep Discovery Web Inspector appliance: `show system timezone country`	

show system uptime

TABLE 8-104. show system uptime

Displays information about Deep Discovery Web Inspector appliance uptime and load information.	
Syntax: `show system uptime`	
View	Normal
Parameters	None
Examples:	
To display how long Deep Discovery Web Inspector has been running: `show system uptime`	

show system version

TABLE 8-105. show system version

Displays the version number for the Deep Discovery Web Inspector appliance.

Syntax: `show system version`	
View	Normal
Parameters	None
Examples:	
To display the version number of the Deep Discovery Web Inspector appliance: `show system version`	

shutdown

TABLE 8-106. shutdown

Shuts down the Deep Discovery Web Inspector appliance immediately or after a specified delay.	
Syntax: `shutdown [time]`	
View	Privileged
Parameters	**[time]**: Optional delay in minutes before shutting down the Deep Discovery Web Inspector appliance
Examples:	
To shut down the Deep Discovery Web Inspector appliance immediately: `shutdown`	
To shut down the Deep Discovery Web Inspector appliance after a 5 minute delay: `shutdown 5`	

start service

TABLE 8-107. start service

Command family starts system services for the Deep Discovery Web Inspector appliance.	
Syntax: `start service`	
View	Privileged

start service product

TABLE 8-108. start service product

Starts the product service.	
Syntax: `start service product`	
View	Privileged
Parameters	None
Example:	
To start the product service: `start service product`	

start service ssh

TABLE 8-109. start service ssh

Starts the SSH service.
Syntax: `start service ssh`

View	Privileged
Parameters	None
Example:	
To start the SSH service: `start ssh service`	

stop process

TABLE 8-110. stop process

Stops a running process on the Deep Discovery Web Inspector appliance.	
Syntax: `stop process [target]`	
View	Privileged
Parameters	**[target]**: Specify a process name
Example:	
To stop a process: `stop process`	

stop process core

TABLE 8-111. stop process core

Stops a running process on the Deep Discovery Web Inspector appliance and generates a core file.	
Syntax: `stop process core [target]`	
View	Privileged

Parameters	**[target]**: Specify a process name
Example:	
To stop a process and generate a core file: `stop process core`	

stop service

TABLE 8-112. stop service

Command family stops system services for the Deep Discovery Web Inspector appliance.	
Syntax: `stop service`	
View	Privileged

stop service product

TABLE 8-113. stop service product

Stops the product service.	
Syntax: `stop service product`	
View	Privileged
Parameters	None
Example:	
To stop the product service: `stop service product`	

stop service ssh

TABLE 8-114. stop service ssh

Stops the SSH service.	
Syntax: `stop service ssh`	
View	Privileged
Parameters	None
Example:	
To stop the SSH service: `stop ssh service`	

traceroute

TABLE 8-115. traceroute

Displays the route a packet takes to a specified destination.	
Syntax: `traceroute [hops] <dest> [-n]`	
View	Normal
Parameters	**[hops]**: Specifies the maximum number of hops to the destination The minimum number of hops to specify is 6. The default is 30 hops. **<dest>**: Specifies the host name or IP address of the remote system to trace **[-n]**: Do not resolve a host name
Examples:	

To display the route to IP address 172.10.10.1 with a maximum of 30 hops: `traceroute 172.10.10.1`
To display the route to IP address 172.10.10.1 with a maximum of 20 hops: `traceroute 20 172.10.10.1`

Chapter 9

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 9-2*
- *Contacting Trend Micro on page 9-3*
- *Sending Suspicious Content to Trend Micro on page 9-4*
- *Other Resources on page 9-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

Tip

To submit a support case online, visit the following URL:

http://esupport.trendmicro.com/srf/SRFMain.aspx

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	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 connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

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.

