TREND MICRO™

2.5

TREND MICRO™

Deep Discovery Web Inspector

Administrator's Guide

Advanced Protection Against Targeted Web Attacks

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

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/

Document Part No.: APEM28796/190819

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

Chapter 1: Introduction

Chapter 2: Preparing for Deployment

Chapter 3: Deployment

Chapter 4: Getting Started

Chapter 5: Dashboard

Chapter 6: Detections

Chapter 7: Policy

Chapter 8: Alerts and Reports

Chapter 9: Administration

Chapter 10: Licensing and Maintenance

Chapter 11: Technical Support

Appendices

Appendix A: Using the Command Line Interface

Appendix B: SNMP Object Identifiers

Index

Preface

Preface

Topics include:

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:

Chapter 1

Introduction

Topics include:

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.

A New Threat Landscape

Where once attackers were content to simply deface a website or gain notoriety through mass system disruption, they now realize that they can make significant money, steal important data, or interfere with major infrastructure systems via cyber warfare instead.

A targeted attack is a long-term cyber-espionage campaign against a person or organization to gain persistent access to the target network. This allows them to extract confidential company data and possibly damage the target network. These compromised networks can be used for attacks against other organizations, making it harder to trace the attack back to its originator.

Advanced Persistent Threats

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

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

TABLE 1-1. APT Attack Sequence

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

Phase	Description
Asset/Data Discovery	Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest
Data Exfiltration	Unauthorized data transmission to external locations Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.

Deep Discovery Web Inspector can detect APT and targeted attacks by identifying malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

C&C Callback

The following actions usually occur when malicious software installs and communicates back to a C&C server:

- Software called a "downloader" automatically downloads and installs malware.
- A human monitoring the C&C server (attacker) responds to the connection with an action. Software called a "remote access Trojan" (RAT) gives an attacker the ability to examine a system, extract files, download new files to run on a compromised system, turn on a system's video camera and microphone, take screen captures, capture keystrokes, and run a command shell.

Attackers will attempt to move laterally throughout a compromised network by gaining additional persistent access points. Attackers will also attempt to steal user credentials for data collection spread throughout the network. If successful, collected data gets exfiltrated out of the network to another environment for further examination.

Attackers move at a slow pace to remain undetected. When a detection occurs, they will temporarily go dormant before resuming activity. If an organization eradicates their presence from the network, the attackers will start the attack cycle all over again.

A New Solution

Deep Discovery Web Inspector prevents network-based attacks and cyber threats by investigating suspicious domain and network objects and associated file types and social engineering attack patterns in web content before they can threaten your network. Designed to integrate into your existing network topology, Deep Discovery Web Inspector monitors your network for cyber threats using either transparent bridge or forward proxy mode.

Whichever deployment method is chosen, Deep Discovery Web Inspector investigates web traffic for suspicious file types, domains, URLs, or embedded links (URLs). If an object exhibits malicious behavior, Deep Discovery Web Inspector can block the threat and notify security administrators about the malicious activity.

After Deep Discovery Web Inspector scans a network object for known threats in the Trend Micro Smart Protection Network, it passes suspicious files to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

After investigating the suspicious object, Deep Discovery Web Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Web Inspector calculates the risk level based on the highest risk assigned between the Deep Discovery Web Inspector scanners and Virtual Analyzer.

Deep Discovery Web Inspector acts upon network objects according to the assigned risk level and policy settings. Configure Deep Discovery Web Inspector to block the content or monitor the network content and allow the network content to pass to the end user. While Deep Discovery Web Inspector monitors your network for threats, you can access dashboard widgets and reports for further investigation.

Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

After detecting an unknown or low-prevalence file, Deep Discovery Web Inspector scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

Depending on how you configure your policies, Deep Discovery Web Inspector can block the object to prevent the threat from continuing to spread across your network. Alternatively, you can configure the policy to monitor and log information about the object without blocking it.

Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH). Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation
- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change

- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.

Advanced Threat Scan Engine

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

Major features include:

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

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web Reputation Services assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

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

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 9-63*.

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

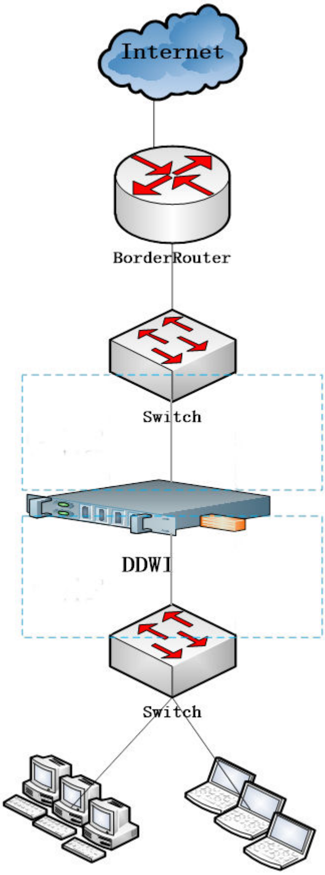


FIGURE 2-1. Transparent Bridge mode

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

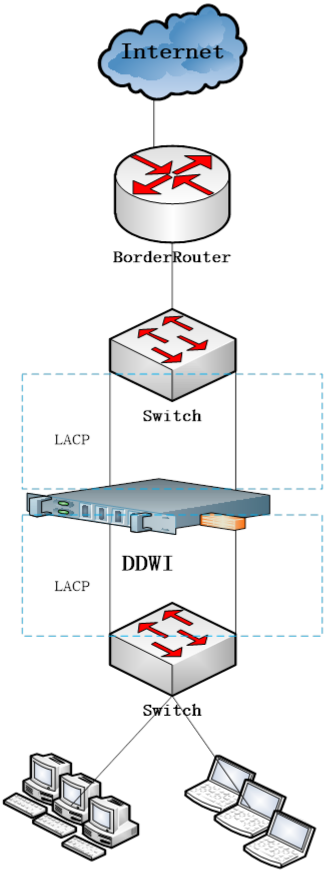


FIGURE 2-2. Transparent Bridge mode with trunks

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

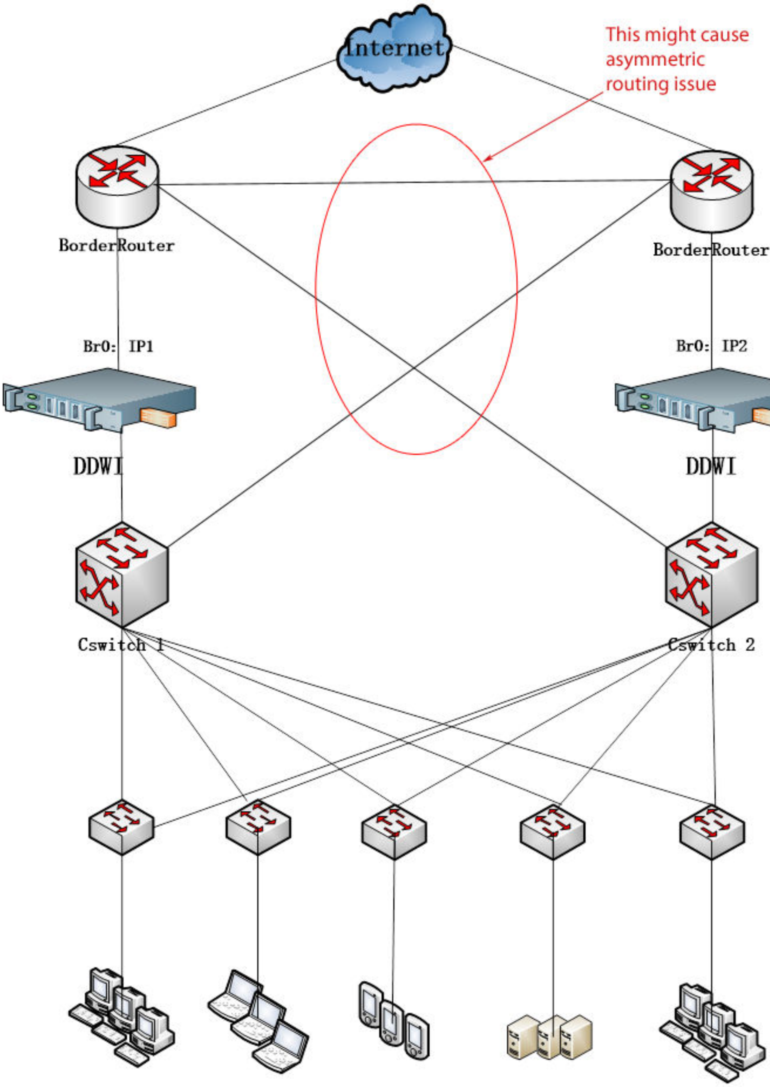


FIGURE 2-3. Transparent HA mode

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

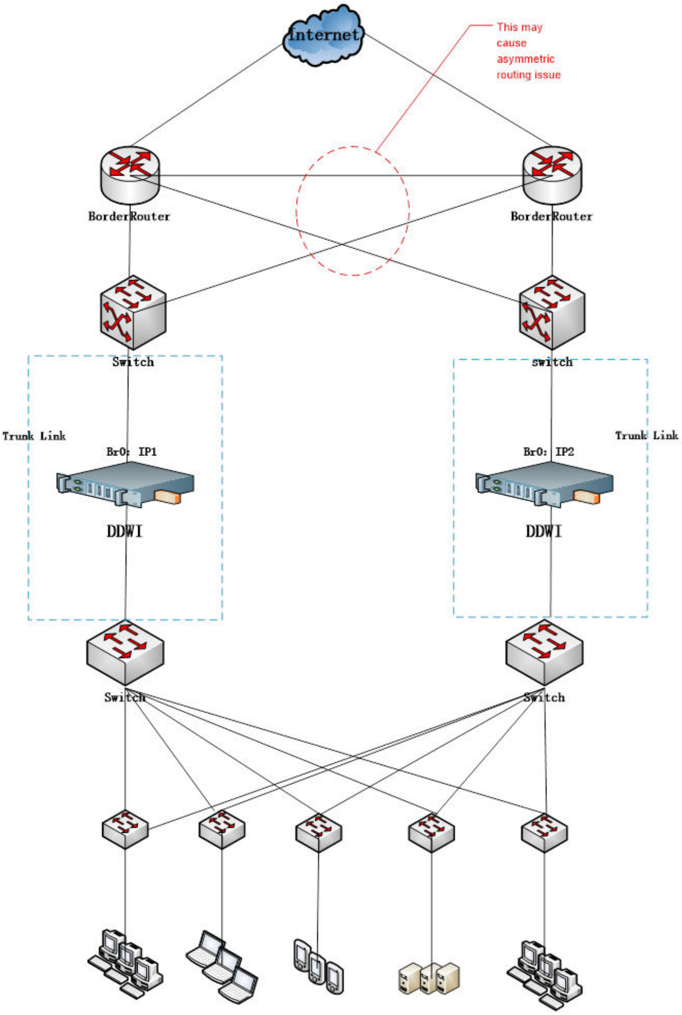


FIGURE 2-4. Transparent HA with trunk links

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.

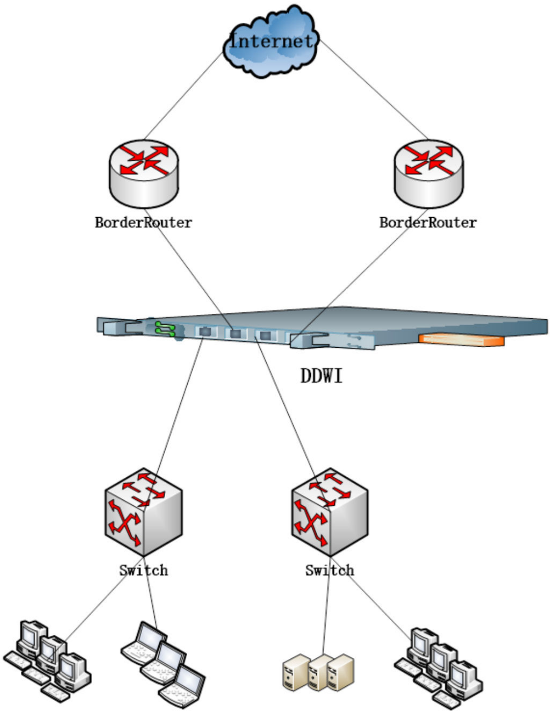


FIGURE 2-5. Multi-Bridge mode deployment

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*.

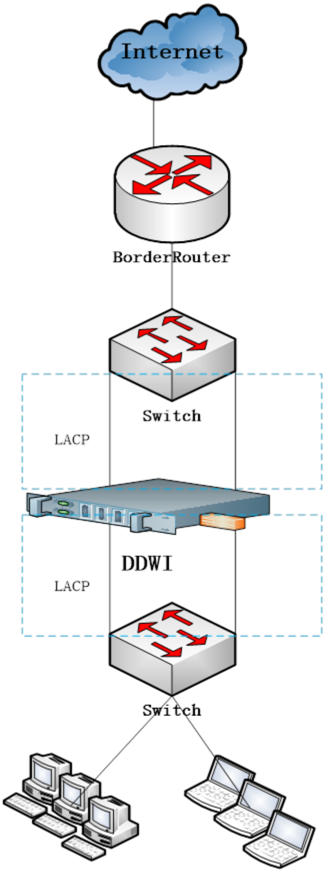


FIGURE 2-6. Transparent Bridge mode with LACP

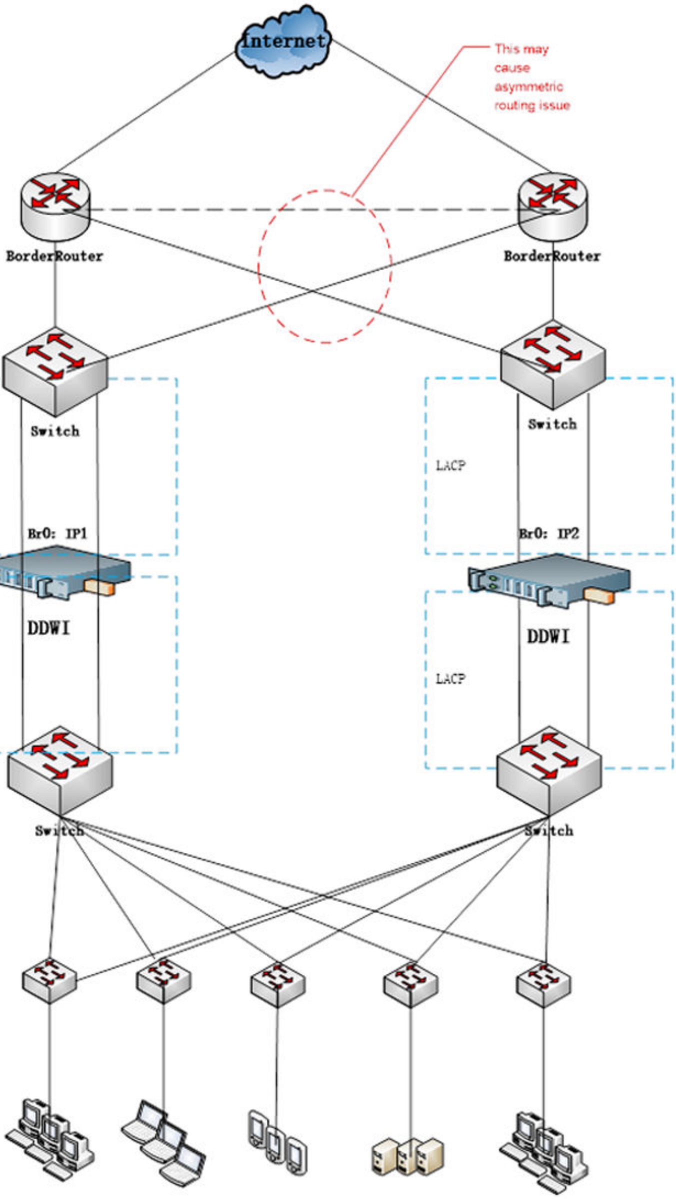


FIGURE 2-7. Transparent HA mode with LACP

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

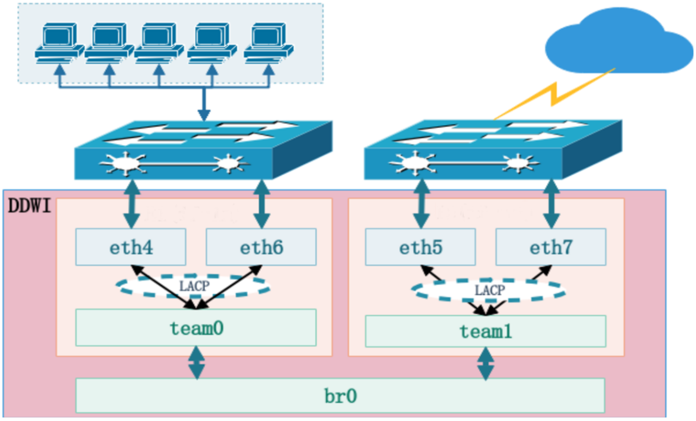


FIGURE 2-8. LACP enabled on Transparent Bridge mode

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

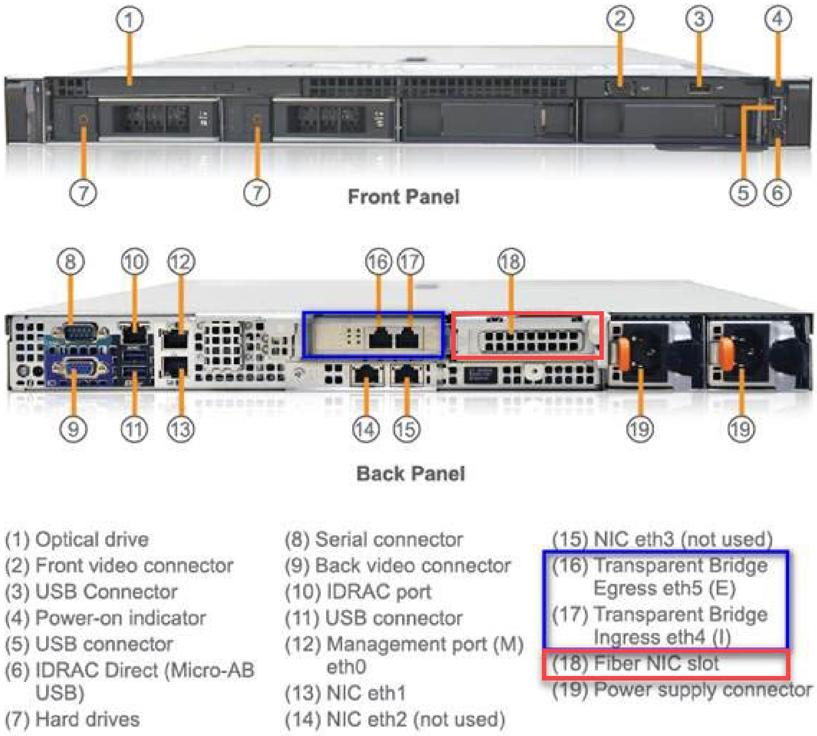
When deploying Multi-Bridge mode or LACP-enabled configurations on your Deep Discovery Web Inspector appliance, the appliance configures data ingress/egress using the eth4/eth5 (bypass card 1), eth6/eth7 (bypass card 2) interfaces.

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:



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

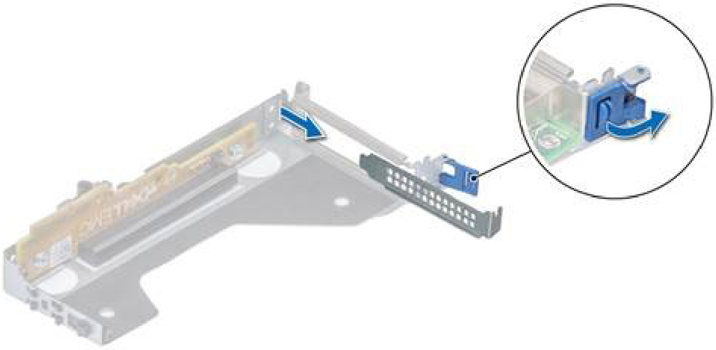
P/N	Description	Notes
PE2G2PBI80-SD-R	Dual Port Copper Gigabit PCI Ethernet PCI Express Bypass Server Adapter	x4, Based on Intel 82580DB, PCI-E Gen 2.0, RoHS compliant

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.

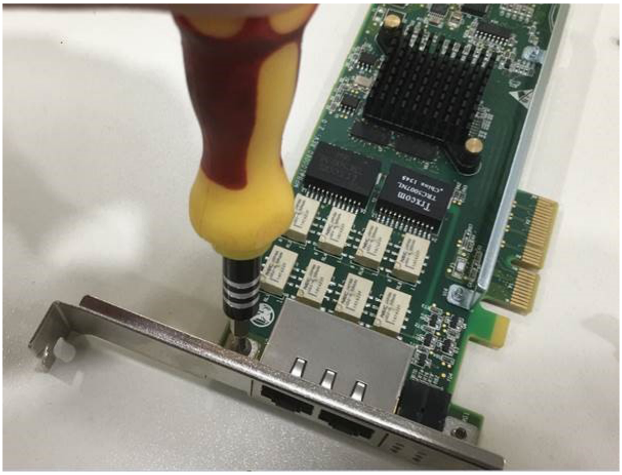
   b. Disconnect the appliance from the power supplies.

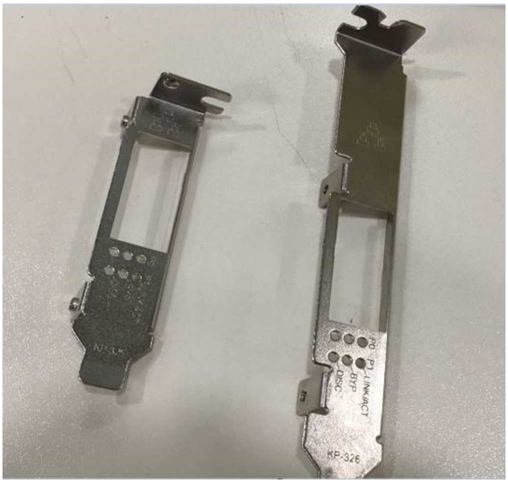
   c. Open the appliance chassis and pull the PCIe adapter holder latch, then remove the filler bracket.



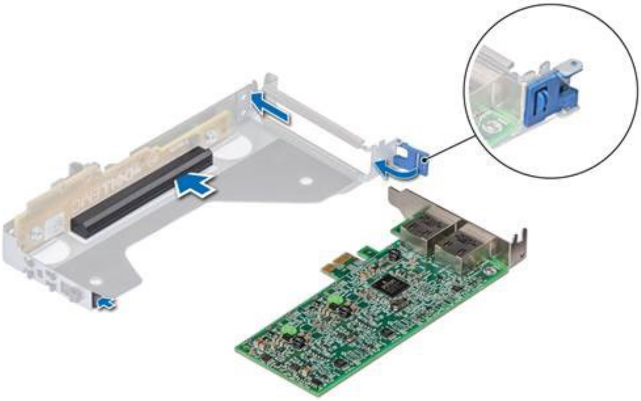
   d. Replace the standard adapter riser with the provided low-profile riser using the following images for guidance.

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.

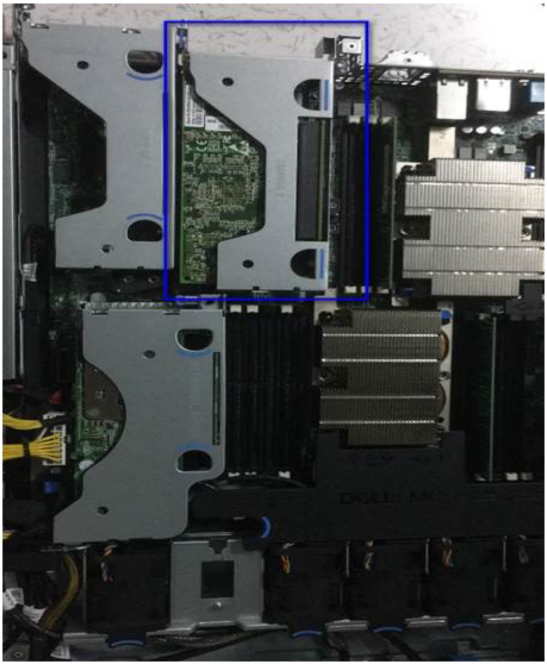




e. Hold the adapter by its edges and align the adapter edge connector with the adapter connector on the riser. Insert the adapter edge connector firmly into the adapter connector until the adapter is fully seated. Then close the adapter retention latch.