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.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

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

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Index

A

accessing
- Command Line Interface, 8-2
- management console, 3-5
- using the CLI to configure management console, 3-2

access syslog
- benefits, sending to a syslog server, 1-5

actions
- configuring for policies, 4-27

activating
- product licenses, 4-5

activating license
- during deployment, 3-6

activation code
- requirements, 2-32

Active Directory
- Active Directory Services providing integration with, 1-5

Active Directory Services
- providing integration with Microsoft Active Directory, 1-5

adding
- domain objects, 4-24
- HTTPS decryption rules, 4-31, 4-34
- network objects, 4-22, 4-23
- policies, 4-26, 4-27
- second bypass adapter, 2-21

administration, 6-4, 6-5
- back up settings, 6-4, 6-5
- configure integration with Deep Discovery Analyzer, 4-16
- hotfixes, 5-2

integrated products/services, Apex Central, 1-7

integrated products/services, Apex Central overview, 4-39

integrated products/services, overview of integration with Deep Discovery Director, 4-42

integrated products/services, registering Apex Central, 4-40

licenses, activating product licenses, 4-5

licenses, managing product licenses, 4-5

licenses, viewing product licenses, 4-5

managing contacts, 4-21

product updates, hotfixes and patches overview, 5-2

product upgrades, firmware upgrades, 5-3

product upgrades, managing patches, 5-2

reasons to perform backups, 6-1

restore settings, 6-4, 6-5

system maintenance, backing up or restoring a configuration, 6-1

system maintenance, network services diagnostics, 4-18

system maintenance, testing network connections, 4-18

system settings, configuring network settings, 4-5

system settings, configuring proxy settings, 4-17

system settings, notification SMTP server, 4-8

system settings, X-Header handling, 4-44
unable to restore settings, 6-4, 6-5
Virtual Analyzer, configuring network connections for, 4-13
Virtual Analyzer, image preparation overview, 4-11
Virtual Analyzer, importing images, 4-10
Virtual Analyzer, importing images from HTTP or FTP server, 4-12
Virtual Analyzer, importing images from local source, 4-11
Virtual Analyzer, network types, 4-15
admin menu
changing passwords, 3-6
advanced detection
benefits of, 1-3
aggregating
suspicious objects using Apex Central, 4-39
alert rules
configuring alert notifications, 4-20
modifying, 4-20
overview, 4-19
alerts
adding contacts for receiving, 4-21
configuring alert notifications, 4-20
critical alerts, 4-19
informational and important alerts, 4-19
notification parameters, 4-20
overview, 4-19
Apex Central
integration with, 1-7
overview, 1-7, 4-39
preparing for deployment, 2-38
providing synchronized suspicious objects integration with, 1-7
registering, 4-40
support for synchronizing suspicious objects, 4-39
what functionality is integrated with, 1-7
appliance
setting up for deployment, 3-2
auto tunneling
HTTP decryption rules, 4-34

B

backup, 6-4, 6-5
backups
creating to restore configuration or replicate settings across devices, 6-1
benefits
advanced detection, 1-3
description of, 1-2
easy-to-use policy management, 1-2
flexible deployment, 1-2
HTTP/2 scanning, 1-4
HTTPS inspection, 1-4
patient zero protection, 1-5
real-time visibility, analysis, action, 1-2
send access syslogs to a syslog server, 1-5
Virtual Analyzer sandbox analysis, 1-4
browsers
supported, 2-27, 2-32
supported for deployment, 2-27
bypass adapter
adding second, 2-21

C

cables
requirements, 2-32

changing
passwords, 3-6
CLI, 8-1. *See also* Command Line Interface
command line interface
entering the shell environment, 8-3
using to configure management console access, 3-2
Command Line Interface
accessing, 8-2
using the, 8-1
configuration
additional tasks, 4-43
configuration settings
backup or restore, 6-1
configuring
management console access, 3-2
network settings, 4-5
notification SMTP servers, 4-8
proxy settings, 4-17
using the management console, 3-5
X-Header handling settings, 4-44
considerations
before reinstalling, 7-2
pre-deployment, 2-2
console navigation, 4-1
contacts
adding for notifications alerts, and reports, 4-21
managing, 4-21
creating
backups for restoring configuration or to replicate settings across devices, 6-1
critical alerts
configuring notifications for, 4-20
overview, 4-19
CSR
generating for HTTPS decryption rules, 4-31, 4-38
custom network
configuring for Virtual Analyzer network connections, 4-13
Virtual Analyzer network type, 4-15