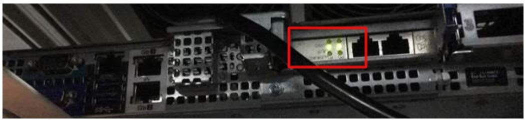


f. Fix the adapter holder latch into the appliance's chassis.



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 A-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 9-60* 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

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

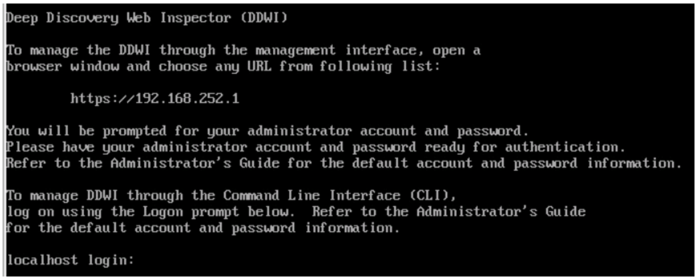
Before you can perform the initial deployment of Deep Discovery Web Inspector, you must log on to the Command Line Interface (CLI) and configure access to the Deep Discovery Web Inspector management console.

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.

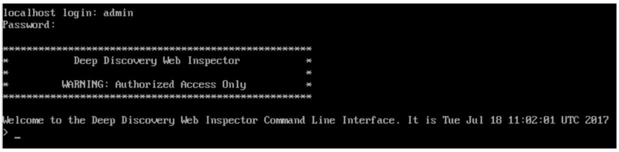
The appliance's command line interface is displayed on the monitor. You can log in to the CLI and perform basic tasks.



```
Deep Discovery Web Inspector (DDWI)

To manage the DDWI through the management interface, open a
browser window and choose any URL from following list:

        https://192.168.252.1

You will be prompted for your administrator account and password.
Please have your administrator account and password ready for authentication.
Refer to the Administrator's Guide for the default account and password information.

To manage DDWI through the Command Line Interface (CLI),
log on using the Logon prompt below.  Refer to the Administrator's Guide
for the default account and password information.

localhost login:
```

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

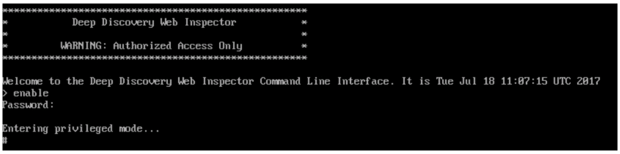
    - User name: `admin`
    - Password: `ddwi`



```
localhost login: admin
Password:

****************************************************
*           Deep Discovery Web Inspector           *
*                                                  *
*         WARNING: Authorized Access Only          *
****************************************************

Welcome to the Deep Discovery Web Inspector Command Line Interface. It is Tue Jul 18 11:02:01 UTC 2017
> _
```

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

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



```
****************************************************
*           Deep Discovery Web Inspector           *
*                                                  *
*         WARNING: Authorized Access Only          *
****************************************************

Welcome to the Deep Discovery Web Inspector Command Line Interface. It is Tue Jul 18 11:07:15 UTC 2017
> enable
Password:

Entering privileged mode...
#
```

    The prompt changes from > to #.

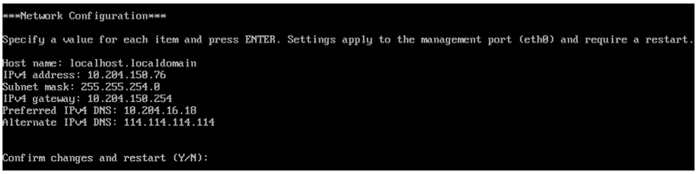
6. Configure network settings with the following command:

    ```
    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



```
***Network Configuration***

Specify a value for each item and press ENTER. Settings apply to the management port (eth0) and require a restart.

Host name: localhost.localdomain
IPv4 address: 10.204.150.76
Subnet mask: 255.255.254.0
IPv4 gateway: 10.204.150.254
Preferred IPv4 DNS: 10.204.16.18
Alternate IPv4 DNS: 114.114.114.114


Confirm changes and restart (Y/N):
```

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 A-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**

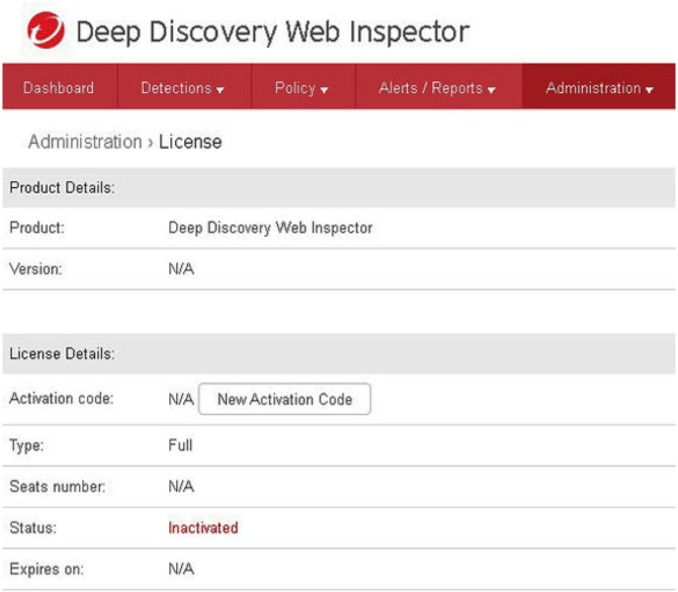
3. Click **Save**.

Activating the License

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

Procedure

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

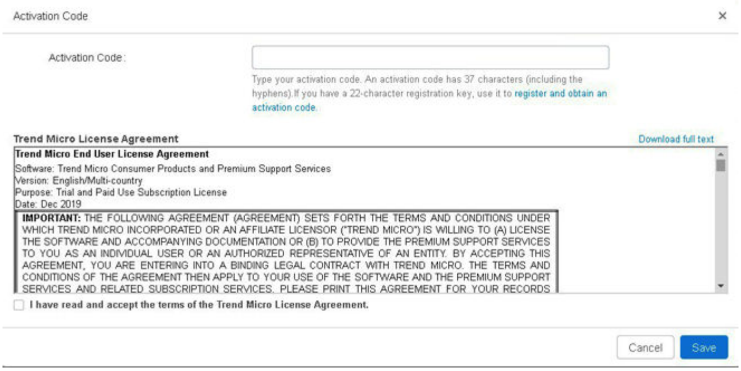


Product Details:	
Product:	Deep Discovery Web Inspector
Version:	N/A

License Details:	
Activation code:	N/A New Activation Code
Type:	Full
Seats number:	N/A
Status:	Inactivated
Expires on:	N/A

2. Click **New Activation Code**.

The **Activation Code** screen displays.



Activation Code ×

Activation Code:

Type your activation code. An activation code has 37 characters (including the hyphens).If you have a 22-character registration key, use it to register and obtain an activation code.

Trend Micro License Agreement Download full text

Trend Micro End User License Agreement
Software: Trend Micro Consumer Products and Premium Support Services
Version: English/Multi-country
Purpose: Trial and Paid Use Subscription License
Date: Dec 2019

IMPORTANT: THE FOLLOWING AGREEMENT (AGREEMENT) SETS FORTH THE TERMS AND CONDITIONS UNDER WHICH TREND MICRO INCORPORATED OR AN AFFILIATE LICENSOR ("TREND MICRO") IS WILLING TO (A) LICENSE THE SOFTWARE AND ACCOMPANYING DOCUMENTATION OR (B) TO PROVIDE THE PREMIUM SUPPORT SERVICES TO YOU AS AN INDIVIDUAL USER OR AN AUTHORIZED REPRESENTATIVE OF AN ENTITY. BY ACCEPTING THIS AGREEMENT, YOU ARE ENTERING INTO A BINDING LEGAL CONTRACT WITH TREND MICRO. THE TERMS AND CONDITIONS OF THE AGREEMENT THEN APPLY TO YOUR USE OF THE SOFTWARE AND THE PREMIUM SUPPORT SERVICES AND RELATED SUBSCRIPTION SERVICES. PLEASE PRINT THIS AGREEMENT FOR YOUR RECORDS

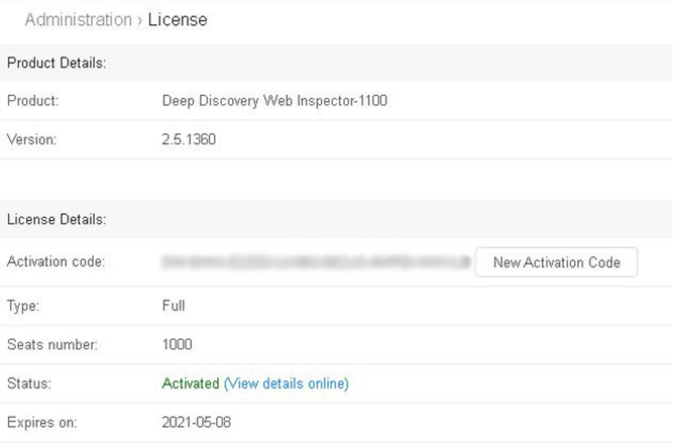
□ **I have read and accept the terms of the Trend Micro License Agreement.**

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.



Administration › License

Product Details:	
Product:	Deep Discovery Web Inspector-1100
Version:	2.5.1360

License Details:	
Activation code:	[redacted] New Activation Code
Type:	Full
Seats number:	1000
Status:	Activated (View details online)
Expires on:	2021-05-08

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 9-42*.

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**.

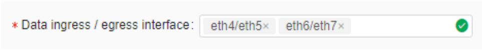
4. In the **Working Mode Settings** page, specify the following:

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**.  * Data ingress / egress interface: 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 4-3*

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 *Dashboard Overview on page 5-2*. • Name of the user currently logged on: Click and select one of the following: • **Change password** to change the account password (see *Changing Your Password on page 3-6*) Note If using an Active Directory user account to access the Administrative Web console, the **Change password** option is not available. • **Log off** to log out of the management console. • **Change server certificate** to change the certificate used for the Administrative Web console or Captive Portal. • 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.

SECTION	DETAILS
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. The following steps provide a high-level overview of these additional tasks. Each step links to more detailed instructions later in the document.

Note

If you have not completed the initial deployment, see *Deployment on page 3-1*.

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 10-5*.

3. Configure additional network settings as needed.

For details, see *Configuring Network Settings on page 9-27*.

4. Configure the notification SMTP server.

For details, see *Configuring the Notification SMTP Server on page 9-33*.

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 *Virtual Analyzer Images on page 9-82*. For details, see *Importing Virtual Analyzer Images on page 9-83*. **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 9-87*. No network access is the default.
External	a. Record the Deep Discovery Analyzer API key. 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 9-90*.

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

For details, see *Configuring Proxy Settings on page 9-31*.

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

For details, see *Alerts on page 8-2*.

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 7-3* and *Managing User-Defined Settings on page 7-46*.

9. (Optional) Configure HTTPS decryption rules.

For details, see *Managing HTTPS Decryption Rules on page 7-13*.

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 9-59* or *Deep Discovery Director on page 9-63*.

    > **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.

Chapter 5

Dashboard

Topics include:

Dashboard Overview

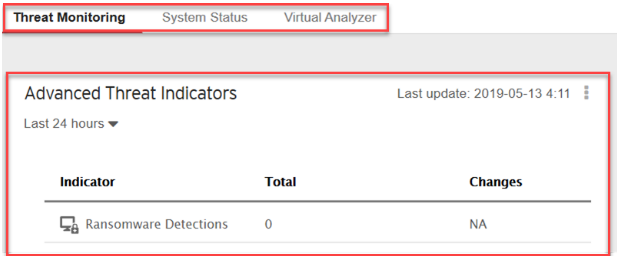
Monitor your network integrity with the dashboard. Each management console user account has an independent dashboard. Changes made to one user account dashboard do not affect other user account dashboards.

Some dashboard widgets allow you to view data that automatically updates over time. To provide continuity when viewing this data, there is no session timeout if you are accessing the dashboard widgets screen.

Tip

If you have security considerations, you can log off the web console manually.

The dashboard consists of the following user interface elements:

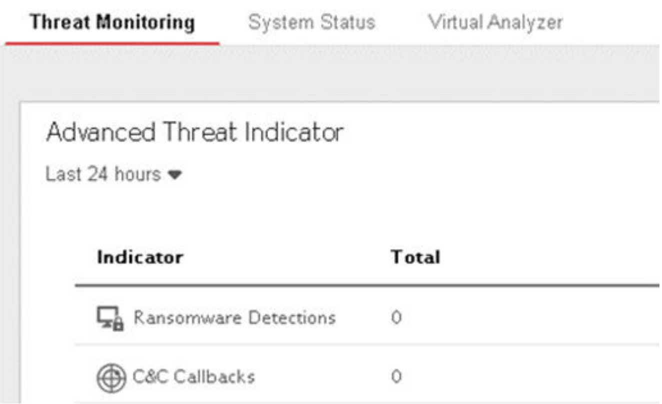


Indicator	Total	Changes
Ransomware Detections	0	NA

ELEMENT	DESCRIPTION
Tabs	Tabs provide a container for widgets. For details, see *Tabs on page 5-11*.
Widgets	Widgets represent the core dashboard components. For details, see *Widgets on page 5-13*.

Default Dashboard View

The default dashboard view comes with predefined tabs, each with a set of widgets. You can rename, delete, and add widgets to these tabs.



Advanced Threat Indicator

Last 24 hours ▾

Indicator	Total
Ransomware Detections	0
C&C Callbacks	0

The predefined tabs include:

- *Threat Monitoring Tab on page 5-3*
- *System Status Tab on page 5-7*
- *Virtual Analyzer Tab on page 5-10*

Threat Monitoring Tab

The **Threat Monitoring** tab is displayed on the dashboard by default.

You can view threat-monitoring widgets to understand what is threatening your network and the pattern of the threats over time.

The following threat-monitoring widgets are displayed by default:

- *Advanced Threat Indicators on page 5-4*

- *C&C Callback Detections Over Time on page 5-5*
- *Ransomware Detections Over Time on page 5-5*
- *Top Affected Users on page 5-6*
- *Top Detected URLs on page 5-7*
- *Virtual Analyzer Sandbox Analysis on page 5-7*

Advanced Threat Indicators Widget

The **Advanced Threat Indicators** widget displays the total advanced detections for each threat indicator type per selected time period and the change between the number of detections from the last period for each indicator.

- Click a number under the **Total** column to learn more about the detections for that indicator. Clicking a number opens the **All Detections** screen with the appropriate threat indicator filter set to see detections only for that indicator type.
- Threat indicators include:
    - **Ransomware Detections**

      All ransomware detections found by URL category or Scan Engine.
    - **C&C Callbacks**

      Detections found for C&C Callbacks by URL category or Scan Engine
    - **Suspicious URLs**

      Detections that are part of the Suspicious Object blacklist URLs detections.
    - **Suspicious Documents**

      High risk detections for Office and PDF documents.
    - **Suspicious Scripts**

      High risk detections for certain scripts including html/html application, javascript, java jar/class, vb, windows shell or script, .bat, or .svg files.

- **Suspicious Malware**

  High risk file detections that do not fall into the SO suspicious document or suspicious script indicators

- **Coin Miners**

  All coin miner detections found by URL category or Scan Engine.

C&C Callback Detections Over Time Widget

You can view the **C&C Callback Detections Over Time** widget to see the number of C&C callback detections over the selected time period.

- Deep Discovery Web Inspector uses the C&C URL category for detections.
- You can hover over a specific entry to see the C&C callbacks count for that time.
- If you click on an entry, the **All Detections** screen opens and displays results for the selected time with results filtered for the C&C callback threat indicator.

  You can view detailed information about each detection including the time, risk level, host, URL, threat name, and action for each detection.

- If you click **View all C&C callbacks**, the **Detections > All Detections** screen opens with the `C&C Callbacks` **Threat Indicator** filter applied.

  You can view detailed information about C&C callback detections in this screen.

Ransomware Detections Over Time Widget

You can view the **Ransomware Detections Over Time** widget to see the number of ransomware detections over the selected time period.

- Deep Discovery Web Inspector uses all available Trend Micro detections engines for ransomware detection.
- You can hover over a specific ransomware entry to see the ransomware count for that time.

- If you click on an entry, the **All Detections** screen opens and displays results for the selected time with results filtered for the ransomware threat indicator.

  You can view detailed information about each detection including the time, risk level, host, URL, threat name, and action for each detection.

- If you click **View all ransomware detections**, the **Detections > All Detections** screen opens with the `Ransomware` **Threat Indicator** filter applied.

  You can view detailed information about ransomware detections in this screen.

Top Affected Users Widget

You can view the **Top Affected Users** widget to see the users with the highest number of critical risks detected over the selected time period.

If you have configured the Deep Discovery Web Inspector appliance to use Active Directory Services and Deep Discovery Web Inspector can determine which Active Directory user is logged on to the host, the user name is displayed. If Deep Discovery Web Inspector cannot determine who the logged on user is, the IP address of the host is displayed instead.

- From the drop-down, you can adjust the top number of users to include in the graph: 5, 10, 15, or 20

- You can hover over a specific user entry to see the number of detections for that user.

- If you click on the user entry, the **All Detections** screen opens with results filtered for the selected user (IP address or logged on Active Directory user).

  From this page, you can view detailed information about detections for that user, including the risk level, domain, threat name, and action for each detection.

- If you click **View all users**, the **Detections > Users** screen opens where you can view detailed information for all users with detections during the selected time period.

Top Detected URLs Widget

You can view the **Top Detected URLs** widget to see the URLs with the highest number of critical risks detected over the selected time period.

Trend Micro Web Reputation Services is used to determine the URL risk level.

- You can adjust the top number of hosts to include in the graph: 5, 10, 15, or 20
- You can hover over a specific URL to see the entire URL path and the number of detections for that URL.
- If you click on the URL entry, the **All Detections** screen opens with results filtered for the selected URL where you can view detailed information about detections for that URL.
- If you click **View all URLs**, the **Detections > URLs** screen opens where you can view detailed information about all URLs detected during the selected time period.

Virtual Analyzer Sandbox Analysis Widget

You can view the **Virtual Analyzer Sandbox Analysis** widget to see how many objects were analyzed over a specified time period.

The widget displays the following information:

- The count and percentage of analyzed objects that were suspicious
- The count and percentage of analyzed objects that were non-suspicious
- The total number of objects analyzed

System Status Tab

The **System Status** tab is displayed on the dashboard by default.

You can view the system status widgets to monitor the Deep Discovery Web Inspector appliance hardware and the connection and throughput status.

The following system status widgets are displayed by default:

- *Hardware Status Widget on page 5-8*
- *Connection Status Widget on page 5-8*
- *Traffic Status Widget on page 5-9*
- *Bandwidth Status Widget on page 5-9*

Hardware Status Widget

The **Hardware Status** widget shows the Deep Discovery Web Inspector appliance's CPU, memory, and disk usage over the selected time period.

- The time periods you can select include **Realtime**, **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Status categories displayed include **Memory usage**, **Disk usage**, and **CPU usage**.
- You can hover over any point on the time line to see the system usage for each category for that time.
- Click an item in the widget legend (Memory usage, Disk usage, or CPU usage) to show or hide data related to that category.

Note

"Disk usage" refers to the amount of data stored on the disk partition `/var/app_data`.

Connection Status Widget

You can view the **Connection Status** widget to see the number of connections that Deep Discovery Web Inspector processed per protocol over the selected time period.

- The time periods you can select include **Realtime**, **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Protocol categories displayed include **Total**, **HTTP**, **HTTPS**, and **HTTP2**.
- You can hover over any point on the time line to see the number of connections by protocol for that time.

- Click an item in the widget legend (Total, HTTP, HTTPS, or HTTP2) to show or hide data related to that metric.

Traffic Status Widget

You can view the **Traffic Status** widget to see the amount of traffic (KB, MB, GB, or TB) that Deep Discovery Web Inspector processed per protocol over the selected time period.

- The time periods you can select include **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Traffic by protocol categories displayed include **Total**, **HTTP**, **HTTPS**, and **HTTP2**.
- You can hover over any point on the time line to see the amount of traffic processed by protocol for that time.
- Click an item in the widget legend (Total, HTTP, HTTPS, or HTTP2) to show or hide data related to that metric.

Bandwidth Status Widget

You can view the **Bandwidth Status** widget to see the total bps (Kbps, Mbps, Gbps, or Tbps) that Deep Discovery Web Inspector processed per protocol over the selected time period.

- The time periods you can select include **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Bandwidth (bps) by protocol categories displayed include **Total**, **HTTP**, **HTTPS**, and **HTTP2**.
- You can hover over any point on the time line to see the total bps by protocol for that time.
- Click an item in the widget legend (Total, HTTP, HTTPS, or HTTP2) to show or hide data related to that metric.

Virtual Analyzer Tab

The **Virtual Analyzer** tab is displayed on the dashboard by default.

View Virtual Analyzer widgets to assess performance based on analysis processing time, queue size, and the volume of suspicious objects discovered for a specified time period.

The following Virtual Analyzer status widgets are displayed by default:

- *Average Virtual Analyzer Processing Time on page 5-10*
- *Suspicious Objects from Virtual Analyzer on page 5-10*
- *Virtual Analyzer Queue on page 5-11*

Average Virtual Analyzer Processing Time Widget

The **Average Virtual Analyzer Processing Time** widget shows the average time in seconds between when Virtual Analyzer receives an object and completes analysis.

- The graph is based on the selected period. The Y-axis represents the average length of time required to analyze the object. The X-axis represents the period.
- Mouse-over a point on the graph to view the average processing time and the period.
- Click **Manage Virtual Analyzer** to reallocate instances, to add or remove images, or to make other changes to Virtual Analyzer settings.

Suspicious Objects from Virtual Analyzer Widget

The **Suspicious Objects from Virtual Analyzer** widget shows the suspicious objects found by Virtual Analyzer over the selected time period.

Suspicious objects are objects with the potential to expose systems to danger or loss. Virtual Analyzer detects and analyzes suspicious URLs, IP addresses, domains, and files.

- The graph is based on the selected time period. The Y-axis represents the number of suspicious object detected. The X-axis represents the time line.

- Mouse-over a point on the graph to view the number of high risk detections for each object type for that selected time.
- Click an item in the widget legend (URLs, IPs, Domains, or Files) to show or hide data related to that metric.
- If you click **View all suspicious objects**, the **Detections > Suspicious Objects** screen opens where you can view detailed information about all suspicious objects for the selected time period.

Virtual Analyzer Queue Widget

The **Virtual Analyzer Queue** widget shows all files queued for analysis in Virtual Analyzer for the specified time.

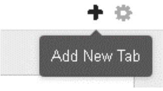
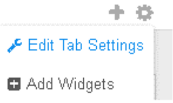
- The graph is based on the selected period. The Y-axis represents the file count. The X-axis represents the period.
- Mouse-over a point on the graph to view the number of queued files and the period.

Tabs

Tabs provide a container for widgets. Each tab on the dashboard can hold up to 20 widgets. The dashboard supports up to 30 tabs.