D

decryption categories
HTTP decryption rules, 4-34
decryption domain objects
HTTP decryption rules, 4-34
decryption rules
for HTTPS, overview, 4-32
viewing HTTPS, 4-33
decryption sources
HTTP decryption rules, 4-34
Deep Discovery Analyzer
configuring integration with, 4-16
integration with, 1-6
providing virtual analysis by integration with, 1-6
Deep Discovery Analyzer integration, 4-16
Deep Discovery Director
integration with, 1-6
overview of integration with, 4-42
providing centralized management by integration with, 1-6
providing synchronized suspicious objects integration with, 1-6
support for synchronizing suspicious objects with, 4-42
deploying
forward proxy mode using deployment wizard, 3-9
LACP using deployment wizard, 3-22

multi-bridge mode using deployment wizard, 3-19
transparent bridge mode using deployment wizard, 3-12
transparent HA mode using deployment wizard, 3-15
deployment, 3-1
activating the license, 3-6
Apex Central, 2-38
benefits of flexible, 1-2
browser and system requirements, 2-27
deployment mode overview, 2-3
enabling and starting SSH service, 2-28
forward proxy mode, 2-3
fresh installation, 7-2
initial deployment for LACP, 3-22
initial deployment of forward proxy mode, 3-9
initial deployment of multi-bridge mode, 3-19
initial deployment of transparent bridge mode, 3-12
initial deployment of transparent HA mode, 3-15
items to prepare, 2-32
LACP, 2-16
multi-bridge mode, 2-14
opening the management console, 3-5
ports used by appliance, 2-29
recommended network environment, 2-27
setting up the appliance, 3-2
setting up the hardware, 3-2
tasks to perform before, 2-2
transparent bridge mode, 2-4, 2-5
transparent bridge mode with trunks, 2-6
transparent HA, 2-9
transparent HA mode, 2-8
transparent HA mode with trunk links, 2-11
using CLI to configure management console access, 3-2
using the deployment wizard, 3-9
deployment mode
forward proxy, 2-3
multi-bridge, 2-14
transparent bridge, 2-4, 2-5
transparent bridge with trunk links, 2-4
transparent bridge with trunks, 2-6
transparent HA, 2-8, 2-9, 2-11
transparent HA with trunk links, 2-8
with LACP, 2-16
deployment modes
ports used for each mode, 4-5
deployment wizard
initial deployment for LACP, 3-22
initial deployment of forward proxy mode, 3-9
initial deployment of multi-bridge mode, 3-19
initial deployment of transparent bridge mode, 3-12
initial deployment of transparent HA mode, 3-15
performing initial deployment, 3-9
diagnostics
system maintenance, network services diagnostics, 4-18
documentation feedback, 9-6
domain objects

managing, 4-24
selecting for policies, 4-27
viewing, adding, editing, removing, importing, exporting, 4-24
Download Center
downloading firmware, 5-3
downloading patches and hotfixes, 5-2
URL, 5-2, 5-3
downloading
patches and hotfixes, 5-2
duplicating
HTTPS decryption rules, 4-31
policies, 4-26

E

editing
domain objects, 4-24
HTTPS decryption rules, 4-31, 4-34
network objects, 4-22, 4-23
enabling and starting
SSH service, 2-28
enabling or disabling
HTTPS decryption rules, 4-31
policies, 4-27
entering
Command Line Interface, 8-2
Ethernet cables
requirements, 2-32
exporting
domain objects, 4-24
network objects, 4-22
export settings, 6-4

F

features
Active Directory Services, providing integration with Microsoft Active Directory, 1-5
advanced detection, 1-3
description of, 1-2
easy-to-use policy management, 1-2
flexible deployment, 1-2
HTTP/2 scanning, 1-4
HTTPS inspection, 1-4
integration with Apex Central, 1-7
integration with Deep Discovery Analyzer, 1-6
integration with Deep Discovery Director, 1-6
patient zero protection, 1-5
real-time visibility, analysis, action, 1-2
send access syslogs to a syslog server, 1-5
Virtual Analyzer sandbox analysis, 1-4
file types
selecting for policies, 4-27
firmware
downloading and updating, 5-3
forward proxy
deployment mode, topology overview, 2-3
mode overview, 2-3
requirements, 2-32
forward proxy mode
initial configuration using the deployment wizard, 3-9
initial deployment using deployment wizard, 3-9
FTP servers
importing Virtual Analyzer images from, 4-12