Tab Tasks

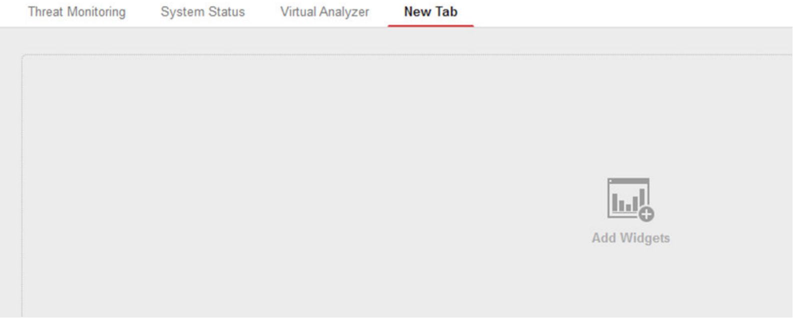
The following table lists the tab-related tasks:

Task	Steps
Add a tab	Click the plus icon (✚) on the top right of the dashboard. The **New Tab** window displays.  For information about this window, see *New Tab Window on page 5-12*.
Edit a tab's settings	Click the settings icon (⚙) on the top right of the dashboard. A window opens, where you can choose whether to edit tab settings or add widgets. 
Delete a tab	Click the **Delete** icon (☒) next to the tab title. Deleting a tab deletes all the widgets in the tab. This does not delete the widgets from the widget list in the **Add Widgets** screen.

New Tab Window

The **New Tab** window opens when you click the **Plus** icon (+) located at the top of the dashboard.

From the **New Tab** window, you can add new widgets.



Widgets

Widgets are the core components of the dashboard. Widgets contain charts and graphs that allow you to monitor the system status and track threats.

List of Widgets

You can add any of the following widgets to the dashboard:

- System Status widgets (4)
  - Connection Status*
  - Hardware Status*
  - Traffic Status*
  - Bandwidth Status*
- Threat Monitoring widgets (6)
  - Advanced Threat Indicators*
  - C&C Callback Detections Over Time*

  - Ransomware Detections over Time*
  - Top Affected Users*
  - Top Detected URLs*
  - Virtual Analyzer Sandbox Analysis*
- Virtual Analyzer widgets (3)
  - Average Virtual Analyzer Processing Time*
  - Suspicious Objects from Virtual Analyzer*
  - Virtual Analyzer Queue*

* denotes widgets displayed by default.

Adding New Widgets

You can add new widgets to tabs on the dashboard.

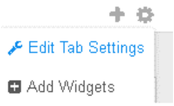
Procedure

1. Go to **Dashboard**.

2. Select the tab to which you want to add a widget.

3. Click the settings icon (⚙) in the upper-right corner of the tab selected on the dashboard.

   The **Settings** menu opens where the **Add Widgets** setting displays.



4. Select **Add Widgets** and then select one or more widgets from the widget list by selecting the check box next to the widget's title.

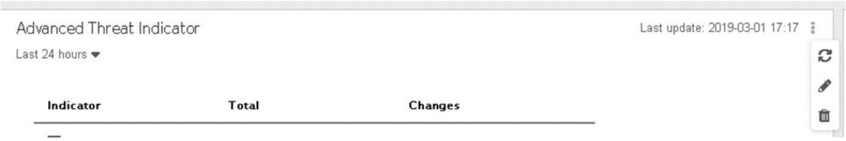
5. Click **Add**.

   After adding a widget, you can drag-and-drop the widget to various locations within the tab.

   Managing Widgets on page 5-15

Managing Widgets

All widgets follow a widget framework and offer similar task options.



Advanced Threat Indicator

Last 24 hours ▾

Last update: 2019-03-01 17:17

Indicator	Total	Changes
—		

Table 5-1. Widget Options Menu

Task	Steps
Access widget options	Click the widget settings icon (⋮) at the widget's top-right corner to view the menu options.
Edit a widget	Click the edit icon (✎) to change settings.
Refresh widget data	Click the refresh icon (⟳) to refresh widget data.
Delete a widget	Click the delete icon (🗑) to close the widget. This action removes the widget from the tab that contains it, but not from any other tabs that contain it or from the widget list in the **Add Widgets** screen.
Move a widget within the same tab	Use drag-and-drop to move the widget to a different location within the tab.
Change period	If available, click the **Period** drop-down menu to select the time period.

Chapter 6

Detections

Understanding Risk Levels

Deep Discovery Web Inspector assesses risk using multi-layered threat analysis and then assigns a risk level for each detection. Deep Discovery Web Inspector checks objects for known threats in the Trend Micro Smart Protection Network and other Trend Micro scanning engines, including the Advanced Threat Scanning Engine and Predictive Machine Learning.

If the object has unknown or suspicious characteristics, the detected object is sent to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious behavior to identify potential threats.

Deep Discovery Web Inspector assigns a risk level to the object based on the highest risk assigned between the Deep Discovery Web Inspector scanners and Virtual Analyzer.

For details about how Deep Discovery Web Inspector investigates objects, see *A New Solution on page 1-10*.

Detection Risk Levels

The following table explains the detected risk levels after investigation. View the table to understand why detected objects are classified as high, medium, low, or user-defined risk.

TABLE 6-1. Risk Definitions

RISK LEVEL	DESCRIPTION
High	High-risk detections have with malicious characteristics. A high-risk object contains: • Files with unknown threats detected as high risk by Virtual Analyzer Filter • Objects detected as high risk based on analysis by Trend Micro multi-layered threat detection

RISK LEVEL	DESCRIPTION
Medium	Medium-risk detections have characteristics that are most likely malicious. A medium-risk object contains: • Known malware • Known dangerous links • Objects detected as medium risk by Virtual Analyzer Filter
Low	Low-risk detections have suspicious characteristics. A low-risk object contains: • Known highly suspicious or suspicious links • Links detected as low risk by Virtual Analyzer • Files detected as low risk by Virtual Analyzer • URLs detected as low risk based on suspicious URL matching
Potential Threat	Potential Threat risk detections are recorded for samples submitted to the Virtual Analyzer sandbox. A Potential Threat risk object contains: • Suspicious detection results by Advanced Threat Scan Engine • Suspicious detection results by Script Analyzer Engine • Predictive Machine Learning Engine supported files and Community File Reputation query results that match the threshold • File types that must be submitted to the Virtual Analyzer sandbox
User Defined	An object that is blocked/receives warning under the following scenarios: • Untrusted server certificate • User-defined policy

Virtual Analyzer Risk Levels

The following table explains the Virtual Analyzer risk levels after object analysis. View the table to understand why a suspicious object was classified as high, medium, or low risk.

Risk Level	Description
High	The object exhibited highly suspicious characteristics that are commonly associated with malware. Examples: • Malware signatures; known exploit code • Disabling of security software agents • Connection to malicious network destinations • Self-replication; infection of other files • Dropping or downloading of executable files by documents
Medium	The sample exhibited moderately suspicious characteristics that are also associated with benign applications.
Low	The object exhibited mildly suspicious characteristics that are most likely benign.

Threat Indicator and Detected By Classifications

Understanding what the threat indicators are and what type of Trend Micro detection technology detected each threat can be useful in understanding how to interpret detection data.

Threat Indicator Classifications

The following table explains the threat indicators detected during scanning or analysis. View the table to understand the malicious activity affecting your network.

TABLE 6-2. Threat Indicator Classifications

THREAT INDICATOR	CLASSIFICATION
Ransomware	Malware that limits user access to a system either by locking the user out of the system or encrypts the user's files unless a ransom is paid.
Coin Miners	Malware used by attackers for cryptocurrency mining.
C&C Callbacks	Communication with Command and Control (C&C) servers, which are used to remotely send commands to, download malicious content to, or exfiltrate data from infected clients.
Suspicious Malware	Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems. Detections are included in this category if they are not included in the Suspicious Documents or Suspicious Scripts indicator categories.
Suspicious URLs	A domain or URL that links to an unknown malicious website.
Suspicious Documents	High risk detections for Office and PDF documents.
Suspicious Scripts	High risk detections for script files that exhibits malicious characteristics. Script files include HTML, HTML application, JavaScript, Java jar/class, VB, Windows shell/script, BAT, and SVG files. **Important** Always handle suspicious files with caution.

Detected By Classifications

The following table explains the categories that you can select in the **Detected by** advanced filter field. View the table to understand how objects are detected.

TABLE 6-3. Detected By Advanced Filter List

DETECTED BY	DESCRIPTION
All	Objects detected by all detection sources.
Untrusted Server Certificate	The secure URL or domain has an untrusted SSL server certificate.
Blocked List	Domain, URL, of File (SHA1) accessed is listed in the blocked list.
Temporary Blocked URLs	URL is blocked by Deep Discovery Web Inspector cache because the same violation is detected again within four hours.
Web Reputation Services	Web Reputation Services is a part of the Trend Micro Smart Protection Network and scrutinizes URLs before users access potentially dangerous websites.
URL Filtering	URL accessed was included in a policy. When a user requests a URL, Deep Discovery Web Inspector looks up the category for that URL and then blocks the access to the dangerous URL category, such as the category for “Ransomware” or “C&C Callback”.
True File Type	True file type accessed was included the file types section of a policy. Including file types in the policy can trigger a detection based on certain defined true file types (archives, executables, Office documents, PDF files, and scripts).
Anti-Malware (Advanced Threat Scan Engine)	Malware detected by the Advanced Threat Scan Engine.
Anti-Malware (Static Intelligence Engine)	Malware detected by the Static Intelligence Engine. Static signature-based detection involves searching for known patterns of data within executable code or behavior analysis.
Anti-Malware (Script Analyzer Lineup)	Malware detected by the Script Analyzer Lineup.
Predictive Machine Learning	Malware detected by Predictive Machine Learning.
Anti-Botnet	Monitoring and analyzing network traffic to help identify bot activity so it can be blocked or eradicated.

DETECTED BY	DESCRIPTION
Suspicious Objects Analysis (Virtual Analyzer)	Suspicious object detected through Virtual Analyzer. Virtual Analyzer can analyze IP address, domain, URL, and file objects.
Suspicious Objects Filtering (Virtual Analyzer)	Violations detected by Virtual Analyzer reported IP addresses, domains, URLs, and files objects.

Viewing Detections

You can query and view detections to:

- Better understand the threats affecting your network and their relative risk
- Discover trends and learn about related detections
- See how Deep Discovery Web Inspector handled the detected object

Related information

- ➥ *Viewing All Detections*
- ➥ *Viewing Detections for Users*
- ➥ *Viewing Detections for URLs*
- ➥ *Viewing Detections for Files*
- ➥ *Investigating Details About a Detection*

Viewing All Detections

All detections are the cumulative detections for URLs, users, and files that contain malicious or suspicious content. Deep Discovery Web Inspector assigns a risk rating to each detection based on the investigation results.

By viewing all detections, you can gain intelligence about the context of suspicious detections by investigating a wide array of information facets. You can investigate attacks trending on your network by correlating common characteristics. Based on the detections, you can change your policy configuration and warn your users to take preventive measures against similar attacks.

You can narrow your results by applying basic and advanced search filters.

Procedure

1. Go to **Detections** > **All Detections**.

2. Specify the search criteria.

   See the following for details:

   - *Applying Basic Filters on page 6-9*
   - *Creating and Editing Advanced Search Filters on page 6-10*
   - *List of Advanced Search Filters on page 6-12*
   - *Applying a Saved Advanced Search Filter on page 6-14*

3. Review the detection results.

   For each detection, Deep Discovery Web Inspector displays the following information:

Header	Description
Time	View the date and time that the malicious or suspicious object was detected in Deep Discovery Web Inspector.
Risk Level	View the risk level assigned to the selected object.
User Name	View the user name logged on to the host with detections of malicious or suspicious objects. **Note** When Active Directory Services are configured and Deep Discovery Web Inspector can identify the logged on user for the detection, the user name is displayed. Otherwise the IP address of the host is displayed.

Header	Description
Domain	View the name of the domain where Deep Discovery Web Inspector detected the malicious or suspicious object.
Threat Name	View the threat name of the discovered object. You can click on the threat name to learn more information about that threat.
Action	View the final result after scanning and analyzing the malicious or suspicious object. The result is the executed policy action. For samples submitted to the Virtual Analyzer for analysis and patient-zero is enabled, the action is “Analyzing”.

4. Click the expansion icon (▸) beside a detection to view detailed results.

   Detection Details on page 6-16

Related information

↳ *Threat Indicator and Detected By Classifications*
↳ *Understanding Risk Levels*

Applying Basic Filters

When viewing all detections, you can use basic filters to narrow the results.

Procedure

1. Go to **Detections** > **All Detections**.

2. Specify the information to filter.

   The following table explains the basic search filters for querying detections.

> **Note**
>
> Search filters do not accept wildcards. Deep Discovery Web Inspector uses fuzzy logic to match search criteria to detection data.

FILTER	DESCRIPTION
Risk level	Select **All**, **High and Medium**, **High**, **Medium**, **Low**, **Potential Threat**, or **User Defined**. The default risk level is **High and Medium**. For details about risk levels, see *Understanding Risk Levels on page 6-2*.
Action	Select **All**, **Monitor**, **Block**, **Warning**, or **Analyzing**.
User Name	Search for a specific user name by specifying a user name or the logged on user's host IP address. To display results filtered by **User Name**, click on the Search (🔍) icon or press **Enter** to filter the results. **Note** Your search parameter might be the logged on user if Active Directory services are configured or it might be the client IP address. This is because the user is displayed if Deep Discovery Web Inspector can identify the logged on user for the detection. Otherwise the IP address is displayed for User Name.
Period	Select a predefined time range or specify a custom range. If specifying a custom range, specify a starting and ending time for the range.

When applying **Risk level**, **Action**, and **Period** basic filters, Deep Discovery Web Inspector dynamically displays the filtered results.

All detections matching the search criteria appear.

3. Click on **Clear all** before starting a new filter search.

Creating and Editing Advanced Search Filters

You can choose and apply an existing saved search filter or you can create a new search filter. If you choose an existing search filter, you can edit it before applying it.

Note

If you want to apply a saved advanced search filter without editing it before applying it, see *Applying a Saved Advanced Search Filter on page 6-14*.

Procedure

1. Go to **Detections** > **All Detections**, and then click **Advanced**.

   The **Advanced** search pane opens.

2. Perform the appropriate action:

   a. To create a new advanced search filter, begin adding search criteria as described in the following steps.

   b. To edit an existing advanced search filter, use the **New search** drop down in this pane to choose an existing saved search filter.

   The criteria for the saved search is displayed in the advanced search pane. You can edit or remove existing criteria and add new criteria to the saved search.

3. To add a search criteria, select a filter and a filter operator from the filter drop-down menu.

   For example, you can select the **URL** filter and then select either the **Contains** or **Does Not Contain** filter operator.

   To see the list of filters that you can add, along with supported filter operators, see *List of Advanced Search Filters on page 6-12*.

4. Do one of the following:

   - Click on **New Value** and type a value in the text box and then click **Enter** (for **Domain**, **URL**, **Server IP**, **File SHA1**, and **Policy name** filters).

   - Click on the drop-down box and choose an action from the menu (for **Detected by** and **Threat indicator** filters).

   Note

   You can add multiple entries for each criteria. You can remove an entry by clicking on the "x" box for that entry.

5. (Optional) Click the plus icon (+) to include other criteria sets in the search filter.

6. (Optional) Click on the delete icon (🗑) beside a search criteria to remove it from the current search filter.

7. Click **Apply**.

   The **All Detections** screen updates and displays data filtered by the search criteria.

8. To save the search, do one of the following:

   a. To save a new search, click on **Save as**, then type a search name and description and click **Save**.

      The new saved search is added to the list of saved searches.

   b. To save an existing search that you have modified, click **Save**.

9. Select basic search criteria (Risk level, Action, User Name, or Period) that you would like to additionally apply to the current search results.

   Basic search criteria are not saved to advanced search filters, but can be added to the current search results.

10. (Optional) Clear the current search by clicking on **Clear all**.

    Applied basic and advanced search filters are cleared from the current results. Results from the default basic filters display.

11. (Optional) Delete a saved search by selecting the search in the **New search** drop down and click on the delete icon (🗑).

12. (Optional) Click the close icon (›) beside the saved searches drop-down list to close the advanced search feature.

List of Advanced Search Filters

Use the following advanced search filter criteria to create and apply customized searches.

To view specific data, select from the following optional attributes and operators, and type an associated value.

TABLE 6-4. Search Criteria: All Detections

ATTRIBUTE	OPERATOR	ACTION
Domain	**Contains/Does Not Contain**	Type a value
URL	**Contains/Does Not Contain**	Type a value
Server IP	**Contains/Does Not Contain/In Range/Not in Range**	Type a value
File SHA1	**Contains/Does Not Contain**	Type a value
Policy name	**Contains/Does Not Contain**	Type a value
Detected by	**Is**	Select **All** or one or more of the following: • **Untrusted Server Certificate** • **Blocked List** • **Temporary Blocked URLs** • **Web Reputation Service** • **URL Filtering** • **True File Type** • **Anti-Malware (Advanced Threat Scan Engine)** • **Anti-Malware (Static Intelligence Engine)** • **Anti-Malware (Script Analyzer Lineup)** • **Predictive Machine Learning** • **Anti-Botnet** • **Suspicious Objects Analysis (Virtual Analyzer)**

Attribute	Operator	Action
		• **Suspicious Objects Filtering (Virtual Analyzer)**
Threat indicator	**Is**	Select **All** or one or more of the following: • **Ransomware** • **C&C Callbacks** • **Suspicious Domains/URLs** • **Suspicious Documents** • **Suspicious Scripts** • **Suspicious Malware** • **Coin Miners**

Applying a Saved Advanced Search Filter

You can apply an existing saved search filter.

Procedure

1. To apply a saved advanced search filter, go to **Detections** > **All Detections**, and then click on the **Advanced Search** menu icon (☰)located to the right of **Advanced**.

   The list of saved searches displays.

2. Select the saved search that you want to apply.

   The detections list displays the results filtered by the saved search.

What to do next

To edit the saved advanced search filter, see *Creating and Editing Advanced Search Filters on page 6-10*

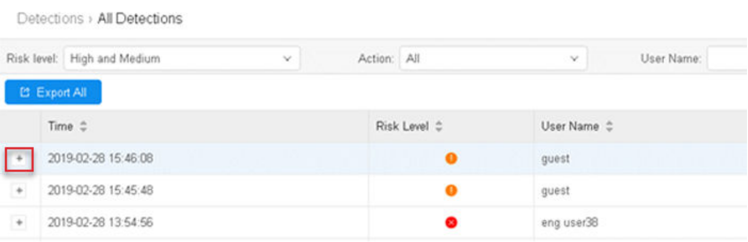
Investigating Details About a Detection

Procedure

1. Search for the detection.

   See *Viewing All Detections on page 6-7*.

2. Click the plus sign next to the detection in the table.



Detections › All Detections

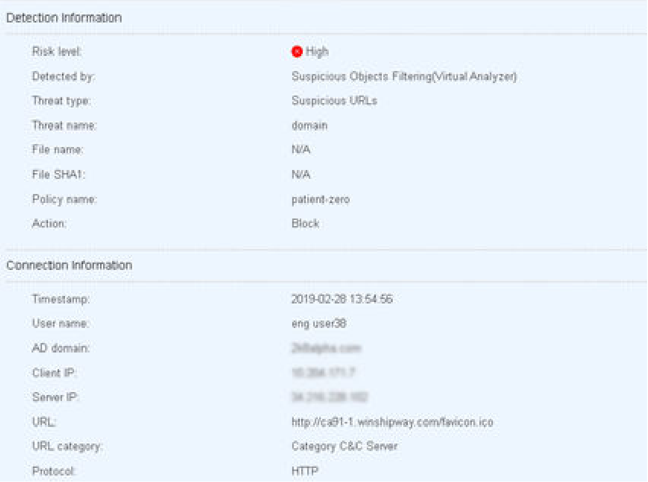
Risk level: High and Medium

Action: All

User Name:

	Time	Risk Level	User Name
+	2019-02-28 15:46:08	●	guest
+	2019-02-28 15:45:48	●	guest
+	2019-02-28 13:54:56	●	eng user38

The table row expands to display detailed information.



Detection Information

Risk level:	● High
Detected by:	Suspicious Objects Filtering(Virtual Analyzer)
Threat type:	Suspicious URLs
Threat name:	domain
File name:	N/A
File SHA1:	N/A
Policy name:	patient-zero
Action:	Block

Connection Information

Timestamp:	2019-02-28 13:54:56
User name:	eng user38
AD domain:	[redacted]
Client IP:	[redacted]
Server IP:	[redacted]
URL:	http://ca91-1.winshipway.com/favicon.ico
URL category:	Category C&C Server
Protocol:	HTTP

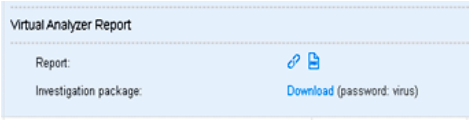
3. Examine the detection details.

   See *Detection Details on page 6-16*.

4. (Optional) If a threat name is displayed in the **Threat name** field, click on the threat name to open the ThreatConnect page where you can view detailed information about that threat.

5. (Optional) If the value displayed in the **Detected by** field is **Suspicious Objects Analysis (Virtual Analyzer)** or **Suspicious Objects Filter (Virtual Analyzer)**, you can display or download the Virtual Analyzer report and download the Virtual Analyzer investigation package for a specified detection.

   a. Go to the **Virtual Analyzer Report** section at the bottom of the details page.



Virtual Analyzer Report

Report:	🔗 🗎
Investigation package:	Download (password: virus)

   b. Open the Virtual Analyzer report in HTML or PDF format.

   c. Download the Virtual Analyzer investigation package.

Detection Details

The following table explains the detection details viewable after expanding a detection entry. Detection details are divided into three sections: **Detection Information**, **Connection Information**, and **Virtual Analyzer Report**. The **Virtual Analyzer Report** section displays only if there are Virtual Analyzer reports for that detection. The contents of each display field varies depending on the type of detected threat.

Detection Information

Field	Description
Risk level	High, Medium, Low, or User Defined. See *Detection Risk Levels on page 6-2*.

FIELD	DESCRIPTION
Detected by	See *Detected By Classifications on page 6-5*.
Threat type	See *Threat Indicator Classifications on page 6-4*.
Threat name	Click the listed threat name to get correlated information about suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network, which provides relevant and actionable intelligence.
File name	The name of the file, if any, for the detection.
File SHA1	The file SHA1, if any, for the detection.
Policy name	The name of the policy applied to the detection.
Action	Monitor or Block.

Connection Information

FIELD	DESCRIPTION
Timestamp	The latest detection time.
User name	The user name or IP address (if Active Directory Services is not enabled).
Active Directory domain	Active Directory domain information
Client IP	The source for the object.
Server IP	The destination for the object.
URL	The URL of the detected object.
URL category	The URL category of the detected object.
Protocol	The network protocol used for the detected object.

Virtual Analyzer Report

The reports and investigation package summarize the sandbox analysis overview and detailed threat characteristics. The Virtual Analyzer reports are available for the detection types "Suspicious Objects Analysis (Virtual Analyzer)" and "Suspicious Objects Filter (Virtual Analyzer)".

Note

If the detection log can be associated with an existing Virtual Analyzer report, the section “Virtual Analyzer Report” is shown. If a report does not exist for the selected detection, the section is hidden.

FIELD	DESCRIPTION
Report	Provides links to download the Virtual Analyzer HTML and PDF report.
Investigation package	Provides the link to download the raw investigation package. The decompress password is 'virus'.

Viewing Detections for Users

Detected users are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.

Procedure

1. Go to **Detections** > **Users**.

2. Optionally, filter the result set by specifying search criteria.

   - **User Name**

   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a user name, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.

3. View the results.

Header	Description
User Name	View the user name logged on to the host with detections of malicious or suspicious objects. **Note** When Active Directory Services are configured and Deep Discovery Web Inspector can identify the logged on user for the detection, the user name is displayed. Otherwise the IP address of the host is displayed.
Detections	View the number of detections with malicious or suspicious characteristics for the selected object.
High Risk	View the number of high risk detections for the selected object. These are detections with malicious characteristics.
Medium Risk	View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.
Low Risk	View the number of low risk detections for the selected object. These are detections with suspicious characteristics.
Potential Threat	View the number of potential threat risk detections for the selected object. These are detections for sample submission to Virtual Analyzer.
User Defined Risk	View the number of detections for user-defined objects. These detections might include the following: “Untrusted Server Certificate” or user-defined policy.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.