G

generating
CSR for HTTPS decryption rules, 4-31, 4-38
getting started, 4-1
console navigation, 4-1
getting started tasks, 4-1
opening the management console, 3-5
tasks, 4-2
guest user
selecting as traffic source for policies, 4-27

H

hardware
setting up for deployment, 3-2
hotfixes
managing, 5-2
hot fixes
overview, 5-2
HTTP/2 scanning
benefits, 1-4
HTTP decryption rules
generating an CSR for, 4-38
HTTPS
overview of decryption rules for, 4-32
HTTPS decryption rules
managing, 4-31
overview, 4-32
viewing, 4-33
viewing, adding, editing, duplicating, removing, ordering, creating CSR file for, 4-31
HTTP servers
importing Virtual Analyzer images from, 4-12
HTTPS inspection
benefits and features, 1-4

I

image import tool
Virtual Analyzer, using to import from local source, 4-11
image preparation
Virtual Analyzer, overview of, 4-11
image preparation tool
Virtual Analyzer, overview of, 4-11
images
importing for internal virtual analyzer, 4-9
Virtual Analyzer, importing, 4-10
Virtual Analyzer, importing from HTTP or FTP server, 4-12
Virtual Analyzer, importing from local source, 4-11
important alerts
configuring notifications for, 4-20
overview, 4-19
importing
domain objects, 4-24
internal virtual analyzer images, 4-9
network objects, 4-22
Virtual Analyzer images, 4-10
Virtual Analyzer images from HTTP or FTP server, 4-12
Virtual Analyzer images from local source, 4-11
importing certificates
HTTP decryption rules, 4-34
import settings, 6-5
informational alerts
configuring notifications for, 4-20
overview, 4-19
initial deployment

using the deployment wizard, 3-9
installation
fresh, operating system, 7-2
getting started, 4-1
installing
firmware upgrades, 5-3
patches and hotfixes, 5-2
integrated products/services
Apex Central, overview, 1-7
Apex Central overview, 4-39
overview of integration with Deep Discovery Director, 4-42
registering Apex Central, 4-40
integration, 4-16
with Apex Central, 1-7
with Deep Discovery Analyzer, 1-6
with Deep Discovery Director, 1-6
with Microsoft Active Directory with Active Directory Services, 1-5
intelligent decryption
HTTP decryption rules, 4-34
internal virtual analyzer
importing images, 4-9
introduction
Deep Discovery Web Inspector, 1-2
IP addresses
requirements, 2-32

L

LACP
adding second bypass adapter for, 2-21
deployment modes that support, 2-19
graphical representation of LCAP on appliance, 2-19
how LCAP works with Deep Discovery Web Inspector, 2-19
initial configuration using the deployment wizard, 3-9
initial deployment of transparent bridge mode with, 3-12
initial deployment using deployment wizard, 3-22
support information, 2-19
topology and overview, 2-3
transparent bridge with trunks, mode overview, 2-6
transparent HA mode topology using LACP trunks, 2-8
LACP deployments
deployment mode, topology overview, 2-3
overview and topology, 2-16
license
activating during deployment, 3-6
licenses
activating product, 4-5
managing product, 4-5
viewing product, 4-5
Link Aggregation Control Protocol. *See* LACP
local or network folders
importing Virtual Analyzer images from, 4-11

M

management console
navigation, 4-2
opening the, 3-5
using the CLI to configure, 3-2
management network
configuring for Virtual Analyzer network connections, 4-13
Virtual Analyzer network type, 4-15

management port, 4-5
managing
contacts, 4-21
domain objects, 4-24
HTTPS decryption rules, 4-31
network objects, 4-22
policies, 4-26
product licenses, 4-5
user-defined settings, 4-21
using the management console, 3-5
maximum throughput
expected for each appliance model, 2-27
Microsoft Active Directory. *See* Active Directory
modifying
alert rules, 4-20
policies, 4-26
multi-bride mode
adding second bypass adapter for, 2-21
multi-bridge
deployment mode, topology overview, 2-3
mode overview, 2-14
multi-bridge mode
initial configuration using the deployment wizard, 3-9
initial deployment using deployment wizard, 3-19