4. Under **Detections**, click on the number to view more detailed information about detections for that user name.

   The **All Detections** screen opens with the results filtered for that user name.

See *Viewing All Detections on page 6-7*.

What to do next

After viewing user detections, you can export the results by clicking on **Export All**.

Viewing Detections for URLs

Detected URLs are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.

Procedure

1. Go to **Detections** > **URLs**.
2. Optionally, filter the result set by specifying search criteria.
   - **URL**
   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a URL, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.
3. View the results.

HEADER	DESCRIPTION
URL	View the URLs where Deep Discovery Web Inspector detected malicious or suspicious objects.
Detections	View the number of detections with malicious or suspicious characteristics for the selected object.

Header	Description
High Risk	View the number of high risk detections for the selected object. These are detections with malicious characteristics.
Medium Risk	View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.
Low Risk	View the number of low risk detections for the selected object. These are detections with suspicious characteristics.
Potential Threat	View the number of potential threat risk detections for the selected object. These are detections for sample submission to Virtual Analyzer.
User Defined Risk	View the number of detections for user-defined objects. These detections might include the following: “Untrusted Server Certificate” or user-defined policy.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.

4. Under **Detections**, click on the number to view more detailed information about detections for that URL.

   The **All Detections** screen opens with the results filtered for that URL.

   See *Viewing All Detections on page 6-7*.

What to do next

After viewing URL detections, you can export the results by clicking on **Export All**.

Viewing Detections for Files

Detected files are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.

Procedure

1. Go to **Detections** > **Files**.
2. Optionally, filter the result set by specifying search criteria.

   - **File SHA1**
   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a file SHA1, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.

3. View the results.

Header	Description
File SHA1	View the file SHA1s that Deep Discovery Web Inspector detected as malicious or suspicious objects.
Threat Name	View the threat name of the discovered suspicious file.
Detections	View the number of detections with malicious or suspicious characteristics for the selected object.
High Risk	View the number of high risk detections for the selected object. These are detections with malicious characteristics.
Medium Risk	View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.
Low Risk	View the number of low risk detections for the selected object. These are detections with suspicious characteristics.
Potential Threat	View the number of potential threat risk detections for the selected object. These are detections for sample submission to Virtual Analyzer.

Header	Description
User Defined Risk	View the number of detections for user-defined objects. These detections might include the following: “Untrusted Server Certificate” or user-defined policy.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.

4. Under **Detections**, click on the number to view more detailed information about detections for that file.

   The **All Detections** screen opens with the results filtered for that file SHA1.

   See *Viewing All Detections on page 6-7*.

What to do next

After viewing file detections, you can export the results by clicking on **Export All**.

Viewing Suspicious Objects

Suspicious objects are objects that Virtual Analyzer analysis determined have the potential to expose systems to danger or loss.

Query suspicious objects to:

- Better understand the threats affecting your network and their relative risk
- Assess the prevalence of suspicious IP addresses, domains, URLs, and files
- Find infected endpoints in your network
- Proactively contain or block infections

Related information

- ⤷ *Viewing Suspicious IP Address Objects*
- ⤷ *Viewing Suspicious Domain Objects*

- *Viewing Suspicious URLs*
- *Viewing Suspicious File Objects*
- *Viewing Synchronized Suspicious Objects*

Viewing Suspicious IP Address Objects

A suspicious IP address has the potential to expose systems to danger or loss.

View suspicious IP addresses to understand your risk and assess the relative prevalence of the suspicious IP address. Find out detailed information about the detections found for a specific IP address.

Procedure

1. Go to **Detections** > **Suspicious Objects** > **IP Addresses**.

2. Specify the search criteria.

   - **IP Address**

   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying an IP address, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.

3. View the results.

HEADER	DESCRIPTION
Suspicious Object	View the IP address used by the suspicious object.
Port	View the port number used by the suspicious object.
Risk Level	View the level of potential danger in an suspicious object.

Header	Description
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.
Detections	View the number of detections with malicious or suspicious characteristics for the selected suspicious IP address.

Viewing Suspicious Domain Objects

A suspicious domain has the potential to expose systems to danger or loss.

View suspicious domains to understand your risk and assess the relative prevalence of the suspicious domain. Find out detailed information about the detections found for a specific domain.

Procedure

1. Go to **Detections** > **Suspicious Objects** > **Domains**.
2. Specify the search criteria.
   - **Domain**
   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a domain, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.
3. View the results.

Header	Description
Suspicious Object	View the domain name used by the suspicious object.

Header	Description
Risk Level	View the level of potential danger in an suspicious object.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.
Detections	View the number of detections with malicious or suspicious characteristics for the selected suspicious domain.

Viewing Suspicious URLs

A suspicious URL has the potential to expose systems to danger or loss.

View suspicious URLs to understand your risk and assess the relative prevalence of the suspicious URL. Find out detailed information about the detections found for a specific URL.

Procedure

1. Go to **Detections** > **Suspicious Objects** > **URLs**.

2. Specify the search criteria.

    - **URL**

    - **Period**

    When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

    When specifying a URL, click on the Search (🔍) icon or press **Enter** to filter the results.

    All detections matching the search criteria appear.

3. View the results.

Header	Description
Suspicious Object	View the web address of the suspicious object.
Risk Level	View the level of potential danger in an suspicious object.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.
Detections	View the number of detections with malicious or suspicious characteristics for the selected suspicious URL.

Viewing Suspicious File Objects

.A suspicious file has the potential to expose systems to danger or loss.

View suspicious file SHA1s to understand your risk and assess the relative prevalence of the suspicious file. Find out detailed information about the detections found for a specific file SHA1.

Procedure

1. **Detections** > **Suspicious Objects** > **Files**.

2. Specify the search criteria.

   - **File SHA1**
   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a file SHA1, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.

3. View the results.

Header	Description
Suspicious Object	View the SHA1 value that uniquely identifies a file.
Risk Level	View the level of potential danger in an suspicious object.
Latest Detection	View the date and time for the most recent occurrence of the malicious or suspicious object detected in Deep Discovery Web Inspector.
Detections	View the number of detections with malicious or suspicious characteristics for the selected suspicious file SHA1.

Viewing Synchronized Suspicious Objects

Deep Discovery Web Inspector can synchronize suspicious objects with an external source (either Apex Central or Deep Discovery Director). View synchronized suspicious objects to understand your risk and assess the relative prevalence of the suspicious object.

Note

You can use only one of Apex Central or Deep Discovery Director as a source for synchronized suspicious objects with Deep Discovery Web Inspector at any given time. You cannot register Deep Discovery Web Inspector with both products at the same time. If Deep Discovery Web Inspector is already registered with one of the two sources, you cannot register with the other source until you unregister the currently registered product.

Procedure

1. Go to **Detections** > **Suspicious Objects** > **Synchronized Suspicious Objects**.
2. Filter the suspicious object results.
   a. Specify the search criteria by suspicious object type or time period.
      - **Type** (All, File, IP Address, URLs, or Domains)
      - **Period** (Last 4 hours, Last 24 hours, Last 7 days, Last 30 days, Last 90 days, Custom range)

The chosen period represents the last synchronization time.

When specifying a type or period, Deep Discovery Web Inspector dynamically filters the results.

b. Filter the results by entering the search criteria in the search box (IP address, domain, URL, or file SHA-1) and then press ENTER.

All detections matching the search criteria appear.

3. View the results.

Header	Description
Suspicious Object	View the IP address, domain, URL, or file SHA-1 associated with the synchronized suspicious object.
Type	View the suspicious object type (File, IP address, URL, or Domain).
Risk Level	View the level of potential danger in an suspicious object.
Source	View the source of the synchronized suspicious object. The source can be one of the following: • Apex Central • Deep Discovery Director
User Defined	View whether the synchronized suspicious object is user-defined or not.
Expiration	View the date and time the object is not considered suspicious.
Last Synchronized	View the date and time the entry was last synchronized with the source.

What to do next

You can add synchronized suspicious objects to the Blocked/Approved Lists. See *Adding Synchronized Suspicious Objects to the Approved/Blocked Lists on page 6-30*.

Adding Synchronized Suspicious Objects to the Approved/ Blocked Lists

You can add objects from the **Synchronized Suspicious Objects** detection page to the Blocked List or Approved List.

Procedure

1. Go to **Detections** > **Suspicious Objects** > **Synchronized Suspicious Objects**.
2. Select one or more suspicious objects from the list.
3. Do one of the following:
   - Click **Add to Approved List**.
   - Click **Add to Blocked List**.

   The **Add to Approved List** or **Add to Blocked List** screen opens, depending on which button you clicked.
4. Enter a description in **Comment**.
5. Click **Add**.

What to do next

To view and manage the suspicious objects that you add to the Approved/Blocked Lists, go to **Policy** > **User Defined Settings** > **Approved/Blocked Lists**.

Chapter 7

Policy

Topics include:

Policy Overview

Deep Discovery Web Inspector integrates with a variety of powerful Trend Micro security filtering engines and technologies to scan web traffic coming in and out of your organization. Policy-related functionality allows you to control what happens to web traffic going through the Deep Discovery Web Inspector appliance.

Policies

You can create one or more policies to take action on specific network and user and group events reported by Deep Discovery Web Inspector. Policies are compared against incoming traffic in sequence, with the first policy that matches the traffic being applied. This provides flexibility while helping protect your network from advanced persistent threats and emerging unknown threats according to the configured policies.

You can configure risk-level actions for each policy that determines what happens for detections at each risk level. Possible actions are scan, allow, and block.

Control whether scans are performed on iOS and Android mobile device traffic by enabling or disabling scanning bypass for these device types.

HTTPS Inspection

You can manage HTTP Inspection by performing the following:

- Configure HTTPS decryption rules that define which objects, users and groups, and URL categories Deep Discovery Web Inspector should decrypt for scanning. HTTPS traffic is encrypted, and must be decrypted before Deep Discovery Web Inspector can scan the traffic.
- Manage digital certificates in Trusted, Untrusted, Invalid certificates stores and manage the exception list.
- Manage HTTPS tunnels, which allow the tunneling of HTTPS traffic without decryption.
- Manage fingerprint patterns used by Intelligent Decryption to determine whether traffic should be decrypted or not decrypted based on the fingerprint signature of the browser.

User Defined Settings

You can do the following with user defined settings:

- Create and customize network and domain objects that you use in policies and HTTPS inspection rules.
- Configure approved and blocked lists to control which domains, IP addresses, URLs, or file (SHA1)s are allowed or blocked without needing to scan them.
- Manage notifications that are sent to users when a violation occurs while they are requesting network resources.

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.

Information About How Policies Work

Each policy can be as general or specific as needed. Policies are compared against incoming traffic in sequence, and because the first policy that matches the traffic is applied, the more specific policies must precede the more general ones. For example, a policy for a single IP address must come before a rule for a network range that includes the single IP address if all other traffic-related settings are the same.

Policies define what actions to take if there is a traffic match: allow the traffic while bypassing scanning, block the traffic, or scan the traffic and perform the appropriate action configured for each risk level.

Note

Under certain circumstances, for example if the file size is large or the network is slow, Deep Discovery Web Inspector triggers a deferred scan where part of the file is passed to the requesting client while Deep Discovery Web Inspector scans the remainder of the file. If a deferred scan is triggered, no notification will be displayed in client side. If Deep Discovery Web Inspector determines the file is malicious after the scan finishes, a notification page is not displayed on the client; however, the client only receives part of file data. Deep Discovery Web Inspector will not send the last chunk of received data to the client's browser. This results in an incomplete file on the client that is unusable and cannot be opened.

- Policies contain specified policy parameters that are composed of traffic sources, domain objects, and selected file types.
- The traffic source parameter includes four options that you can select: any, network objects, users and groups, and guest users.
    - Network objects are configured under user-defined settings, and can be created ahead of time or at the time of policy creation.

- To select users and groups, you must configure Microsoft Active Directory Services ahead of time.

  See *Active Directory Services on page 9-44*.

- Domain objects are configured under user-defined settings, and can be created ahead of time or at the time of policy creation.
- The file types are predefined and include archives, executables, Office documents, PDF files, and script files.

How Patient Zero Protection Works

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

When 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.

By enabling Patient Zero Protection, you ensure that malicious objects are not passed through to the destination while waiting for sandbox analysis to complete. This provides a higher level of protection against malware intrusions and attacks.

- Deep Discovery Web Inspector takes no action and delivers the object to the endpoint if it is marked as “No risk”.
- 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.

  The default risk-level actions for a policy are to block high-risk and medium-risk objects and monitor low-risk objects.

- If Virtual Analyzer did not finish the sandbox analysis or even start the analysis during the allotted time, Deep Discovery Web Inspector allows the object to pass through to the destination.

  If Deep Discovery Web Inspector encounters the object that did not finish or even start analysis again, the object is not sent to Virtual Analyzer for sandbox analysis; Deep Discovery Web Inspector allows the object to pass through.

Note

If Patient Zero Protection is disabled, suspicious objects are not held while analysis is ongoing. The suspicious objects are passed straight through.

The Default Policy

The **default** policy is a predefined default policy and is always the last one in the policy list.

The only operation that you can perform on the **default** policy is to enable or disable it.

You cannot do the following to the **default** policy:

- Select it or move it up or down in the policy rule list
- Delete the **default** policy
- Change the policy name or description
- Change the policy settings such as which traffic sources, domain objects, and file types are scanned
- Change the policy action and risk-level scan actions
- Enable or disable **Patient-Zero**

Viewing Policies

Procedure

1. Go to **Policy** > **Policy**.
2. View summary information about existing policies including:
   - The name of the policy.
   - The traffic source, domain objects, and file types included in the policy.

The traffic source can be one of the following: **Any**, **Selected network objects**, **Selected users and groups**, or **Guest users**.

- The action for each policy (**Scan**, **Allow**, or **Block**).
- If the policy action is **Scan**, the action to take (**Block** or **Monitor**) for each risk level (**Low**, **Medium**, and **High**) when a scanned object matches the policy.
- Whether **Patient-Zero** is enabled or disabled (only applicable if the action is **Scan**).
- The **default** policy is predefined and is always the last one in the policy list.

3. Click on the name of a policy to view more details about that policy.

Related information

↳ *The Default 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 7-48*.

- **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 7-10*.

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 7-49*.

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.

Configuring iOS/Android Device Bypass

You can configure whether iOS and Android mobile devices are screened for network threats by enabling or disabling bypass scanning of traffic for these device types.

Procedure

1. Go to **Policy** > **Policy**.
2. Click **Configure Device Bypass Settings**.

   The **Global Device Bypass Settings** screen opens.
3. To bypass scanning of iOS devices, enable **Bypass iOS traffic**.
4. To bypass scanning of Android devices, enable **Bypass Android traffic**.
5. Click **Save**.

   The device bypass settings are applied to all policies.

Managing HTTPS Inspection

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols widely adopted and deployed in network communication today. The traffic over SSL/TLS is encrypted and signed using digital certificates to ensure security.

Digital certificates are electronic documents that are used to create secure connections between clients and servers or websites. A valid and trusted certificate ensures clients that they are connecting to a trusted server or website, and helps protect against man-in-the-middle attacks. Certificates become trusted by going through a validation process of a Certificate Authority (CA). Certificate Authorities themselves are usually third-party companies that are trusted by both the client and server or website.

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.

Manage HTTPS Inspection by performing any of the following tasks:

Procedure

- HTTPS Inspection Rules: Configure HTTPS Inspection rules and optionally import a certificate that is used when resigning decrypted traffic.

  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.

  Managing HTTPS Decryption Rules on page 7-13

- Digital Certificates: Maintain the lists of trusted, untrusted, and invalid digital certificates and configure digital certificate exceptions.

  Managing Digital Certificates on page 7-21

- Auto-tunneling: Maintain a list of trusted domains or URLs used by Deep Discovery Web Inspector to determine which traffic to auto-tunnel.

  Auto-tunneled traffic will not be subject to decryption.

  You can also maintain the auto-tunnel exception list, which means that when decryption failed the domain is not added into the auto-tunnel list. If it is already in the tunnel list, the tunnel list has higher priority than the tunnel exception list.

  The auto-tunnel exception has a precondition that the traffic from the client must first match the HTTPS decryption rule policy. And for traffic that matches a decryption rule but something wrong happened during the decryption, Deep Discovery Web Inspector would not tunneled the traffic.

  And for the situation where the domain has not been added into the tunnel exception list and something wrong happens during the decryption, the traffic might be auto-tunneled by Deep Discovery Web Inspector to ensure continuity. This is used for the following scenario: A customer has a higher security requirement for specific domain and traffic from that domain must be decrypted even if it will block the normal network behavior.

  Managing HTTPS Domain Tunnels on page 7-39

- Intelligent Decryption: Manage fingerprint patterns to customize which application traffic will be auto-tunneled.

Managing Intelligent Decryption on page 7-43

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 *Managing HTTPS Domain Tunnels on page 7-39* for 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, Deep Discovery Web Inspector will skip checking what application the client is using, which can impact some applications and affect business continuity. Trend Micro recommends enabling Intelligent Decryption for HTTPS decryption policies.

See *Managing Intelligent Decryption on page 7-43* for 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 7-48*.

    - **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 7-49*.

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.

Managing Digital Certificates

You can manage the trusted, untrusted, and inactive CA digital certificate lists.

You can also configure endpoint certificate exceptions, which allows you to specify what action to take (Allow, Block, or Warn) for endpoint HTTPS access to websites.

See *Information About Digital Certificates on page 7-22*.

Go to **Policy** > **Digital Certificates** to perform any of the following tasks to manage HTTPS digital certificates.

Procedure

- Click on the **CA Certificates** tab and manage:
  - **Trusted CA Certificates**:

    Managing Trusted CA Certificates on page 7-23
  - **Untrusted CA Certificates**:

    Managing Untrusted CA Certificates on page 7-25
  - **Inactive CA Certificates**:

    Managing Inactive CA Certificates on page 7-27
- Click on the **Exceptions** tab and manage exceptions:

  Managing Certificate Exceptions on page 7-29
- Install the digital certificate on clients:

  Installing the Deep Discovery Web Inspector CA on Clients on page 7-31

Information About Digital Certificates

For Deep Discovery Web Inspector to determine if a server's signature is trusted, the root Certification Authority (CA) certificate on which the signature is based must be added to the Deep Discovery Web Inspector certificate store.

There are three types of digital certificates that are involved in producing a digital signature:

- The "end" or "signing" certificate, which contains the public key to be used to validate the actual digital signature.
- One or more "intermediate" Certification Authority (CA) certificates, which contain the public keys to validate the signing certificate or another intermediate certificate in the chain.
- The "root" CA certificate, which contains the public key used to validate the first intermediate CA certificate in the chain (or, rarely, the signing certificate directly). An otherwise valid signature is "trusted" by Deep Discovery Web Inspector if the CA certificate of the signature is known to Deep Discovery Web Inspector and is active.

If Deep Discovery Web Inspector encounters an unknown CA certificate during SSL handshake processing, it automatically saves the certificate in the **Inactive CA Certificates** list. Intermediate and root CA certificates are collected in this way. If required later, a CA certificate collected in this way can be "activated" (made trusted or untrusted by Deep Discovery Web Inspector so that the signatures of websites depending on it can be processed as valid or invalid.

Accessing secure resources that traverse through a Deep Discovery Web Inspector appliance with an untrusted or expired certificate displays a security warning in the web browser.

Managing Trusted CA Certificates

Procedure

1. Go to **Policy** > **Digital Certificates** > **CA Certificates**.
2. Select **Trusted CA Certificates** from the drop-down list.
3. Manage trusted CA certificates:

   Note

   This tab only collects and displays root and intermediate CA certificates.

Task	Details
View existing CA certificates	a. View the CA certificate information: • **Common Name**: CommonName (CN) field in the CA certificate. • **Type**: Type of the CA certificate, which is **Root** or **Intermediate**. • **Valid to**: Date and time after which the CA certificate becomes invalid. • **Expired Status**: Whether the CA certificate is expired or not. ⚠ indicates that the certificate expired and serves as a reminder to the administrator to take action on it. b. Click a CommonName under **Common Name** to view the certificate details.
Add a CA certificate	Add CA certificates to the to the **Trusted CA Certificates** list: a. Click **Add**. b. On the **Add Trusted CA Certificate** screen that appears, click **Select File** and select a certificate to upload. **Note** Deep Discovery Web Inspector supports uploading CA certificates in .pem or .p7b format. c. Click **Add**. **Note** If Deep Discovery Web Inspector encounters an unknown CA certificate, it automatically saves it in the **Inactive CA Certificates** list.

TASK	DETAILS
Move a CA certificate	• To move a trusted CA certificate to the **Untrusted CA Certificates** list, select it and click **Move to Untrusted**. This CA certificate is still kept in the Deep Discovery Web Inspector certificate store, but Deep Discovery Web Inspector does not trust certificates that use it in their certification path. • To move a trusted CA certificate to the **Inactive CA Certificates** list, select it and click **Move to Inactive**.
Delete a CA certificate	To delete a CA certificate, select it and click **Delete**.
Search for a CA certificate	Type a CommonName or part of the CommonName in the **Search** text box. **Note** If there are many entries in the table, you can type some characters of the CommonName in the **Search** text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed immediately.

Managing Untrusted CA Certificates

Procedure

1. Go to **Policy** > **Digital Certificates** > **CA Certificates**.

2. Select **Untrusted CA Certificates** from the drop-down list.

3. Manage untrusted digital certificates:

Note

This tab only collects and displays root and intermediate CA certificates.

Task	Details
View existing CA certificates	a. View the CA certificate information: • **Common Name**: CommonName (CN) field in the CA certificate. • **Type**: Type of the CA certificate, which is **Root** or **Intermediate**. • **Valid to**: Date and time after which the CA certificate becomes invalid. • **Expired Status**: Whether the CA certificate is expired or not. ⚠ indicates that the certificate expired and serves as a reminder to the administrator to take action on it. b. Click a CommonName under **Common Name** to view the certificate details.
Add a CA certificate	Add CA certificates to the to the **Untrusted CA Certificates** list: a. Click **Add**. b. On the **Add Untrusted CA Certificate** screen that appears, click **Select File** and select a certificate to upload. **Note** Deep Discovery Web Inspector supports uploading CA certificates in .pem or .p7b format. c. Click **Add**. **Note** If Deep Discovery Web Inspector encounters an unknown CA certificate, it automatically saves it in the **Inactive CA Certificates** list.

Task	Details
Move a CA certificate	• To move an untrusted CA certificate to the **Trusted CA Certificates** list, select it and click **Move to Trusted**. Certificates that use this CA certificate in their certification path are trusted. • To move an untrusted CA certificate to the **Inactive CA Certificates** list, select it and click **Move to Inactive**.
Delete a CA certificate	To delete a CA certificate, select it and click **Delete**.
Search for a CA certificate	Type a CommonName or part of the CommonName in the **Search** text box. **Note** If there are many entries in the table, you can type some characters of the CommonName in the **Search** text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed immediately.

Managing Inactive CA Certificates

Procedure

1. Go to **Policy** > **Digital Certificates** > **CA Certificates**.
2. Select **Inactive CA Certificates** from the drop-down list.
3. Manage inactive digital certificates:

Note

This tab only collects and displays root and intermediate CA certificates.

Task	Details
View existing CA certificates	a. View the CA certificate information: • **Common Name**: CommonName (CN) field in the CA certificate. • **Type**: Type of the CA certificate, which is **Root** or **Intermediate**. • **Valid to**: Date and time after which the CA certificate becomes invalid. • **Expired Status**: Whether the CA certificate is expired or not. ⚠ indicates that the certificate expired and serves as a reminder to the administrator to take action on it. b. Click a CommonName under **Common Name** to view the certificate details.
Add a CA certificate	Add CA certificates to the to the **Inactive CA Certificates** list: a. Click **Add**. b. On the **Add Inactive CA Certificate** screen that appears, click **Select File** and select a certificate to upload. **Note** Deep Discovery Web Inspector supports uploading CA certificates in .pem or .p7b format. c. Click **Add**. **Note** If Deep Discovery Web Inspector encounters an unknown CA certificate, it automatically saves it in the **Inactive CA Certificates** list.

TASK	DETAILS
Move a CA certificate	• To move an inactive CA certificate to the **Trusted CA Certificates** list, select it and click **Move to Trusted**. Certificates that use this CA certificate in their certification path are trusted. • To move an inactive CA certificate to the **Untrusted CA Certificates** list, select it and click **Move to Untrusted**.
Delete a CA certificate	To delete a CA certificate, select it and click **Delete**.
Search for a CA certificate	Type a CommonName or part of the CommonName in the **Search** text box. **Note** If there are many entries in the table, you can type some characters of the CommonName in the **Search** text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed immediately.

Managing Certificate Exceptions

The list of digital certificate exceptions displays the end certificates that fail to pass the certificate validation test and the certificates that the administrator needs to set special actions according to the organization's information security policies.

When users attempts to access a website whose certificate does not pass the certificate validation test for the first time, Deep Discovery Web Inspector automatically adds the certificate to the exceptions list and displays a page warning the user about the invalid or unknown certificate. By default, the **Action** is set to **Warn** and can be changed as necessary. Deep Discovery Web Inspector will process subsequent attempts to websites using this certificate according to the update.

You can also manually add a certificate exception.

Procedure

1. Go to **Policy** > **Digital Certificates** > **Exceptions**.
2. Manage certificate exceptions:

Task	Details
Add/Edit a certificate exception	See *Adding/Editing Certificate Exceptions on page 7-30*.
View existing certificate exceptions	The **Common Name**, **Description**, **Type**, and **Action** fields automatically populate with the related data after a certificate exception is added. • **Type**: There are two types of the certificate exception ◦ **cn**: Added from the Deep Discovery Web Inspector web console ◦ **cert**: Automatically added by Deep Discovery Web Inspector • **Action**: Action to take on access to the websites using the certificate in their certification path (Allow, Warning, Block).
Delete a certificate exception	Select one or several certificate exceptions to delete and then click **Delete**.

Adding/Editing Certificate Exceptions

You can manually add or edit a certificate exception.

Procedure

1. Go to **Policy** > **Digital Certificates** > **Exceptions**.
2. Perform the appropriate action:

   Add an exception:

a. Click **Add** to add a new exception.

The **Add Certificate Exception** screen opens.

b. Configure the following:

- **Common name**: CommonName (CN) field in the certificate.
- **Action**: Action to take on access to websites using the certificate in their certification path. Options include **Allow**, **Warn**, and **Block**.
- **Description**: (Optional) Meaningful description to easily identify the certificate exception.

Edit an existing exception:

a. Select an existing certificate exception under **Common Name** to edit an exception.

The **Edit Certificate Exception** screen opens.

b. Under **Action**, select which action to take on access to websites using the certificate in their certification path.

Options include **Allow**, **Warn**, and **Block**.

3. Click **Save**.

Installing the Deep Discovery Web Inspector CA on Clients

Deep Discovery Web Inspector can decrypt HTTPS traffic and enforce security policies to the content. To do so, Deep Discovery Web Inspector uses its own CA certificate to resign a server certificate and to secure the traffic to client.

By default, the Deep Discovery Web Inspector CA certificate is not trusted by clients, which might result in clients receiving **Untrusted Issuer** warnings. You can use the following procedures to deploy the Deep Discovery Web Inspector CA certificate to clients to avoid the warnings.

- *Installing the CA Using Active Directory GPOs on page 7-32*
  - *Downloading the Default CA Certificate on page 7-32*
  - *Deploy the Default CA Using Group Policy Objects (GPOs) on page 7-33*
  - *Deploy the Default CA on Firefox Using Group Policy Objects (GPOs) on page 7-34*
- *Deploy a Subordinate CA Based On An Organization's Root CA on page 7-36*

Installing the CA Using Active Directory GPOs

As a network administrator of an Active Directory network environment, you can automatically install the Deep Discovery Web Inspector root CA in all of your users' browsers by creating a Group Policy Object (GPO) on your Active Directory server.

Procedure

1. Download the Deep Discovery Web Inspector default CA certificate.

Downloading the Default CA Certificate on page 7-32

2. Perform the appropriate procedure:

a. Deploy the Deep Discovery Web Inspector default CA to clients using group policy.

To *Deploy the Default CA Using Group Policy Objects (GPOs) on page 7-33*

b. Deploy the Deep Discovery Web Inspector default CA on Firefox using group policy.

Deploy the Default CA on Firefox Using Group Policy Objects (GPOs) on page 7-34

Downloading the Default CA Certificate

Before you can automatically install the Deep Discovery Web Inspector default root CA certificate in all of your users' browsers, you must download it from the Trend Micro web site.

Procedure

1. Download the Deep Discovery Web Inspector default CA certificate and save it to an internally accessible location.

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

Deploy the Default CA Using Group Policy Objects (GPOs)

If there is Active Directory network, you can create a Group Policy Object (GPO) on the Active Directory server to deploy the Deep Discovery Web Inspector default CA certificate automatically.

Procedure

1. Log in to an Active Directory server using an administrator account.

2. Select **Start** > **All Programs** > **Administrative Tools** > **Group Policy Management**.

3. In the left pane, right-click the domain name, and select **Create and Link a GPO Here** from the context menu and then input the GPO name.

   For example, **ddwi-cert-deploy**.

4. In the right pane, right-click the GPO created in the previous step (example: **ddwi-cert-deploy**) and select **Edit**.

5. In the left panel, expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Root Certification Authorities**, then right-click in the right panel and select **Import**.

   The **Import Wizard** screen opens.

6. In the **Import Wizard** screen, click **Browse** and navigate to the location where the Deep Discovery Web Inspector CA certificate was downloaded.

7. Use the default option **Place all certificates in the following store (Trusted Root Certification Authorities**”, and finish the wizard.

> **Note**
>
> The GPO might not take effect immediately on all client machines. By default, GPO synchronization occurs every 90 to 120 minutes. You can run the **`gpupdate`** command on client machines to force synchronization. You can run the **`gpresult`** command to check the deployment status.

Deploy the Default CA on Firefox Using Group Policy Objects (GPOs)

By default, Active Directory GPO deployment of certificates does not work for Firefox users, because Firefox uses its own certificate stores. Starting with Firefox version 49, a new option allows Firefox to trust root authorities in the Windows Certificate Store. However, the option is disabled by default. You must enable it before Firefox can trust root authorities in the Windows Certificate Store.

Procedure

1. Create files that will mandate that Firefox use the Windows Certificate Store so that Deep Discovery Web Inspector certificates can be deployed for Firefox using GPOs.

    a. Create a configuration file `ddwi.cfg`.

       The `ddwi.cfg`' file must be placed in the root of the Firefox directory.

       `C:\Program Files\Mozilla Firefox\ddwi.cfg`

    b. Add the following to the `ddwi.cfg` file.

```
   //
lockPref("security.enterprise_roots.enabled", true);
```

Note

Note: The files must be ANSI encoded. Don’t miss the “//” at the first line.

c. Place

d. Create the file `local-settings.js`.

The `local-settings.js` file must be placed in the `\defaults\pref` sub-directory.

`C:\Program Files\Mozilla Firefox\defaults\pref\local-settings.js`

e. Add the following to the `local-settings.js` file.

```
pref("general.config.obscure_value", 0);
 pref("general.config.filename", "ddwi.cfg");
```

2. Distribute the Firefox preference files using a Group Policy Object.

Note

This process requires that Firefox be installed to the default location on the client computers.

a. Add the files `ddwi.cfg` and `local-settings.js` to a network share. Ensure that the share has read permissions for 'Domain Computers'.

b. Create/Edit a group policy using the Active Directory **Group Policy Management** console.

c. Edit the settings in **Computer Configuration** > **Preferences** > **Windows Settings** > **Files**.

d. Right-click and select **New File**.

e. For **Source File**, select `ddwi.cfg` on the Network Share.

f. Point the **Destination** file to be `C:\Program Files\Mozilla Firefox\ddwi.cfg` and then click **Apply**.

g. Repeat the above step to copy the same file to `C:\Program Files (x86)\Mozilla Firefox\ddwi.cfg`.

h. Repeat these steps to copy '`local-settings.js`' to `C:\Program Files\Mozilla Firefox\defaults\pref\local-settings.js`.

i. Repeat these steps to copy `local-settings.js` to `C:\Program Files (x86)\Mozilla Firefox\defaults\pref\local-settings.js`.

3. Force Firefox to use the Windows Certificate Store by manually enabling the feature on the Firefox clients.

a. In Firefox, type **about:config** in the address bar.

b. If prompted, accept any warnings.

c. Search “security.enterprise_roots.enabled” and set the value to **true**.

Deploy a Subordinate CA Based On An Organization's Root CA

Deep Discovery Web Inspector allows administrators to generate and then download a CSR (Certificate Sign Request) using the Deep Discovery Web Inspector management console. You can use the downloaded CSR to request a subordinate certificate from the Microsoft Active Directory Certificate Server. You can then use the subordinate certificate on Deep Discovery Web Inspector for HTTPS decryption by uploading and applying the subordinate certificate using the Deep Discovery Web Inspector management console.

Procedure

1. Generate the CSR from the Deep Discovery Web Inspector management console.

a. In a web browser, type the IP address of the Deep Discovery Web Inspector management console.

```
https://<management_IP_address>
```

b. Go to **Policy** > **HTTPS Inspection**.

c. Click **Generate CSR** to generate the CSR file.

The **Generate CSR** window opens.

d. 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.

e. Click **Generate CSR**.

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

2. 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.

3. Generate the subordinate certificate from the Microsoft Active Directory Certificate Server.

   The procedure below shows you how to generate a Subordinate Certificate based on Windows Active Directory Certificate Server. You must be an Administrator and sign in to the domain using the format **domain\user**. If you do not sign in using **domain\user**, you will not see the **Submit an advanced certificate request** option on the second page of the requesting a certificate process.

   a. Go to the Microsoft Active Directory Certificate Server main page.

      The URL might look like `http://IP_address/certsrv` with `IP_address` being dependent on your environment.

      The **Welcome** screen opens.

   b. Under **Select a task**, select **Request a Certificate**.

      The **Request a Certificate** screen opens.

   c. Select **Advanced certificate request**.

      The **Submit a Certificate Request or Renewal Request** screen opens.

   d. Paste the content of the CSR file generated in the last section into the **Saved Request** text box.

   e. Under **Certificate Template**, choose **Subordinate Certification Authority**, and then click **Submit**.

      The **Certificate Issued** screen opens.

   f. Select **DER encoded**, then click **Download certificate**.

      While downloading the file, rename the certificate to `subca.cer` for further use.

4. From the Deep Discovery Web Inspector management console, import the new certificate and private key and enable HTTPS decryption.

   a. Under **Certificate**, click **Browse** and import the `subca.cer` generated in last step.

b. Under **Private Key**, click **Browse** and choose the private key `subca.key` generated in last section, then import the private key.

c. Input and confirm the private key password.

d. Click **Verify Certificate**.

The **Save** button will get focus if the verification is OK.

e. Click **Save**.

The `subca.cer` takes effect for this policy after the service restarts.

5. For clients where certificates cannot be deployed using Active Directory GPOs, install the certificate on the clients using the procedures provided by the client or operating system vendor.

Managing HTTPS Domain Tunnels

HTTPS domain tunnels allow administrators to maintain a list of trusted domains or URLs, whose HTTPS traffic are not subject to applicable HTTPS decryption rules and are not decrypted and inspected by Deep Discovery Web Inspector. You can also configure an exception list of specific pages, links, or sub-domains that will not be tunneled within the trusted domains and are subject to the configured HTTPS inspection and policy rules. For more, see *Overview of HTTPS Domain Tunnels on page 7-40*.

Important

HTTPS domain tunnels and tunnel exceptions are applicable only for HTTPS decryption rules that have auto tunneling enabled.

Go to **Policy** > **HTTPS Tunnels** to manage HTTPS domain tunnels:

Procedure

- View information about entries in the tunneled domain list and the exception list.

  Viewing HTTPS Domain Tunnels and Exceptions on page 7-41

- Add entries to the tunnel domain list or the exception list.

  Adding HTTPS Tunnels on page 7-42

- Remove entries from the tunnel domain list of the exception list.

Overview of HTTPS Domain Tunnels

Before Deep Discovery Web Inspector can apply scanning and filtering policies on encrypted content, you must configure HTTPS decryption rules to decrypt the content. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules are applied.

Deep Discovery Web Inspector uses HTTPS domain tunnels to except certain HTTPS traffic from decryption.

Domain tunnels records consist of a domain and a fingerprint pattern. HTTPS traffic matching both the fingerprint pattern and the domain in an existing tunnel record should be tunneled before matching the HTTPS decryption rules.

Note

If a domain tunnel record does not specify any fingerprint patterns, all traffic for that domain is tunneled.

There are two types of HTTPS domain tunnels:

- Tunnels added by the administrator

  In some cases, administrators might determine that there is no need to decrypt certain HTTPS traffic. HTTPS tunnels allow administrators to maintain a list of trusted domains or URLs, whose HTTPS traffic are not subject to HTTPS decryption rules and policies, and are always accessible by end users without being decrypted and inspected by Deep Discovery Web Inspector.

  Deep Discovery Web Inspector also provides an exception list to let administrators add specific pages, links, or sub-domains they do not want to tunnel within the trusted domains. Subsequent inspection of the matched URLs in the exception list are subject to the configured HTTPS inspection and policy rules.

- Auto tunnels added by Deep Discovery Web Inspector

  Deep Discovery Web Inspector automatically adds tunnels in response to certain HTTPS error codes along with the corresponding traffic's fingerprint pattern belonging to the defined browsers.

  After tunneling the traffic, the corresponding fingerprint pattern and the domain of the traffic is added as a record to the domain tunnel list with a 24 hour expiration date. This allows time for the administrator to remedy issues that are causing the HTTPS errors because the errors might otherwise prevent decryption from taking place. Because this might result in affected HTTPS traffic being blocked, administrators have 24 hours to correct issues before any HTTPS traffic is blocked because of the listed errors.

  Administrators can remove these domain tunnels before the 24 hour expiration if they wish to immediately block HTTPS traffic that has not been scanned.

Viewing HTTPS Domain Tunnels and Exceptions

Procedure

1. Go to **Policy** > **HTTPS Tunnels**
2. View summary information about entries in the HTTPS domain tunnel list and the exceptions list:

   - Domain Name.
   - Pattern Name

     The pattern name is defined in the Intelligent Decryption screen. A pattern consists of the fingerprint pattern for a browser/operating system. If there is no entry for Pattern Name, all traffic for the domain is tunneled.
   - Type

     - Tunnel: An administrator added the entry into the domain tunnel list or the exception list.

  - Auto tunnel: Deep Discovery Web Inspector automatically added the entry into the domain tunnel list in response to certain HTTPS error codes.

- Created At

  The time when the entry was added.

- Expire Time.

  - Manually added entries never expire.
  - Auto tunnel entries expire 24 hours after Created At time.

Adding HTTPS Tunnels

You can add HTTPS tunnels to the Tunneled Domain List or to the Exceptions list.

The Tunneled Domain List contains a list of trusted domains or URLs, whose HTTPS traffic are not subject to applicable HTTPS decryption rules and are not decrypted and inspected by Deep Discovery Web Inspector.

The exception list contains specific pages, links, or sub-domains that will not be tunneled within the trusted domains and are subject to the configured HTTPS inspection and policy rules.

All the matched URLs in the exception list are subject to the configured Deep Discovery Web Inspector policy rules for subsequent inspection.

Procedure

1. Go to **Policy** > **HTTPS Tunnels**.
2. Enter the domain name for which traffic should be auto tunneled or excepted from tunneling in **Domains**.

   Deep Discovery Web Inspector automatically adds an asterisk (*) at the beginning and end of the domain.
3. If you want to limit the domain tunnel or exception to those from the Intelligent Decryption pattern list or a sub-list of the pattern list, select either **Use Intelligent**

Decryption for common browsers or use the drop-down to select the list of browsers patterns using intelligent decryption.

4. Click **Add to Tunneled Domains List** or **Add to Exceptions List** as desired.

   The domains are added in the **Tunneled Domains List** or **Exceptions List**, together with the date and time when each domain was added.

   Note

5. To remove one or several domains from a list, select them and click **Remove**.

Managing Intelligent Decryption

Intelligent Decryption is designed to bypass HTTPS decryption for application-based HTTPS traffic. You can use Intelligent Decryption settings within an HTTPS decryption rule to better manage decryption of application traffic over specific browsers.

Important

You must enable Intelligent Decryption in the decryption rule for which you want Intelligent Decryption functionality to apply.

Deep Discovery Web Inspector includes a list of built-in intelligent decryption patterns that correspond to a combination of common browsers and operating systems. By default, traffic from all built-in patterns are decrypted. You can change the status for any pattern from "Decrypt" to "Do Not Decrypt" or you can rename the pattern.

You can detect and add custom patterns to the Defined Patterns list or delete custom patterns when they are no longer needed.

Note

For traffic that matches an HTTPS decryption rule with Intelligent Decryption enabled: All the patterns with status **Decrypt** are decrypted and subject to the configured Deep Discovery Web Inspector policy rules for subsequent inspection. All patterns with status **Do Not Decrypt** are not decrypted.

The **Intelligent Decryption** screen is divided into two sections:

- **Detect and Add Pattern**: Where you can detect and add custom patterns to the defined intelligent decryption pattern list
- **Defined Patterns**: Contains the list of built-in decryption patterns provided by Deep Discovery Web Inspector and custom patterns added by an administrator

Go to **Policy** > **Intelligent Decryption** to perform the following:

Procedure

- Detect a custom pattern and add a custom pattern to the **Defined Patterns** list.

  Adding a Custom Pattern for Intelligent Decryption on page 7-44
- View the **Defined Patterns** list.
- Configure what action to take for traffic that matches a selected pattern: **Decrypt** or **Do Not Decrypt**.

  The default is **Decrypt**.
- Select a pattern and edit the pattern name.
- Select a custom pattern and click **Delete** if the pattern is no longer needed.

  You cannot delete built-in patterns.

Adding a Custom Pattern for Intelligent Decryption

Intelligent decryption is designed to bypass HTTPS decryption for application-based HTTPS traffic. You can add custom intelligent decryption pattens to better manage decryption of application traffic over browsers that are not included in the built-in Defined pattern list.

Procedure

1. Go to **Policy** > **Intelligent Decryption**.

2. Enable the custom pattern detection by clicking on **Enable**.

   Enabling custom pattern detection allows Deep Discovery Web Inspector to detect the pattern generated from the following step.

3. Copy the URL displayed in **URL used to for browser pattern check** (https://localhost.localdomain/check_browser.html) to the client's browser for which you want to detect and add the custom pattern and then hit **Enter**.

   The Deep Discovery Web Inspector **Supported Browser** page open and displays information about the browser including the **Signature** (example: 17e5f659107133474090194f5e4e6713), which is used to generate the custom pattern.

   This information is also recorded as an entry in the **Detect and Add Pattern** list on the **Intelligent Decryption** screen. You can now add the entry to the **Defined Patterns** list.

   Note

   If the resultant pattern is already in the **Defined Patterns** list, it is not displayed in the **Detect and Add Pattern** list.

   It is possible that a pattern is a duplicate even if the browser or version number differs from the one listed in the **Defined Patterns** list. It is also possible that the **Defined Patterns** list contains multiple patterns for the same browser and version number.

4. In the **Detect and Add Pattern** list, find the new custom pattern entry and then click on **Add Pattern Name** under the **Action** column.

   The **Add Pattern Name** screen opens.

5. Enter a **Pattern name**, and then click **Add**.

   The pattern is added to the **Defined Patterns** list. By default, the status is set to **Decrypt**.

   Note

   All the patterns with status **Decrypt** are decrypted and subject to the configured Deep Discovery Web Inspector policy rules for subsequent inspection.

6. (Optional): If you do not want traffic from this pattern decrypted, select the pattern and then click on **Do Not Decrypt**.

What to do next

You can continue to add custom patterns to the **Defined Patterns** list by performing the procedure for each client/browser type and version for which you want to apply intelligent decryption.

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".
• 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 the Approved/Blocked Lists

Go to **Policy** > **User Defined Settings** > **Approved/Blocked Lists** to perform any of the following tasks to manage the approved and blocked lists.

Procedure

- View summary information about the approved and blocked lists.
- Configure and add entries to the approved and blocked lists.

> **Note**
>
> You can also add synchronized suspicious objects to the approved or blocked lists from the **Detections** > **Suspicious Objects** > **Synchronized Suspicious Objects** screen.

- Select an object in the approved or blocked list and then click **Delete** to remove the object.
- Click **Import/Export** to import or export a CSV file of the approved and blocked lists.

Approved/Blocked Lists

The approved and blocked lists allow traffic to override the defined policies, web reputation, and advanced threat protection settings.

If authentication is enabled, the approved and blocked lists are matched after authentication. The end user has already finished authentication before entries are matched in the approved and blocked lists.

Note

You cannot use the Approved List to bypass authentication. However, you can use a bypass policy (destination IP addresses) to bypass authentication.

By default, Deep Discovery Web Inspector automatically determines whether to add an input entry as a Server IP address match, a domain match, a URL match, or a File SHA1 object type.

Instead of using auto mode, you can use advanced options to manually specify the object type when adding the entry.

Match Entries

Keep the following in mind when adding entries to a list:

- The approved list takes precedence over the blocked list.
- An asterisk (*) denotes a wild card.
- You can add multiple entries to the approved or blocked list at the same time by using a delimiter between each entry.

  Valid delimiters are semicolon (;), comma (,), or linefeed (\r, \n, or \r\n).

Match Type	Description	Examples
Auto	You can let Deep Discovery Web Inspector automatically determine the object type when adding an entry to the approved and blocked lists. **Domain** and **URL** • Deep Discovery Web Inspector matches the traffic if the site `domain+port+path` string matches the input keyword. • Input entries are protocol insensitive.	• `www.test.com` matches sites "*www.test.com*" and "*www.test.com.cn". • `www.t*est.com` matches sites "www.ttest.com", "www.test.com", and "a.www.ttest.com.b". • `www.test.com/path1` matches site " a.www.test.com/path1/path2".

MATCH TYPE	DESCRIPTION	EXAMPLES
	Deep Discovery Web Inspector automatically removes the protocol from the input string. - You can use wild cards for intermediate position matches. - If the input entry does not contain a wild card, Deep Discovery Web Inspector matches the entire domain with a wild card at the start and end. - The domain part of the input string is case-insensitive; however, the path part of a URL is case sensitive. **Server IP address** - You can input an IP address entry as a single entry or delimited list of IP addresses, Class InterDomain Routing (CIDR) networks, or IP address ranges. **File (SHA1)** - Deep Discovery Web Inspector adds the SHA1 string as a File (SHA1) type.	- 192.168.1.1, 10.0.1.100/24,10.0.0.1-10.0.0.100 - `058f2491a3e13ce2078b7b5e3e62c59dc518ecbb`
Server IP address	You can input an IP address entry as a single entry or delimited list of IP addresses, Class InterDomain Routing (CIDR) networks, or IP address ranges.	- 192.168.1.2 - 192.168.1.1, 10.0.1.100/24,10.0.0.1-10.0.0.100
Domain	- A match is found if the site domain for the traffic matches the input domain name. - If the input entry does not contain a wild card, Deep Discovery Web Inspector matches the entire domain only. - Traffic matches are protocol sensitive if the input record contains the protocol.	- `www.test.com` matches the domain site “www.test.com” only. - `https://www.test.com` matches the domain site “https://www.test.com” but not “http://www.test.com”.