N

navigating
management console, 4-2
network
services diagnostics, system maintenance, 4-18
network connections
configuring for Virtual Analyzer, 4-13
network environment
recommended, 2-27
network objects
managing, 4-22
selecting as traffic sources for policies, 4-27
viewing, adding, editing, importing/exporting, removing, 4-22
network services diagnostics
system maintenance, 4-18
network setting
ports used for each deployment mode, 4-5
network settings
configuring, 4-5
network topology
forward proxy mode, 2-3
LACP, 2-16
multi-bridge mode, 2-14
overview of deployment modes, 2-3
transparent bridge, 2-5
transparent bridge mode, 2-4, 2-5
transparent bridge mode with trunk links, 2-4
transparent bridge mode with trunks, 2-6
transparent HA, 2-9
transparent HA mode, 2-8
transparent HA mode with trunk links, 2-8, 2-11
network topology with LACP
deployments, 2-16
network topology with trunk links
transparent HA mode, 2-11
network topology with trunks
transparent bridge, 2-6

network types
Virtual Analyzer, 4-15
Virtual Analyzer, custom network, management network, no access, 4-15
new features and enhancements, 1-8
no access
Virtual Analyzer network type, 4-15
no network access
configuring for Virtual Analyzer network connections, 4-13
notifications
adding contacts for receiving, 4-21
configuring for alert rules, 4-20
configuring SMTP server for, 4-8
parameters for alert, 4-20

O

opening
management console, 3-5
ordering
HTTPS decryption rules, 4-31
policies, 4-26
overview
Apex Central, 4-39
Deep Discovery Web Inspector, 1-2
domain objects, 4-24
features and benefits, 1-2
hotfixes and patches, 5-2
HTTPS decryption rules, 4-32
network objects, 4-22
of integration with Deep Discovery Director, 4-42
Virtual Analyzer, image preparation, 4-11

P

parameters
for alert notifications, 4-20
passwords
changing, 3-6
patches
managing, 5-2
overview, 5-2
patient zero. *See* patient zero protection
patient zero protection
benefits of, 1-5
definition, 1-5
Patient Zero Protection
enabling for policies, 4-27
policies
adding, 4-27
adding, viewing, modifying, duplicating, removing, and ordering, 4-26
benefit of enabling patient zero protection, 1-5
default policy, 4-26
enabling or disabling, 4-26, 4-27
enabling Patient Zero Protection, 4-27
how exception lists are used, 4-30
managing, 4-26
traffic source exceptions, 4-30
policy management
benefits of easy-to-use, 1-2
policy rules. *See* policies
ports, 2-29
used by appliance, 2-29
used for each deployment mode, 4-5
pre-deployment
Apex Central, 2-38
browser and system requirements, 2-27
considerations, 2-2
deployment mode overview, 2-3
enabling and starting SSH service, 2-28

items to prepare, 2-32
ports used by appliance, 2-29
recommended network environment, 2-27
tasks, 2-2
preparing
for deployment, Apex Central, 2-38
for deployment, ports used by appliance, 2-29
items for deployment, 2-32
preparing for deployment, 2-1
product updates
hotfixes and patches overview, 5-2
product upgrades
managing patches, 5-2
updating firmware, 5-3
proxy setting
what is affected by, 4-17
proxy settings
configuring, 4-17

R

recommendations
network environment, 2-27
registering
Apex Central, 4-40
reinstalling
considerations, 7-2
operating system, 7-2
tasks to consider before, 7-2
removing
domain objects, 4-24
HTTPS decryption rules, 4-31
network objects, 4-22
policies, 4-26
replicate settings
across devices using backups, 6-1
reports
adding contacts for receiving, 4-21
required tasks
you must perform to get started, 4-2
requirements
deployment, 2-27
enabling and starting SSH service, 2-28
multi-bridge, 2-32
pre-deployment, 2-32
SSH access, 2-27
transparent bridge with trunk links, 2-32
transparent HA, 2-9
restore, 6-4, 6-5
restoring configuration
using backups, 6-1
rolling back
hotfixes and patches, 5-2