Match Type	Description	Examples
	If the input entry does not contain the protocol, traffic matches include both HTTP and HTTPS traffic. • Wild cards can be used to do prefix, intermediate, or suffix position matches. • An IP address is a valid entry for a domain match. • The domain input string is case-insensitive.	• `*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”.
URL	• Deep Discovery Web Inspector matches the traffic if the URL's `site domain+port+path+query` parameter matches the input URL. • If the input entry does not contain a wild card, Deep Discovery Web Inspector matches the entire URL only. • 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. • Wild cards can be used to do prefix, intermediate, or suffix position matches. • The domain part of the input string is case-insensitive. .	• `www.test.com/t` matches the URL “www.test.com/t” only. The entry does not match the URLs “www.test.com.cn/test” or “www.test.com/test”. • `https://www.test.com/t` matches the URL “https://www.test.com/t” only but not “http://www.test.com/t”. • `www.test.com*` matches the URLs “www.test.com/”, “www.test.com/test”, and “www.test.com.cn/test”

MATCH TYPE	DESCRIPTION	EXAMPLES
		- `www.test.com` matches the URL "www.test.com" only. "www.test.com.cn/test" and "www.test.com/test" are not matches. - `*www.test.com` matches "server.www.test.com".
File (SHA1)	- Deep Discovery Web Inspector adds the SHA1 string as a File (SHA1) type.	`058f2491a3e13ce2078b7b5e3e62c59dc518ecbb`

Adding to the Approved/Blocked Lists

You can define Server IP address, domain, URL, or file (SHA1) matches to add to the approved or blocked lists.

Note

You can also add synchronized suspicious objects to the approved or blocked lists from the **Detections** > **Suspicious Objects** > **Synchronized Suspicious Objects** screen.

By default, Deep Discovery Web Inspector automatically determines whether to add an input entry as a Server IP address match, a domain match, a URL match, or a file (SHA1) match. Instead of using auto mode, you can use advanced options to manually specify the object type when adding the entry.

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

For information about and examples for configuring entries, see *Approved/Blocked Lists on page 7-51*.

Procedure

1. Go to **Policy** > **User Defined Settings** > **Approved/Blocked Lists**.

   By default, **Object type** is set to **Auto**.

2. Enter Server IP address, domain, URL, or file (SHA1) entries in the **Input** text box.

3. Do one of the following:

   - Click **Add to Approved**.
   - Click **Add to Blocked**.

4. (Optional): To manually enter an object type, click on **Advanced** and in **Object type**, perform the appropriate action:

   - Click on **Server IP address** to configure an entry using the Server IP address match mode.
   - Click on **Domain** to configure an entry using the domain match mode.
   - Click on **URL** to configure an entry using the URL match mode.
   - Click on **File (SHA1)** to configure an entry using the File (SHA1) match mode.

5. If you added entries using the **Advanced** option, do one of the following:

   - Click **Add to Approved**.
   - Click **Add to Blocked**.

6. Click **Save**.

Managing Notifications

Notifications are sent to end-users when a violation occurs while they are requesting network resources.

Note

Under certain circumstances, for example if the file size is large or the network is slow, Deep Discovery Web Inspector triggers a deferred scan where part of the file is passed to the requesting client while Deep Discovery Web Inspector scans the remainder of the file. If a deferred scan is triggered, no notification will be displayed in client side. If Deep Discovery Web Inspector determines the file is malicious after the scan finishes, a notification page is not displayed on the client; however, the client only receives part of file data. Deep Discovery Web Inspector will not send the last chunk of received data to the client's browser. This results in an incomplete file on the client that is unusable and cannot be opened.

List of User Notifications on page 7-57

Go to **Policy** > **User Defined Settings** > **Notifications** to perform any of the following tasks to manage notifications.

Procedure

- View summary information about predefined notification templates.
- Click a notification name to view or modify the notification text or formatting.
- Click a notification name and then click **Reset** to reset the notification back to its predefined template.

  Note

  You cannot delete a predefined notification template or create any new templates.

List of User Notifications

Notification	Reason Notification Sent
Website Blocked: Advanced Threat Protection notification	When traffic was blocked because Deep Discovery Web Inspector detected an advanced threat on the page being accessed.

Notification	Reason Notification Sent
Blocked List notification	When traffic was blocked by the **Blocked List**.
HTTPS Certificate Verification Failure notification	When traffic was blocked because a user tried to access an HTTPS website where the certificate is not trusted.
Website Blocked: Patient-Zero notification	When Patient Zero Protection is enabled and a file has been submitted to Virtual Analyzer for sandbox analysis. The page will be blocked until sandbox analysis is complete. The action taken after analysis is complete is determined by the 'risk-level actions' of the matched policy. For the default settings, the high-risk and medium-risk levels will be blocked.
Website Blocked: Scan Policy Block notification	When a policy violation occurred because the policy restricts access to inappropriate content and the action is **Block**.
Website Blocked: HTTPS Certificate Verification	When access to this website was blocked because the website's certificate is not trusted. User cannot choose to go to the website anyway.

Notification Message Tokens

Deep Discovery Web Inspector sends notifications to alert end users about a security violation or if Deep Discovery Web Inspector detects other issues when a user attempts to access a web resource.

Each notification uses tokens to customize the message content and to provide information that is specific to that violation. Not all tokens are valid in every notification.

If you want to customize the notifications, you can use the following table to determine which tokens are accepted in each notification.

TABLE 7-1. Notification Message Tokens

TOKEN	FIELD NAME	NOTIFICATIONS WHERE TOKEN VALID
`%URL%`	URL	Blocked List notification HTTPS Certificate Verification Failure notification Website Blocked: Advanced Threat Protection notification Website Blocked: HTTPS Certificate Verification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification
`%DOMAIN%`	Domain	Blocked List notification HTTPS Certificate Verification Failure notification Website Blocked: Advanced Threat Protection notification Website Blocked: HTTPS Certificate Verification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification

Token	Field Name	Notifications Where Token Valid
`%SERVER_IP%`	Server IP	Blocked List notification HTTPS Certificate Verification Failure notification Website Blocked: Advanced Threat Protection notification Website Blocked: HTTPS Certificate Verification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification
`%POLICY_NAME%`	Policy name	Website Blocked: Advanced Threat Protection notification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification
`%URL_CATEGORY%`	URL Category	Website Blocked: Advanced Threat Protection notification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification
`%USER%`	User	Blocked List notification HTTPS Certificate Verification Failure notification Website Blocked: Advanced Threat Protection notification Website Blocked: HTTPS Certificate Verification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification

Token	Field Name	Notifications Where Token Valid
%USER_GROUP%	Group name	Website Blocked: Advanced Threat Protection notification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification **Note** This token is displayed only if domain groups are configured in a policy or HTTPS Inspection policy, and this policy or HTTPS Inspection policy is matched. The token displays the configured domain group name (CommonName).
%FILE_NAME%	File Name in HTTP Request or HTTP Response	HTTPS Certificate Verification Failure notification Website Blocked: Advanced Threat Protection notification Website Blocked: HTTPS Certificate Verification Website Blocked: Patient-Zero notification Website Blocked: Scan Policy Block notification
%MALWARE_NAME%	Malware name	Website Blocked: Advanced Threat Protection notification
%THREAT_TYPE%	Threat type	Website Blocked: Advanced Threat Protection notification
%RISK_LEVEL%	Risk level	Website Blocked: Advanced Threat Protection notification
%TECH_TYPE%	Detection type	Website Blocked: Advanced Threat Protection notification

TOKEN	FIELD NAME	NOTIFICATIONS WHERE TOKEN VALID
`%DETAIL%`	Detail	HTTPS Certificate Verification Failure notification Website Blocked: HTTPS Certificate Verification
`%HTTPS_POLICY_NAME%`	HTTPS policy name	HTTPS Certificate Verification Failure notification Website Blocked: HTTPS Certificate Verification

Editing User Notifications

You can make changes to the messages used in the end-user notifications for security violations.

Procedure

1. Go to **Policy** > **User Defined Settings** > **Notifications**.

2. Click an available notification template.

   List of User Notifications on page 7-57

3. Specify changes to the notification, as required.

   You can use predefined tokens to customize the notification messages. You can also reset any of the notifications back to their predefined template.

   Notification Message Tokens on page 7-58

4. Click **Save**.

Chapter 8

Alerts and Reports

Topics include:

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.

Managing Triggered Alerts

Perform any of the following tasks to manage alerts at **Alerts / Reports** > **Alerts** > **Triggered Alerts**.

Procedure

- View existing triggered alerts.
- Specify search filters to control the display and view of existing triggered alerts.
- Export up to 50,000 triggered alerts to a CSV file.
- Delete triggered alerts after review.

Related information

↳ *Viewing Triggered Alerts*

Viewing Triggered Alerts

Triggered alerts display existing critical, important, and informational alert notifications.

Procedure

1. Go to **Alerts / Reports** > **Alerts** > **Triggered Alerts**.
2. Specify the search criteria.
   - **Level**
   - **Type**
   - **Rule name**
   - **Period**
3. View alert details.

HEADER	DESCRIPTION
Triggered	The date and time when the alert occurred
Level	The importance of the alert: critical, important, or informational
Rule	The name of the alert rule that triggered the alert
Criteria	The alert rule criteria that triggered the alert
Detections	The number of watched detections that triggered the alert
Notification Recipients	The most recent alert notification recipients
Notification Subject	The most recent alert notification subject

Related information

⤷ *Critical Alerts*
⤷ *Important and Informational Alerts*

Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention.

Critical alerts are enabled by default.

TABLE 8-1. Critical Alerts

NAME	DEFAULT CRITERIA	DEFAULT ALERT FREQUENCY
Security: Multiple Advanced Threats Detected in Specified Network Groups	10 or more advanced threats detected on hosts	Once every 5 minutes
Security: Multiple Ransomware Detected in Specified Network Groups	10 or more ransomware detections on hosts	Once every 5 minutes
Security: Multiple C&C Callbacks Detected in Specified Network Groups	10 or more C&C callbacks detected on hosts	Once every 5 minutes
Security: Multiple Coin Miners Detected in Specified Network Groups	10 or more coin miner detections on hosts	Once every 5 minutes
System: Service Stopped/ Abnormal	Service % has stopped and cannot be restarted	Immediate
System: License Expiration	License is about to expire or has expired	Immediate
System: Network Is Down	Device %s's network is down	Immediate

Important and Informational Alerts

The following table explains the important and informational alerts triggered by events that require observation.

Important alerts are enabled by default. Informational alerts are disabled by default.

TABLE 8-2. Important Alerts

NAME	DEFAULT CRITERIA	DEFAULT ALERT FREQUENCY
System: High CPU Usage	CPU usage is at least 90%	Once a day

Name	Default Criteria	Default Alert Frequency
System: Low Free Disk Space	Disk space is 20 GB or less	Once every hour
System: Component Update/ Rollback Unsuccessful	An update/rollback was not successful	Immediate
System: High Memory Usage	Memory usage is at least 90%	Once a day
System: Network Is Up	Device %s's network is up	Immediate

Table 8-3. Informational Alerts

Rule Name	Criteria	Default Alert Frequency
System: Component Update/ Rollback Successful	An update/rollback was successfully completed	Immediate

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 9-33*.

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 9-117*.

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

Critical Alert Parameters

You can customize alert notification parameters for the following critical alerts:

- Security: Multiple Advanced Threats Detected in Specified Network Groups
- Security: Multiple Ransomware Detected in Specified Network Groups
- Security: Multiple C&C Callbacks Detected in Specified Network Groups
- Security: Multiple Coin Miners Detected in Specified Network Groups
- System: Service Stopped/Abnormal
- System: License Expiration
- System: Network Is Down

Important

You must configure an SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-33*.

Security: Multiple Advanced Threats Detected in Specified Network Groups

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Detections	Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20 The default is 10.
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every 5 minutes.
Network Object	Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.
Exception	Select to include exceptions to the alert rule.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.

Parameter	Description
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%Threshold%` • `%ThreatCount%`

Security: Multiple Ransomware Detected in Specified Network Groups

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Detections	Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20 The default is 10.
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every 5 minutes.
Network Object	Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.
Exception	Select to include exceptions to the alert rule.

Parameter	Description
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%Threshold%` • `%ThreatCount%`

Security: Multiple C&C Callbacks Detected in a Specified Network Groups

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Detections	Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20 The default is 10.
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every 5 minutes.

Parameter	Description
Network Object	Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.
Exception	Select to include exceptions to the alert rule.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%Threshold%` • `%ThreatCount%`

Security: Multiple Coin Miners Detected in Specified Network Groups

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Detections	Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20 The default is 10.

Parameter	Description
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every 5 minutes.
Network Object	Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.
Exception	Select to include exceptions to the alert rule.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%Threshold%` • `%ThreatCount%`

System: Service Stopped/Abnormal

Parameter	Description
Status	Select an option to enable or disable the alert.

PARAMETER	DESCRIPTION
Alert level	Displays the alert level in email messages.
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%ServiceName%`

System: License Expiration

PARAMETER	DESCRIPTION
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.

Parameter	Description
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%DaysBeforeExpiration%` • `%ExpirationDate%` • `%LicenseStatus%` • `%LicenseType%`

System: Network Is Down

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.

PARAMETER	DESCRIPTION
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%PortName%`

Important and Informational Alert Parameters

You can customize important and informational alert parameters.

You can customize the following informational alert:

- System: Component Update/Rollback Successful

You can customize the following important alerts:

- System: High CPU Usage
- System: Low Free Disk Space
- System: Component Update/Rollback Unsuccessful
- System: High Memory Usage
- System: Network Is Up

Important

You must configure an SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-33*.

System: Component Update/Rollback Successful

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%ComponentList%`

System: High CPU Usage

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.

PARAMETER	DESCRIPTION
Average CPU usage	Specifies the average CPU usage threshold that will trigger the alert. You can customize this parameter. The default is 90%.
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once a day.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%CPUUsage%` • `%CPUThreshold%`

System: Low Free Disk Space

PARAMETER	DESCRIPTION
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.

Parameter	Description
Free disk space	The lowest disk space threshold in GB that triggers the alert. You can customize this parameter. The default is 20 GB.
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every hour.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%DiskSpace%`

System: Component Update/Rollback Unsuccessful

Parameter	Description
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.

PARAMETER	DESCRIPTION
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%ComponentList%`

System: High Memory Usage

PARAMETER	DESCRIPTION
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Average memory usage	Specifies the memory usage threshold that will trigger the alert. You can customize this parameter. The default is 90%.

PARAMETER	DESCRIPTION
Alert frequency	Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once a day.
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%MemoryUsage%` • `%MemoryThreshold%`

System: Network Is Up

PARAMETER	DESCRIPTION
Status	Select an option to enable or disable the alert.
Alert level	Displays the alert level in email messages.
Alert frequency	**Note** You cannot configure alert frequency for this notification. The default is to send the notification immediately.

Parameter	Description
Recipients	Specify the recipients who will receive the triggered alert email message or select `Send to all contacts` to send the alert to all recipients in the contact list.
Subject	Specifies the subject of the triggered alert email message. You can customize this parameter.
Message	Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message: • `%ConsoleURL%` • `%DateTime%` • `%DeviceName%` • `%DeviceIP%` • `%PortName%`

Reports

Deep Discovery Web Inspector provides reports to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. Deep Discovery Web Inspector offers flexibility in specifying the content for each report.

The reports generate in PDF format.

Scheduling Reports

Scheduled reports automatically generate according to the configured schedules.

Procedure

1. Go to **Alerts / Reports** > **Reports** > **Schedules**.

2. Enable scheduled reports by selecting one or more of the associated intervals.

   - **Generate daily report**
   - **Generate weekly report**
   - **Generate monthly report**

3. Specify when to generate each of the selected reports.

   When a monthly report schedule is set to generate reports on the 29th, 30th, or 31st day, the report generates on the last day of the month for months with fewer days.

   For example, if you select 31, the report generates on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Specify the recipients for each selected report.

   You can choose to send each specified report to all contacts (the default) or specify a list of recipients who should receive the report. If specifying recipients, separate multiple recipients with a semicolon.

   If using the default option and you want to configure the list of contacts, see *Managing Contacts on page 9-117*.

   Important

   You must configure the SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-33*.

5. Click **Save**.

Generating On-Demand Reports

You can generate on-demand reports at any time.

Procedure

1. Go to **Alerts / Reports** > **Reports** > **On Demand**.

2. Configure report settings.

Option	Description
Period	Select the scope and start time or end time for report generation.
Recipients	Specify the recipients. Separate multiple recipients with a semicolon. **Important** You must configure the SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-33*.

3. Click **Generate**.

   The report generates and the following actions occur:

   - The report appears at **Alerts / Reports** > **Reports** > **Generated Reports**.
   - Report notifications are sent to specified recipients.

Chapter 9

Administration

Topics include:

Deployment Wizard

Topics include:

- *Accessing the Deployment Wizard on page 9-2*
- *Configuring Forward Proxy Mode on page 9-2*
- *Configuring Transparent Bridge Mode on page 9-5*
- *Configuring Transparent HA Mode on page 9-9*
- *Configuring Multi-Bridge Mode on page 9-13*
- *Configuring LACP Deployments on page 9-16*

Related information

↳ *Network Deployment Mode Overview*

Accessing the Deployment Wizard

If you want to change basic configuration parameters after the initial deployment is complete, you can access the **Deployment Wizard** at any time and make any desired changes.

When you open the **Deployment Wizard**, the wizard will display the last saved parameters. To save changes, you must proceed through the entire wizard just as you did for the initial configuration and click **Finish**.

Configuring Forward Proxy Mode

You can open the **Deployment Wizard** screen after the appliance is configured and modify deployment mode settings.

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.

If you are performing the initial deployment, see *Deployment on page 3-1*.

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.

Option	Description
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 9-42*.

Related information

- *Network Deployment Mode Overview*

Configuring Transparent Bridge Mode

You can open the **Deployment Wizard** screen after the appliance is configured and modify deployment mode settings for Transparent Bridge mode deployments.

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*.

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.

If you are performing the initial deployment, see *Deployment on page 3-1*.

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	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**.
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.

Option	Description
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*

Configuring Transparent HA Mode

You can open the **Deployment Wizard** screen after the appliance is configured and modify deployment mode settings for Transparent HA deployments. Transparent HA mode is a two-node solution. Perform the following procedure on each node.

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*.

Important

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.

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.

If you are performing the initial deployment, see *Deployment on page 3-1*.

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.
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**.

Option	Description
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**
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*

Configuring Multi-Bridge Mode

You can open the **Deployment Wizard** screen after the appliance is configured and modify deployment mode settings for Multi-Bridge deployments.

Important

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

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.

If you are performing the initial deployment, see *Deployment on page 3-1*.

Procedure

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

   The **Welcome** page opens.

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

3. Click **Next**.

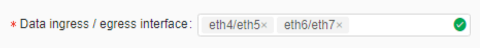
4. In the **Working Mode Settings** page, specify the following:

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.
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.

Option	Description
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**. * Data ingress / egress interface: 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.

Related information

↳ *Network Deployment Mode Overview*

Configuring LACP Deployments

You can open the **Deployment Wizard** screen after the appliance is configured and modify deployment mode settings for deployments using LACP.

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.

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.

If you are performing the initial deployment, see *Deployment on page 3-1*.

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*

Component Updates

Download and deploy product components used to investigate threats. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest ransomware and malware attacks.

- *Components on page 9-20*
- *Updating Components on page 9-22*
- *Rolling Back Components on page 9-22*
- *Scheduling Component Updates on page 9-23*

Components

The **Components** tab at **Administration** > **Component Updates** shows the security components currently in use.

TABLE 9-1. Components

COMPONENT	DESCRIPTION
Advanced Threat Scan Engine for Deep Discovery (64-bit)	The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection.
Bot Pattern	The Bot Pattern is used by the Network Content Inspection Engine to perform bot network scanning.
Deep Discovery Malware Pattern	The Deep Discovery Malware Pattern contains the detection routines for virus and malware scanning. Trend Micro updates the Deep Discovery Malware Pattern regularly with detection routines for new identified threats.

Component	Description
Deep Discovery Trusted Certificate Authorities	Deep Discovery Trusted Certificate Authorities provides the trusted certificate authorities to verify PE signatures.
IntelliTrap Exception Pattern	The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning.
IntelliTrap Pattern	The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats.
Network Content Correlation Pattern	The Network Content Correlation Pattern implements detection rules defined by Trend Micro.
Network Content Inspection Engine (Linux, User mode, 64-bit)	The Network Content Inspection Engine is used to perform network scanning.
Network Content Inspection Pattern	The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning.
Predictive Machine Learning Pattern	The Predictive Machine Learning Pattern is used by Predictive Machine Learning to help classify malware.
Predictive Web Pre-Filter Pattern	The Predictive Web Pre-Filter Pattern is used by the Static Intelligence Engine to help classify malware.
Script Analyzer Pattern (Deep Discovery)	The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.
Smart Scan Agent Pattern	The Smart Scan Agent Pattern contains the detection routines for malware and spyware under Smart Scan mode.
Spyware/Grayware Pattern	The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware.
URL Filtering Engine	The URL Filtering Engine is used to filter URLs based on their reputations.

COMPONENT	DESCRIPTION
Virtual Analyzer Configuration Pattern	The Virtual Analyzer Configuration Pattern contains configuration information for Virtual Analyzer, such as supported threat types and supported file types.
Virtual Analyzer Sensors	The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer.

Updating Components

Update components to immediately download the component updates from the update source server.

Procedure

1. Go to **Administration** > **Component Updates** > **Components**.
2. Select one or more components.
3. Click **Update**.

   "Updating" displays while the update is in progress. And after the update finishes, "Update succeeded" displays.

Rolling Back Components

Roll back components to revert all components to the most recent version.

Procedure

1. Go to **Administration** > **Component Updates** > **Components**.
2. Select one or more components.
3. Click **Roll Back**.

"Rolling back" displays while the rollback is in progress. And after the rollback finishes, the message changes to say that rollback was successful.

The components revert to the most recent version.

Scheduling Component Updates

Procedure

1. Go to **Administration** > **Component Updates** > **Schedule**.

   The **Schedule** tab appears.

2. Enable the scheduled update.

3. Select the update interval.

4. Click **Save**.

Product Updates

Use the **Product Updates** screen to apply hotfixes and patches, or perform a firmware upgrade to Deep Discovery Web Inspector.

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 9-2. 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.

System Settings

Topics include:

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.

Managing Static Routes

Perform any of the following tasks to manage static routes at **Administration** > **System Settings** > **Static Routes**.

Procedure

- Specify search filters to control the display and view of existing static routes.
- Add or delete static routes.

Option	Description
Add	Add a new static route. *Adding a Static Route on page 9-31*
Delete	Delete static routes by selecting one or more static routes from the list and clicking **Delete**.

Adding a Static Route

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

You can configure IPv4 static routes.

Procedure

1. Go to **Administration** > **System Settings** > **Static Routes**.
2. Click **Add**.

   The **Add Static Route** window appears.
3. In **Network ID**, specify the network address.
4. In **IPv4 netmask**, enter the netmask for the network ID.
5. In **Router**, specify the IP address for the next hop router.
6. In **Interface**, specify the interface used to reach the next hop router.
7. Click **Save**.

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.
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 9-94*

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.
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**.

Configuring System Time

Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system date and time and time zone.

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet.

Procedure

1. Go to **Administration** > **System Settings** > **Time**.
2. Set the system time.
    - To synchronize with an NTP server, select **Synchronize appliance time with an NTP server** and then specify the domain name or IP address of the NTP server.
    - To manually set the system time, select **Set time manually** and then select the date and time and select the time zone.
3. Click **Save**.

Configuring SNMP

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

On Deep Discovery Web Inspector, use the **Administration** > **System Settings** > **SNMP** tab to perform the following tasks:

- Configure the appliance to send trap messages

  For details, see *Configuring Trap Messages on page 9-35*.

- Configure the appliance to listen for manager requests

  For details, see *Configuring Manager Requests on page 9-37*.

Configuring Trap Messages

A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Under **Trap Messages**, select **Send SNMP trap messages**.
3. Specify the trap message settings.

Option	Description
Manager server address	Specify the manager server address. You can specify as an IP address or a FQDN.
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: "" (default context) • Context Engine ID: <Auto> • (Optional) MD5 Authentication protocol: HMAC-MD5 • (Optional) DES Privacy protocol: CBC-DES

Option	Description
Community name	**Note** This field is only available for SNMPv1/SNMPv2c. Type a community name that is less than 255 characters and does not contain double-byte encoded characters, spaces, or the following characters: [ ] '/ " { } < > | & ! ( )
Security model	**Note** This field is only available for SNMPv3. Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	**Note** This field is only available for SNMPv3 (all security models). Specify the user name. A valid user name is less than 255 characters and and does not contain double-byte encoded characters, spaces, or the following characters: [ ] ' / " { } < > | & ! ( )
Password	**Note** This field is only available for SNMPv3 using `Authenticated` or `Authenticated with privacy` security model. Specify the password. A valid password is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / " { } < > | & ! ( )

Option	Description
Privacy passphrase	**Note** This field is only available for SNMPv3 using the `Authenticated with privacy` security model. Specify the privacy passphrase. A valid passphrase is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / " { } < > | & ! ( )

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

   - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

   - For a list of Deep Discovery Web Inspector supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request Deep Discovery Web Inspector system information.

Procedure

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

2. Under **Manager Requests**, select **Listen for requests from SNMP managers**.

3. Specify the manager request settings.

Option	Description
Device location	Specify the location of this appliance. A valid device location is less than 255 characters and does not contain the following characters: [ ] ' / " { } < > | & ! ( )
Administrator contact	Specify the administrator contact of this appliance. A valid administrator contact is less than 255 characters and does not contain the following characters: [ ] ' / " { } < > | & ! ( )
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: "" (default context) • Context Engine ID: <Auto> • (Optional) MD5 Authentication protocol: HMAC-MD5 • (Optional) DES Privacy protocol: CBC-DES
Allowed community names	**Note** This field is only available for SNMPv1/SNMPv2c. Specify a maximum of 5 community names. A valid allowed community name is less than 255 characters and does not contain double-byte encoded characters, spaces, or the following characters: [ ] ' / " { } < > | & ! ( )
Trusted manager server addresses	**Note** This field is only available for SNMPv1/SNMPv2c. Specify a maximum of 32 trusted manager server addresses.

Option	Description
Security model	**Note** This field is only available for SNMPv3. Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	**Note** This field is only available for SNMPv3 (all security models). Specify the user name. A valid manager requests user name is less than 255 characters and does not contain double-byte encoded characters, spaces, or the following characters: [ ] ' / " { } < > | & ! ( )
Password	**Note** This field is only available for SNMPv3 using `Authenticated` or `Authenticated with privacy` security model. Specify the password. A valid manager requests password is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / " { } < > | & ! ( )

OPTION	DESCRIPTION
Privacy passphrase	**Note** This field is only available for SNMPv3 using the `Authenticated with privacy` security model. Specify the privacy passphrase. A valid manager requests passphrase is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / " { } < > | & ! ( )

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

   - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

   - For a list of Deep Discovery Web Inspector supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

Managing Authentication Certificates

You can manage the certificates that are used for authenticating administrators accessing the Web console and for Captive Portal authentication for users who want to access web resources.

NOTICE

After saving the configuration performed in this procedure, the Web console and Captive Portal will be restarted. After several seconds, manually re-log-on to the Web console. Since the certificate has been changed, the browser might not log on the user to the Web console automatically.

The recommendation is to perform this operation during non-work time.

Procedure

1. Go to **Administration** > **System Settings** > **Authentication Cert**.

2. Under **Assign certificate**, select one of the following:

   The certificate is used to sign an endpoint certificate for the administrative Web console or Captive Portal.

OPTION	DESCRIPTION
Assign by importing certificate	To import a certificate manually.
Assign by HTTPS policy	To use the CA certificate from a specified HTTPS Inspection policy. **Important** Before selecting and configuring an authentication certificate using the **Assign by HTTPS policy** option, you should ensure that the CA certificate of the selected HTTPS Inspection policy is installed on client machines before changing the authentication certificate. This ensures that clients/browsers can build a complete certificate chain, thus avoiding authentication failures.

3. Perform the appropriate steps, depending on method of certificate assignment.

METHOD	STEPS TO TAKE
Assign by importing certificate	a. Select the **Import type**: • **PEM/DER** The certificate file is in PEM or DER file format. • **PKCS7** The certificate file is in P7B or PKCS#7 file format. • **PKCS12** The certificate file is in PFX or PKCS#12 file format.

METHOD	STEPS TO TAKE
	b. In **Certificate**, browse and choose the certificate file. c. For the **PEM/DER** and **PKCS7** formats: In **Private key**, browse and choose the private key file for the certificate file. d. Enter the password of the private key and then confirm it. e. Click on **Verify Certificate** to verify that the certificate is valid.
Assign by HTTPS policy	a. In **Assign from HTTPS policies** select the HTTPS Inspection policy with the CA certificate that will be used to sign an endpoint certificate and for accessing the Web console and for authentication. b. Verify the correct HTTPS Inspection policy is selected. **Note** When using the CA certificate from an HTTPS Inspection certificate to sign an endpoint certificate: • CommonName = host name of Deep Discovery Web Inspector appliance • Signature algorithm: sha256RSA • Subject Alternative Name: DNS Name = host name of Deep Discovery Web Inspector appliance

4. Click **Save**.

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.
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**.

Active Directory Services

You can configure Deep Discovery Web Inspector Active Directory Services to integrate with Active Directory for authentication Services. With the integrated Services, Deep Discovery Web Inspector can use Active Directory accounts for authentication.

Deep Discovery Web Inspector supports integration with the following Microsoft Active Directory servers:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

You can use Active Directory authentication for the following:

Account management	Create an account using an Active Directory user that can log into the web console, including a user with full administrative rights.
Notification templates	Deep Discovery Web Inspector can insert Active Directory user or group names into the %USER% and %USER_GROUP % tokens used in applicable notification templates.
Policy matching using traffic source	Use Active Directory users or groups to match policy traffic using the traffic source criteria.
HTTPS Inspection rule matching using traffic source	Use Active Directory users or groups to match HTTPS inspection policy traffic using the decryption source criteria.
Web access and Captive Portal authentication	Deep Discovery Web Inspector can use Active Directory users or groups for authentication when end-users access web resources. If Deep Discovery Web Inspector cannot transparently authenticate an end-user, then the user can use Active Directory credentials to log on through Captive Portal.

When configuring Active Directory Services, keep the following in mind:

- Supported format for adding an Active Directory domain account is [DOMAIN]\[USERNAME].

- You can choose users and groups from multiple Active Directory domains.
- You can set one Active Directory domain as the default domain.

Note

NTLM authentication is only supported in the default domain.

- You can specify a list of domain controllers and global catalogs to use for each specified domain or you can have Deep Discovery Web Inspector automatically discover them.

Note

Deep Discovery Web Inspector discovers Active Directory servers by querying DNS servers for service records (SRV). You must ensure that the DNS servers configured in Deep Discovery Web Inspector contain the appropriate "_gc._tcp" or "_ldap._tcp" records.

- Deep Discovery Web Inspector automatically synchronizes Active Directory information with the appliance's account information according to configured settings.

  Alternatively, you can manually synchronize account information.
- You can customize the client IP ranges on which to apply Active Directory authentication.
- Deep Discovery Web Inspector records information in the detection log and access log (via syslog). If traffic is authenticated, the user name and domain information is recorded in these logs. If not authenticated, the user name is recorded as the IP address and the domain field is blank.
- Enabling IP user cache is strongly recommended (default is enabled). If IP user cache is disabled, some applications or browsers might not access the Internet successfully.
- When choosing domain controllers, recommendation is to use the 'nearby-est/fastest/local' domain controllers. The 'far/slow/remote' domain controllers will slow down authentication and user/group synchronization speed.

- It is recommended that you use an administrator account for the Active Directory Services service account when configuring Active Directory domains.

Important

If the service account's password is expired, authentication will not work. Be sure to update the service account's password before it expires.

- The following operation restarts the scan daemon and the authentication daemon; therefore, this operation should be executed during non-working time:

  Configure global authentication settings

- The following operations reload the scan daemon and restart the authentication daemon; therefore, these operations should be executed during non-working time:
  - Adding, modifying, or removing Active Directory domains
  - Operations on the default domain (disable/enable default domain)
- Captive Portal supports the following format for the user name:
  - [Netbios Domain Name]\[sAMAccountName]
  - [sAMAccountName] (only supported for authentication on the default domain)
  - UPN
- NTLM authentication supports the following format for user name: [DOMAIN]\[sAMAccountName] (only supported for authentication on the default domain)

Enabling Authentication Using Active Directory Services

This is a global setting. If enabled, Active Directory authentication is enabled for all Active Directory domains configured for Deep Discovery Web Inspector Active Directory Services.

Note

- If global authentication is enabled, authentication is required for users in configured domains if their web traffic matches configured authentication policies.

  Deep Discovery Web Inspector uses authentication policies to judge how to authenticate. The authentication options are: none, standard mode, standard enforce mode, x-header mode.

  - If there is a match to a policy with none authentication mode or there is not a match to any authentication policies, authentication is performed using the IP address.

  - If a user belongs to a domain that is not configured in Deep Discovery Web Inspector Active Directory Services and he uses his domain to do authentication, the authentication fails.

  Managing Active Directory Services Domains on page 9-52

- After global authentication is enabled, authentication policies determine how authentication is performed for individual users and clients (IP addresses).

  Configuring Global Authentication Settings on page 9-48

  Network objects are the criteria used to determine whether an authentication policy applies to users accessing web resources through the appliance. If a user attempts to access web resources from a client that is not a member of a network object in any of the authentication policies, user authentication is not used. Instead, authentication is performed using the IP address.

  Managing Authentication Policies on page 9-54

Procedure

1. Go to **Administration** > **Active Directory Services**.

   The **Active Directory Services** screen appears.

   Important

   Before you proceed, consider the following: The following operation restarts the scan daemon and the authentication daemon, which interrupts daily traffic; therefore, this operation should be executed during non-working time:

2. Click on **Configure Global Authentication Settings**.

   The **Global Authentication Settings** screen opens.

3. Click on **Enable global authentication** to globally enable the use of Active Directory Services for authentication.

4. Click **Save**.

   For more information about configuring other global authentication settings, see *Configuring Global Authentication Settings on page 9-48*.

Configuring Global Authentication Settings

You can globally enable Active Directory authentication for users accessing web resources, for users accessing the Deep Discovery Web Inspector web console, for policy and HTTPS inspection policy matches, and for account management.

You should consider the following when using Active Directory authentication for Captive Portal:

- If Deep Discovery Web Inspector can do pass-through authentication for the user requesting access to web resources, a separate log on is not required.

- If Deep Discovery Web Inspector is unable to transparently perform pass-through authentication, Captive Portal takes over and authenticates the user. The Captive Portal sign-on page requires users to specify a user name and password before accessing the network or Internet.

  The Captive Portal sign-on page takes over and authenticates for the following reasons:

  - The primary reason why the Captive Portal page is shown is because NTLM/Kerberos/basic authentication failed

> **Note**
>
> Only proxy mode supports basic authentication. Bridge mode does not support basic authentication

- The client computer is not added into an Active Directory domain and the user name/password entered into Windows authentication window is incorrect.
- The keytab file for the domain is imported, which makes this a Kerberos authentication scenario, and the time gap between client and Deep Discovery Web Inspector/KDC is too large (by default the gap must be less than 5 minutes). If the time gap is greater than five minutes, Kerberos authentication fails.
- For some browsers in certain operating systems (for example Firefox in Ubuntu) or because of incompatibility problems with WIN2012R2, NTLM authentication might fail. Under these circumstances, the Captive Portal page is shown.

For more information, see *Captive Portal on page 9-50*.

Procedure

1. Go to **Administration** > **Active Directory Services**.

   The **Active Directory Services** screen appears.

   Important

   Before you proceed, consider the following: The following operation restarts the scan daemon and the authentication daemon, which interrupts daily traffic; therefore, this operation should be executed during non-working time:

2. Click on **Configure Global Authentication Settings**.

   The **Global Authentication Settings** screen opens.

3. Click on **Enable global authentication** to globally enable the use of Active Directory Services for authentication.
4. Under **Kerberos keytable**, perform one of the following:
   - To use Kerberos authentication, click on **Import** to import the Kerberos key table.

- Select **Disable Kerberos Authentication** if you do not want users to use Kerberos authentication.

5. Under **Captive portal logo (customize)**, click on **Import** to import a custom logo image.

   The image displays on the **Welcome to Captive Portal** log on page.

6. (Optional) Customize the **Captive portal description** that displays on the **Welcome to Captive Portal** log on page.

7. Review information in **Preview** to verify that the displayed logo and message are as desired.

8. (Optional) Restore the Captive Portal page to the default template by clicking on **Restore Captive Portal**.

9. Click **Save**.

What to do next

You can change the certificate used for user authentication by clicking on **Click here to change the administration portal certificate**. By clicking on this link, you will be taken to another screen. To return to the **Global Authentication Settings** screen, you will need to manually navigate back to it.

Captive Portal

If the user is unable to pass NTLM/Kerberos authentication, Captive Portal can take over and authenticate the user with a web form.

To receive the web form, users must be using a web browser and be in the process of connecting. Upon successful authentication, users are automatically directed to the originally requested website. The Deep Discovery Web Inspector appliance can now execute policies based on the user information for any applications passing through the appliance, not just for applications that use a web browser.

Administrators can design and create the text that users see when they sign on. The customizable message includes:

- Company logo image
- A welcome message

Note

If you modify Captive Portal-related settings, the operation restarts the scan daemon and the authentication daemon, which interrupts daily traffic; therefore, this operation should be executed during non-working time

The following rules apply to Captive Portal:

- Captive Portal rules work only for web (HTTP/HTTPS) traffic.
- A web page prompts the user to specify a user name and password.
- If allowed via an authentication policy, a user can log on as a guest user. Guest user only matches those policies and HTTPS policies where the traffic source is **Guest users** or **Any**.
- Captive Portal supports the following format for the user name:
  - [Netbios Domain Name]\[sAMAccountName]
  - [sAMAccountName] (only supported for authentication on the default domain)
  - UPN

The Deep Discovery Web Inspector appliance validates the user name and password by connecting to Active Directory server using LDAP. If the LDAP connection is successful, Deep Discovery Web Inspector searches for the user in the local database. If the user information matches, authentication succeeds. If there are no matches, authentication fails. If successfully authenticated, the Deep Discovery Web Inspector appliance adds the IP address-to-user mapping to local cache for the time-to-live (TTL) life cycle.

Note

Deep Discovery Web Inspector does not store any passwords for end users.

Managing Active Directory Services Domains

Go to **Administration** > **Active Directory Services** > **Active Directory** to perform any of the following tasks to manage Active Directory Services domains. Authentication services are provided by domains added to the Deep Discovery Web Inspector Active Directory Services list.

Procedure

- View summary information about existing Active Directory Services domains.
- Under the **Default Domain** column, enable or disable a specified domain as the default domain.
- Click **Add** to configure a new Active Directory Services domain.
- Click an Active Directory Services domain name to view or modify settings.
- Click **Synchronize** to synchronize user information between the selected domain's domain controllers and Deep Discovery Web Inspector.
- Select a domain and then click **Remove** to remove the domain from Active Directory Services.

Adding Microsoft Active Directory Domains

You can integrate Microsoft Active Directory authentication to Deep Discovery Web Inspector by adding one or more Active Directory domains to Deep Discovery Web Inspector Active Directory Services.

Procedure

1. Obtain the information from the Active Directory administrator that is required to add a domain to the Deep Discovery Web Inspector Active Directory Services configuration.
2. Go to **Administration** > **Active Directory Services** > **Active Directory**.

3. Click **Add**.

4. Enter the **Domain name**.

5. Enter the **Service account**.

   This is the Active Directory account used to access resources on the Active Directory domain controllers. The account must exist and must have appropriate permissions.

   You must enter the account name in the following format: [Netbios Domain Name]\[sAMAccountName]

6. Type the service account's password.

   Once the password of service account is nearly expired, you should modify the password manually here. Be aware that modifications to any settings here will restart the authentication daemon. The recommendation is to modify the password during non-working time.

7. If desired, specify that the configuration use Microsoft Active Directory Global Catalog servers by enabling **Global Catalog servers**.

   If you enable Deep Discovery Web Inspector to use global catalog servers, domains in the forest of domains in the selected global catalogs are authenticated. If you do not configure Active Directory Services to use global catalog servers, the standard domain controllers are used for authentication, and only the configured domain is used for authentication. The default is to use the global catalog type.

8. Specify whether to use LDAP StartTLS for connections to the Active Directory servers.

9. (Optional) Click on **Advanced setting** if you want to configure advanced settings.

   a. Select the HA policy to use when connecting to the Active Directory servers.

      - Round robin (default)

      - Fail over

   b. In **LDAP server name**, select the LDAP server names that you want Deep Discovery Web Inspector to use or click on **Auto Detect** to have Deep Discovery Web Inspector automatically detect Active Directory servers.

The default is to auto detect.

Note

When choosing domain controllers, the recommendation is to select the fastest (least time-lag) LDAP servers (domain controllers) and delete the slow (large time-lag) LDAP servers.

If necessary, you can obtain this information by referring to the LDAP server list that is obtained by auto detection. The faster, least time-lag LDAP servers are listed at the top of the total list. The slower, large time-lag LDAP servers are list at the bottom of the total list.

The 'far/slow/remote' domain controllers will slow down authentication and user/group synchronization speed.

---

c. Type the base distinguished name.

The default is the base distinguished name derived from **Domain name**.

10. Click **Test Connection** to verify that a connection to a Microsoft Active Directory server can be established using the specified information.

11. Click **Save**.

Managing Authentication Policies

Go to **Administration** > **Active Directory Services** > **Authentication Policy** to perform any of the following tasks. Authentication policies are part of the Active Directory Services configuration and are used to determine which network objects/IP addresses should be authenticated using Active Directory Services, for configuring the authentication mode to use, and for configuring authentication cache settings.

Note

Deep Discovery Web Inspector applies authentication policies in the order in which they appear in the list. The first authentication policy that matches is applied to the authentication.

The **default** policy is preconfigured. Changes cannot be made to the **default** policy except to enable/disable the policy.

Procedure

- View summary information about existing authentication policies.
- Click a authentication policy's name to view or modify settings, including enabling or disabling the policy.
- Click **Add** to create a new authentication policy.
- Click on the **Drag and Drop** icon (✥) for an authentication policy and drag it to the position to which you want to move that policy.
- Select an authentication policy and then click **Move Up**, **Move Down**, or **Move Top** to change the policy order.
- Select an authentication policy and then click **Duplicate** to make a copy of the policy.
- Select an authentication policy and then click **Remove** to remove the policy.

Configuring Active Directory Services Authentication Policies

You can customize your authentication strategy by configuring authentication policies for Active Directory Services.

Procedure

1. Go to **Administration** > **Active Directory Services** > **Authentication Policy**.
2. Click on **Add**.
3. Enter a name for the authentication policy and optionally add a description.
4. Click on the **Enable** button to enable the policy.
5. Configure **Network objects** by selecting one of the following:
    - **Any**

      For the authentication policy to affect all network objects.

- **Selected network objects**

  For the authentication policy to affect only specific network objects and then move one or more objects from the available network objects box to the selected network objects box.

  You can create a new network object to include in the policy by clicking **Add new network object**.

  See *Managing Network Objects on page 7-46*.

6. (Optional) Select **Exceptions** to configure network object exceptions and then move one or more objects from the available network objects box to the exception network objects box.

   Authentication policy is not applied to network objects in the exception list.

7. Under **Authentication mode**, select one of the available modes:

   - **None**

     Do not use authentication, use the client IP for policy matching.

   - **Standard**

     Authenticates only HTTP traffic. Only authenticates browser traffic (by user-agent).

     Uses Kerberos/NTLM/Basic for transparent authentication. If transparent authentication fails, opens the Captive Portal page for users to authenticate.

   - **Standard Enforce**

     Authenticates all traffic (not just browser traffic).

     Authenticates both HTTP and HTTPS/HTTP2 traffic. For HTTPS/HTTP2 traffic, Deep Discovery Web Inspector does force decryption before authentication and resigns it using the CA certificate of the default HTTPS Inspection policy if the traffic does not match any other customized HTTPS Inspection policy.

Note

If the CA certificate of the default HTTPS policy is not trusted by clients, standard enforce authentication might fail, even if the default HTTPS policy is disabled.

To prevent this from happening, make sure that the CA certificate of the default HTTPS policy is trusted by clients.

- **X-header**

  Uses the X-Authenticated-User header from the downstream proxy to find the client's user name. If there is no header, uses the client IP for policy matching.

  Note

  - Deep Discovery Web Inspector supports only the following format for X-Authenticated-User:

    [Netbios Domain Name]\[sAMAccountName] with Base64 encoded

  - Example: X-Authenticated-User: Mms4YWxwaGFcYXV0byB1c2VyMw==

    In this example, the user is: 2k8alpha\auto user3

  - If the user name cannot be found in the domain controller's local database, Deep Discovery Web Inspector authenticates the traffic with the IP address (uses the client IP for policy matching).

For **Standard** and **Standard Enforce** mode, Deep Discovery Web Inspector tries to authenticate using Kerberos, NTLM, or Basic (Proxy Mode) Authentication. Only one method is chosen. If it fails, another method is not tried. For example, if Kerberos authentication is performed and fails, Deep Discovery Web Inspector does not go on to try NTLM or Basic. If Kerberos/NTLM/Basic authentication fails, Deep Discovery Web Inspector tries Captive Portal Authentication.

Note

Firefox in non-Windows platforms, like MacOS or Ubuntu, does not support NTLM authentication through Deep Discovery Web Inspector. If NTLM authentication fails, the Captive Portal page automatically opens.

To work around this issue, you can do the following:

- Enable NTLM in Firefox on non-Windows systems.
- Exclude problematic clients with non-Windows operating system from authentication policies.

8. Enable or disable the IP authentication cache.

The IP authentication cache provides important functionality when authenticating web traffic. It additionally provides performance benefits for authentication activities.

> **Important**
>
> Enabling IP authentication user cache is strongly recommended (default is enabled). If authentication user cache is disabled, some applications or browsers might not access the Internet successfully.

9. Configure the IP authentication cache time settings.

a. Choose the method for caching data:

- **Last active TTL** (default):

  Elapsed cache time is calculated from time of last web request.

- **Fixed TTL**:

  Elapsed cache time is fixed and calculated from time authentication information was entered into the cache.

b. Enter the number of minutes to cache the data.

Minimum value is 1. Maximum value is 1440. The default value is 120.

10. Enable or disable whether to allow guest access.

11. Click **Save**.

Integrated Products/Services

Deep Discovery Web Inspector integrates with the following products and services:

- *Apex Central on page 9-59*
- *Deep Discovery Director on page 9-63*
- *Threat Intelligence Sharing on page 9-67*
- *Log Settings on page 9-68*

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 synchronization of suspicious objects and suspicious object exceptions between Deep Discovery Web Inspector and Apex Central (formerly known as Trend Micro Control Manager). It can block the traffic if a match is found in the synchronized suspicious object list based on risk level. Deep Discovery Web Inspector can also upload the local virtual analyzer suspicious object black list and suspicious object detection logs to Apex Central.

For more information, see the *Trend Micro Apex Central Administrator's Guide* at the Apex Central documentation site.

Managing Apex Central Tasks

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

Procedure

- Register to an Apex Central server from the Deep Discovery Web Inspector web console, and then register to Deep Discovery Web Inspector from the Apex Central admin console.

  Registering to Apex Central From Deep Discovery Web Inspector Console on page 9-60

- Check the connection status between Deep Discovery Web Inspector and Apex Central.

- Configure the synchronization of suspicious objects with Apex Central.

- Unregister from an Apex Central server.

  Unregistering With Apex Central on page 9-62

- Ensure that both Deep Discovery Web Inspector and the Apex Central server belong to the same network segment.

Related information

↳ *Apex Central*

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.

Unregistering With Apex Central

You can unregister Deep Discovery Web Inspector with Apex Central. After unregistering, Deep Discovery Web Inspector can register to another Apex Central.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Apex Central**.

2. Under **General**, click the **Unregister** button.

What to do next

Then continue to unregister Deep Discovery Web Inspector with Apex Central. Go to the Apex Central admin console and then go to **Administration** > **Server registration**. Select the registered Deep Discovery Web Inspector appliance and then in the **Action** field, click the **Delete** button.