S

sandbox analysis
benefits of, 1-4
sandbox images
Virtual Analyzer, importing, 4-10
Virtual Analyzer, importing from HTTP or FTP server, 4-12
Virtual Analyzer, importing from local source, 4-11
Virtual Analyzer, preparation of, 4-11
security patches
overview, 5-2
services
affected by proxy settings, 4-17
settings
managing user-defined, 4-21
setting up
hardware for deployment, 3-2
shell environment, 8-3

SMTP
notification server, configuring, 4-8
SSH
enabling and starting service, 2-28
requirements for access using, 2-27
SSH service
enabling and starting, 2-28
starting
SSH service, 2-28
support
how LACP works with Deep Discovery Web Inspector, 2-19
resolve issues faster, 9-4
suspicious objects
Apex Central support for synchronizing, 4-39
support for synchronizing with Deep Discovery Director, 4-42
synchronizing
suspicious objects with Deep Discovery Director, 4-42
system maintenance
backing up or restoring a configuration, 6-1
network services diagnostics, 4-18
testing network connections, 4-18
system requirements
deployment, 2-27
enabling and starting SSH service, 2-28
pre-deployment, 2-32
system settings
configuring network settings, 4-5
configuring notification SMTP server, 4-8
configuring proxy settings, 4-17
configuring X-Header handling settings, 4-44

T

tasks
additional, you must perform to get started, 4-2
additional configuration, 4-43
getting started, 4-2
pre-deployment, 2-2
to consider before reinstalling, 7-2
to perform after getting started, 4-43
testing connections. *See* network service diagnostics
testing network connections. *See* network service diagnostics
throughput
maximum expected for each appliance model, 2-27
topology
transparent bridge, 2-4
transparent bridge with trunk links, 2-4
traffic source exceptions
policies, 4-30
traffic sources
selecting for policies, 4-27
transparent bridge
deployment mode, topology overview, 2-3
mode overview, 2-4
overview, 2-5
requirements, 2-32
with trunks, mode overview, 2-6
with trunks, overview, 2-6
transparent bridge mode
initial configuration using the deployment wizard, 3-9

initial deployment using deployment wizard, 3-12
transparent bridge mode with LACP
adding second bypass adapter for, 2-21
transparent bridge with trunk links
mode overview, 2-4
transparent bridge with trunks
mode overview, 2-6
transparent HA
deployment mode, topology overview, 2-3
mode overview, 2-8, 2-9
requirements, 2-32
with trunk links, mode overview, 2-11
transparent HA mode
initial configuration using the deployment wizard, 3-9
initial deployment using deployment wizard, 3-15
network topology, 2-8
with trunk links, network topology, 2-8
transparent HA mode with LACP
adding second bypass adapter for, 2-21
transparent HA with trunk links
mode overview, 2-8, 2-11
triggered alerts
overview, 4-19

U

updating
firmware, 5-3
user-defined settings
managing, 4-21
managing approved/blocked lists, 4-21
managing domain objects, 4-21
managing network objects, 4-21
managing notifications, 4-21
users and groups
selecting as traffic sources for policies, 4-27
using
Command Line Interface, 8-1

V

viewing
domain objects, 4-24
HTTPS decryption rules, 4-31, 4-33
information about CA used to resign, 4-33
network objects, 4-22
policies, 4-26
product licenses, 4-5
virtual analyzer
importing images for internal, 4-9
Virtual Analyzer
benefit of enabling patient zero protection, 1-5
benefits of sandbox analysis, 1-4
configuring network settings for, 4-13
image preparation overview, 4-11
importing images, 4-10
importing images from HTTP or FTP server, 4-12
importing images from local source, 4-11
integration with Deep Discovery Analyzer, 4-16
network types, 4-15

X

X-Authenticated-User settings
configuring, 4-44
XFF settings
configuring, 4-44

X-Forwarded-For settings
configuring, 4-44
X-Header handling settings
configuring, 4-44

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM28795/190819