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**.

Registering to Deep Discovery Director

The following procedure is for registering to Deep Discovery Director. If you have already registered and want to change the connection settings, you must first unregister.

Note

You can register Deep Discovery Web Inspector to only one of the two integrated products (Apex Central or Deep Discovery Director) at any given time. You cannot register Deep Discovery Web Inspector with both products at the same time. If Deep Discovery Web Inspector is already registered with one of the two products, you cannot register with the other product until you unregister the currently registered product.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.

2. Configure **Connection Settings**.

OPTION	DESCRIPTION
Server address	Type the server address for Deep Discovery Director.
Port	Type the port number for Deep Discovery Director. Default is 443.
API key	Type the API key for Deep Discovery Director. **Note** You can find this information on the **Help** screen on the management console of Deep Discovery Director.

3. (Optional) If you have configured proxy settings for Deep Discovery Web Inspector and want to use these settings for Deep Discovery Director connections, select **Connect using a proxy server**.

Note

This setting can be changed after registering to Deep Discovery Director.

To update this setting without unregistering from Deep Discovery Director, click **Update Settings**.

4. Click **Register**.

   The **Status** changes to **Registered | Connected**.

Note

If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust New Fingerprint** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust New Fingerprint**.

After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.

Important

Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering the Deep Discovery Web Inspector appliance to Deep Discovery Director, configure the appliance to delete logs when the total free disk space is less than 20%.

For more information, see *Configuring Storage Maintenance on page 9-91*.

Viewing Deep Discovery Director Information

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.
2. View the overall status of Deep Discovery Director registration and server connection and view other summary information.

The Deep Discovery Director screen displays the following information:

TABLE 9-3. Deep Discovery Director Fields

FIELD	INFORMATION
Registration status	The following appliance statuses can be displayed: • Not registered: The appliance is not registered to Deep Discovery Director. • Registered: The appliance is registered to Deep Discovery Director.
Last connected	The last time this appliance connected to Deep Discovery Director.
Host name	The host name of this appliance.
Server address	The Deep Discovery Director server address.
Port	The Deep Discovery Director port.
API key	The Deep Discovery Director API key.
Fingerprint (SHA-256)	The Deep Discovery Director fingerprint.
Connect using a proxy server	Selected if the appliance uses the system proxy settings to connect to Deep Discovery Director.

Unregistering from Deep Discovery Director

Follow this procedure to unregister from Deep Discovery Director or before registering to another Deep Discovery Director or to Apex Central.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.

2. Click **Unregister**.

The **Status** changes to **Not registered**.

Threat Intelligence Sharing

Deep Discovery Web Inspector can share threat intelligence data (such as suspicious URLs) with other products or services (for example, a Blue Coat ProxySG device) through the HTTPS web service.

Note

When Deep Discovery Web Inspector is registered to Apex Central or Deep Discovery Director, Deep Discovery Web Inspector does not include user-defined suspicious objects synchronized from Apex Central or Deep Discovery Director in the shared threat intelligence data.

Configuring Threat Intelligence Sharing Settings

Procedure

1. On the Deep Discovery Web Inspector management console, go to **Administration** > **Integrated Products/Services** > **Threat Intelligence Sharing**.

2. Select **Enable Threat Intelligence Sharing to allow integrated products/services to get information from Deep Discovery Web Inspector**.

3. (Optional) Under **Schedule Settings**, select **Enabled** for **Scheduled file generation** and configure the schedule settings.

4. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.

   Options include `High only`, `High and medium`, and `High, medium, and low`.

5. Click **Save**.

6. Under **General**, click **Generate Now**.

After the file generation is successfully, you can click the URL to download the threat intelligence data file to view the content.

7. Configure an integrated product/service (for example, a Blue Coat ProxySG device) to obtain threat intelligence data from Deep Discovery Web Inspector. For more information, see the documentation for the integrated product/service.

Log Settings

Deep Discovery Web Inspector maintains access and violation detection logs that can be sent to syslog servers.

Detection Syslog Server Profiles

Deep Discovery Web Inspector can send violation detection logs to up to three syslog servers after saving the logs to its database. You can add up to three detection syslog server profiles.

Only logs saved after enabling a syslog server will be sent to that server. Previous logs are excluded.

The Default Access Syslog Server Profile

Deep Discovery Web Inspector can send access logs to up to one syslog server. There is a default access syslog server profile that is built-in and is preconfigured with certain settings. It is disabled by default. You can use this profile to start sending access logs to a syslog server.

To send the access logs, you must configure the syslog server IP address and port and then enable the profile. Additionally, you can customize which access log entries are sent to the syslog server.

After access logs are sent to the syslog server, Deep Discovery Web Inspector deletes the original data.

Adding a Detection Syslog Server Profile

You can configure Deep Discovery Web Inspector to forward the appliance's violation detection logs to a syslog server.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Log Settings**.

   The **Log Settings** screen appears.

2. Click **Add Detection Syslog**.

   The **Add Syslog Server Profile** screen appears.

3. (Optional) Enable or disable the detection syslog server profile.

   A new profile is enabled by default.

4. Type a profile name.

5. Type the host name (FQDN) or IP address of the syslog server.

6. Type the port number.

7. Select the protocol to be used when transporting log content to the syslog server.

   - TCP
   - UDP
   - SSL

8. Select the format in which event logs should be sent to the syslog server.

   - **CEF**: Common Event Format (CEF) is an open log management standard developed by HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs.
   - **LEEF**: Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar. LEEF comprises an LEEF header, event attributes, and an optional syslog header.
   - **TMEF (Trend Micro Event Format)**: Trend Micro Event Format (TMEF) is a customized event format developed by Trend Micro and is used by Trend Micro products for reporting event information.

9. Click **Save**.

Editing Detection Syslog Server Profiles

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Log Settings**.

   The **Log Settings** screen appears.

2. Click a detection syslog server profile hyperlink.

   The **Edit Detection Syslog Server Profile** screen appears.

3. Make the required changes.

4. Click **Save**.

Modifying the Access Syslog Server Profile

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Log Settings**.

   The **Log Settings** screen appears.

2. Click the default access syslog server profile hyperlink.

   The **Edit Access Syslog Server Profile** screen appears.

3. Make the required changes.

Option	Description
Status	Enable or disable the access syslog server profile.
Profile name	Change the profile name.
Server address	Change the server address. If you change the address on the syslog server, you must enter the new server address in this field.
Port	Change the port.

Option	Description
	If you change the port on the syslog server, you must enter the new port in this field.
Protocol	A read-only field that is set to UDP.
Content format	You can specify that Deep Discovery Web Inspector send only certain access log content to the access syslog server. Use this field, to specify what log information that you want Deep Discovery Web Inspector to send. For information about content format parameters that you can specify, see *Access Syslog Server Profile - Content Format Parameters on page 9-71*.

Use the format shown in the following example when specifying parameters in the **Content format** field. Separate each entry with | (pipe):

{dst} | {src} | {upstream_size} | {downstream_size} | {policy_name} | {request} | {cat} | {act} | {user-agent}h | {local_addr}

4. Click **Save**.

Access Syslog Server Profile - Content Format Parameters

You can modify the **Content format** field in the **Access Syslog Server Profile** to customize which entries in the access logs are sent to the syslog server. Use the following configuration parameters when modifying this field.

Note

Configuration parameters that have the format `{text}h` represent keys that are HTTP headers, which are below the URL. HTTP headers are used by clients and servers to pass additional information with requests and responses.

TABLE 9-4. Access Syslog Server Profile - Content Format Parameters

KEY NAME	CONFIGURATION PARAMETERS	DESCRIPTION
recv_request_begin	{recv_request_begin}	The time (UTC) that the first package in the request was received.
recv_request_end	{recv_request_end}	The time (UTC) that the last package in the request was received.
send_request_begin	{send_request_begin}	The time (UTC) that the first package in the request was sent.
send_request_end	{send_request_end}	The time (UTC) that all packages in the request were sent.
recv_response_begin	{recv_response_begin}	The time (UTC) that the first package in the response was received.
recv_ response _end	{recv_response_end}	The time (UTC) that all packages in the response were received.
send_response_begin	{send_response_begin}	The time (UTC) that the first package in the response was sent.
send_response_end	{send_response_end}	The time (UTC) that all packages in the response were sent.
handle_time	{handle_time}	The time (milliseconds) it took for Deep Discovery Web Inspector to handle one transaction.
request_handle_time	{request_handle_time}	The time (milliseconds) it took for Deep Discovery Web Inspector to handle the request for one transaction.

Key Name	Configuration Parameters	Description
response_handle_time	{response_handle_time}	The time (milliseconds) it took for Deep Discovery Web Inspector to handle the response for one transaction.
refer	{referer}h	Key is HTTP header.
location	{location}h	Key is HTTP header.
user-agent	{user-agent}h	Key is HTTP header.
host	{host}h	Key is HTTP header.
content-length	{content-length}h	Key is HTTP header.
content-type	{content-type}h	Key is HTTP header.
x-forwarded-for	{x-forwarded-for}h	Key is HTTP header.
content-encoding	{content-encoding}h	Key is HTTP header.
accept-encoding	{accept-encoding}h	Key is HTTP header.
content-disposition	{content-disposition}h	Key is HTTP header.
x-requested-with	{x-requested-with}h	Key is HTTP header.
connection	{connection}h	Key is HTTP header.
proxy-connection	{proxy-connection}h	Key is HTTP header.
x-authenticated-user	{x-authenticated-user}h	Key is HTTP header.
method	{method}h	Key is HTTP header.
path	{path}h	Key is HTTP header.
scheme	{scheme}h	Key is HTTP header.
status_code	{status_code}h	Key is HTTP header.
log_type	{log_type}	Fixed value is 1, which means access log.

Key Name	Configuration Parameters	Description
company_id	{company_id}	Company ID Reserved, value is default
ad_domain	{ad_domain}	Active Directory domain Example: trendnet.org
user_name	{user_name}	Client IP Example: 10.204.171.200
group_name	{group_name}	Active Directory group name Example: sales
department	{department}	Active Directory department Example: commercial
device	{device}	Device Reserved, default null
app	{app}	Protocol channel Can be one of the following values: • 1: HTTP • 2: HTTPS • 3: HTTP2 • 4: FTP

Key Name	Configuration Parameters	Description
tls_version	{tls_version}	TLS version Can be one of the following values: • 0: None TLS • 1: SSLv3 • 2: TLSv1.0 • 3: TLSv1.1 • 4: TLSv1.2
size	{size}	Transport bytes by Deep Discovery Web Inspector, unit bytes Example: 15
dst	{dst}	Destination IP address of request Example: 54.148.125.151
src	{src}	Source IP address of request Example: 10.204.171.200
upstream_size	{upstream_size}	The upstream payload from Deep Discovery Web Inspector to server, unit bytes Example: 54
downstream_size	{downstream_size}	The downstream payload from server to Deep Discovery Web Inspector, unit bytes Example: 49
domain	{domain}	Domain Example: ca95-1.winshipway.com

Key Name	Configuration Parameters	Description
tech_type	{tech_type}	Detection type Example: 70
tech_sub_type	{tech_sub_type}	Detection sub-type Reserved, default 0
threat_type	{threat_type}	Threat type • 1: Ransomware • 2: C&C Callback • 3: Suspicious Malware • 4: Suspicious URLs • 5: Suspicious Documents • 6: Suspicious Scripts • 7: Malicious URL • 8: Malicious Content • 9: Suspicious Content • 10: Coin Miners
severity	{severity}	Risk level • 0: user defined • 1: low • 2: medium • 3: high • 4: Potential Threat
policy_name	{policy_name}	Policy name Example: test

Key Name	Configuration Parameters	Description
profile_name	{profile_name}	Profile name Reserved, currently displays as default
wrs_threshold	{wrs_threshold}	WRS threshold Value is set to 50
principal_name	{principal_name}	Principal name Reserved, default is null
request	{request}	URL Example: hxxp://ca95-1.winshipway.com/
cat	{cat}	URL category Example: Ransomware
app_name	{app_name}	Application name Reserved, default is null
wrs_score	{wrs_score}	WRS score Example: 81
malware_type	{malware_type}	Malware type Reserved, default 0
malware_name	{malware_name}	Malware name Example: Ransomware

Key Name	Configuration Parameters	Description
so_data	{so_data}	Suspicious object displayed on the Deep Discovery Web Inspector **Detections** page Can be one of the following types: • Domain • URL • Server IP • File SHA1
fname	{fname}	File name Example: a.txt
filehash	{filehash}	SHA1 Example: 0d3d4cdfff683b0c17843a889e867fe29095c3ac
act	{act}	Action Can be one of the following values: • allow • monitor • block • warning • analyzing
msg	{msg}	Log description Value is null
rt	{rt}	UTC timestamp Example: Oct 20 2017 17:15:57 GMT+00:00

Key Name	Configuration Parameters	Description
local_addr	{local_addr}	The Deep Discovery Web Inspector management console IP address.

Virtual Analyzer

Deep Discovery Web Inspector can send suspicious objects to Virtual Analyzer for further analysis.

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

- *Virtual Analyzer Overview on page 9-79*
- *Virtual Analyzer Status on page 9-81*
- *Virtual Analyzer Images on page 9-82*
- *Virtual Analyzer Network on page 9-87*
- *Virtual Analyzer Integration with Deep Discovery Analyzer on page 9-90*

Virtual Analyzer Overview

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH). Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

If you configure Deep Discovery Web Inspector to use the internal Virtual Analyzer server (the default), you must import Virtual Analyzer images before Deep Discovery Web Inspector can perform sandbox analysis. You can check the status of the internal Virtual Analyzer sandbox environment and view the table to understand the real-time status of Virtual Analyzer and the sandbox images.

As an alternative to using the internal Virtual Analyzer, you can configure Deep Discovery Web Inspector to use Deep Discovery Analyzer to perform suspicious object analysis.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation
- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.

Related information

↳ *Information about viewing and downloading Virtual Analyzer reports and investigative reports for detected suspicious objects.*

Suspicious Object Scanning

When an scannable object enters your network, Deep Discovery Web Inspector scans the object with a series of scan engines: URL Filtering, Network Content Inspection, Advanced Threat Scan, Predictive Web Pre-Filter, Script Analyzer, and TrendX Engine.

After scanning the object for suspicious characteristics, Deep Discovery Web Inspector correlates the results to either assign a risk level and immediately execute a policy action based on the risk level, or sends the object to Virtual Analyzer for further analysis.

If the object need be submitted to the sandbox for further analysis after these engines prefilter, Virtual Analyzer gathers security intelligence from several Trend Micro Smart Protection Network services to investigate the object's risk level.

Virtual Analyzer Status

The Virtual Analyzer **Status** tab provides information in the following sections:

- **Overall Status**: Whether Virtual Analyzer is running.
- **Image Table**: Shows the allocated instances, status (busy or idle), and the utilization information for each sandbox image.

The following table describes the Virtual Analyzer overall statuses.

TABLE 9-5. Virtual Analyzer Overall Statuses

STATUS	DESCRIPTION
Starting...	Virtual Analyzer is starting all sandbox instances.
Stopping...	Virtual Analyzer is stopping all sandbox instances.
Running	Virtual Analyzer is analyzing samples.
No images	No images have been imported into Virtual Analyzer.
Maintenance	Virtual Analyzer is increasing or decreasing the number of instances for one or more images.
Importing images...	Virtual Analyzer is importing an image.
Removing images...	Virtual Analyzer is removing one or more images.

The following table describes status and available information for each image.

TABLE 9-6. Image Status and Information Table

HEADER	DESCRIPTION
Image	Permanent image name
Instances	Number of deployed sandbox instances
Current Status	Distribution of idle and busy sandbox instances
Utilization	Overall utilization (expressed as a percentage) based on the number of sandbox instances currently processing samples

Related information

↳ *Viewing Virtual Analyzer Status*

Viewing Virtual Analyzer Status

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Status**.
2. View the overall status of Virtual Analyzer and view the summary information about existing Virtual Analyzer images.

Related information

↳ *Information about viewing and downloading Virtual Analyzer reports and investigative reports for detected suspicious objects.*

Virtual Analyzer Images

Virtual Analyzer does not contain any images by default. You must import an image before Virtual Analyzer can analyze samples.

Virtual Analyzer supports Open Virtualization Format Archive (OVA) files.

Note

Before importing custom images, verify that you have secured valid licenses for all included platforms and applications.

Use the Image Preparation Tool to check that an image has the correct virtual machine settings, supported platforms and required applications before importing the image to Virtual Analyzer. For details about the Image Preparation Tool, see the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

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 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 9-84*.
   - **HTTP or FTP server**

     See *Importing an Image from an HTTP or FTP Server on page 9-86*.

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.

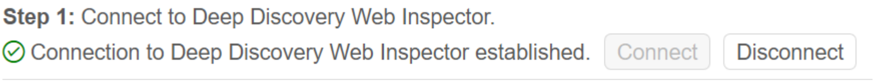
Procedure

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.

   Step 1: Connect to Deep Discovery Web Inspector.

   ✓ Connection to Deep Discovery Web Inspector 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 9-27*.

   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.

Deleting Virtual Analyzer Images

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Images**.
2. Select an image by selecting the box in the left column.
3. Click 🗑 **Delete**.

   The image is removed.

Modifying Instances

Procedure

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

   The **Modify Instances** screen appears.
3. Modify the instance number for any image.
4. Click **Save**.

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 9-89*.

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.

Option	Description
	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.
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 9-31*.

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.

System Maintenance

Go to the **Administration** > **System Maintenance** screen to perform the following operations:

- *Configuring Storage Maintenance on page 9-91*
- *Debug Logs on page 9-92*
- *Testing Network Connections on page 9-94*
- *Network Packet Capture on page 9-95*
- *Enabling/Disabling Bypass Mode on page 9-97*
- *Configuring Bypass/Redirect Policies on page 9-98*
- *Backing Up or Restoring a Configuration on page 9-104*
- *Power Off / Restart on page 9-109*

Configuring Storage Maintenance

Storage maintenance settings allow you to control the amount of log data that the system saves.

Procedure

1. Go to **Administration** > **System Maintenance** > **Storage Maintenance**.

2. Specify the log settings.

   - For **Delete logs older than**, specify the number of days to keep logs.

     Note

     The specified value must be between 3 and 366.

   - For **Delete logs when the total free disk space is equal to or lower than,** specify the disk space threshold (%) for automatic log deletion.

     The threshold value must be between 10 and 50.

     Deep Discovery Web Inspector purges 10% more than the specified percentage.

     Important

     Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering Deep Discovery Web Inspector to Deep Discovery Director, configure Deep Discovery Web Inspector to delete logs when the total free disk space is less than 20%.

3. Click **Save**.

Debug Logs

Deep Discovery Web Inspector creates debug logs that include information Trend Micro Support uses to troubleshoot problems.

You can export the following log levels:

- Error-level logs (for all IP addresses)
- Debug-level logs (for a single IP address or IP address range)

Configuring Debug Log Level

Configure the debug log level that Deep Discovery Web Inspector uses to save debug logs that you can provide to Trend Micro Support for troubleshooting a problem.

Important

If you change the log level, you must wait for Deep Discovery Web Inspector to collect a sufficient number of logs at the new log level before exporting/downloading the debug log.

Procedure

1. Go to **Administration** > **System Maintenance** > **Debug Logs**.

2. Change the log level.

   Options are `Error` (default) or `Debug`.

3. If log level is set to `Debug`, perform one of the following:

   - Enter an IP address in **IP**.

   - Enter an IP address range in **IP Range**.

4. Click **Save**.

   Changing the log level setting restarts the service.

Exporting and Downloading Debug Files

Export and download your debug file to provide information to Trend Micro Support for troubleshooting a problem.

Procedure

1. Go to **Administration** > **System Maintenance** > **Debug Logs**.

   - By default, the debug level is set to `Error`.

- If desired, you can set the debug level to `Debug` and specify an IP address or IP address range on which to collect debug-level logs.

  Changing the log level setting restarts the service. See *Configuring Debug Log Level on page 9-93*.

Important

If you change the log level, you must wait for Deep Discovery Web Inspector to collect a sufficient number of logs at the new log level before exporting/downloading the debug log.

2. If log level is set to `Debug`, perform one of the following:
   - Enter an IP address in **IP**.
   - Enter an IP address range in **IP Range**.
3. Click **Export**.
4. Wait for the export to complete. The time required depends on the amount of data to export.
5. Click **Download**.

What to do next

After downloading the debug file, you must delete the current export result before performing another export.

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

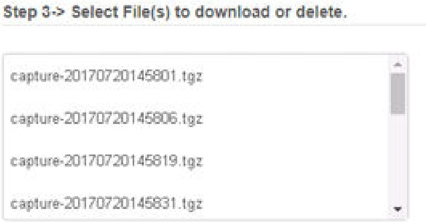
Network Packet Capture

You can use the network packet capture to provide information to Trend Micro Support for troubleshooting a problem.

Choose a single or multiple network interfaces on which to simultaneously capture network packets and then start the capture. After enough time has elapsed to capture data, you can stop the capture. Deep Discovery Web Inspector automatically compresses the capture files. You can then download the compressed packet capture files for analysis.

The packet capture for each interface saves as an individual file using the naming convention of `capture-{interface}-{date:time}.pcap`. After the network packet capture completes, Deep Discovery Web Inspector automatically compresses all `.pcap` files for that capture and saves them in one compressed package file named `capture-{date}.tgz`. For example, if you perform a packet capture on the eth0 network interface on July 27, 2017, the capture file is named `capture-eth0-20170727082849.pcap` and the compressed file is named `capture-20170727082849.tgz`

The compressed file displays in the down-loadable list. You can either download or delete the compressed file.



Step 3-> Select File(s) to download or delete.

capture-20170720145801.tgz

capture-20170720145806.tgz

capture-20170720145819.tgz

capture-20170720145831.tgz

Once you download and uncompress the `.tgz` file, each individual `.pcap` file is available for examination.

Capturing Network Packets

Capture network packets to analyze traffic on selected interfaces or a single interface.

Procedure

1. Go to the **Administration** > **System Maintenance** > **Network Packet Capture**.

2. Select the appropriate interface(s) from the **Available** interfaces box and move them to the **Selected** interfaces box.

3. Click **Start Capture**.

   The capture begins.

4. After sufficient data is captured, click **Stop Capture**.

5. Select the files you want to download and click **Download**.

6. (Optional) You can delete any unneeded files by selecting them and clicking **Delete**.

Enabling/Disabling Bypass Mode

For Bridge Mode deployments, you can enable the Deep Discovery Web Inspector appliance for bypass mode, which allows traffic to bypass inspection as it traverses the appliance. Bypass mode can be used as a diagnostic tool and a fail-over mechanism to ensure that traffic continues flowing through the Deep Discovery Web Inspector appliance during software failure or system upgrade. After issues are corrected or upgrade completed, you can disable bypass mode so that traffic will again be inspected by Deep Discovery Web Inspector.

Bypass mode protects from unexpected events that block web traffic, including the following:

- Scanner is unavailable
- OS kernel crashes
- System powers off

CAUTION!

Do not change the bypass mode setting if you are unsure of the impact to Deep Discovery Web Inspector functionality. Contact Trend Micro Technical Support for assistance if needed.

Procedure

1. Go to **Administration** > **System Maintenance** > **Bypass Mode**.
2. Perform the appropriate action:
    - To enable bypass mode and allow traffic to pass through the device without inspection, turn the option **On**.
    - To disable bypass mode and allow traffic to be inspected, turn the option **Off**.

      If set to **Off** or the device is down, traffic will pass through the device without inspection.

   After you change the bypass status, traffic through the Deep Discovery Web Inspector appliance is temporarily disrupted for a maximum of about 5 seconds. As most browsers and applications have TCP retransmission mechanisms, impact to the end user is limited.

Configuring Bypass/Redirect Policies

You can configure bypass/redirect policies to control how traffic is managed as it traverses the Deep Discovery Web Inspector appliance.

By default, all traffic is scanned according to configured scan policies and HTTPS inspection policies. However, you can use bypass/redirect policies to specify that some traffic is redirected to the scan daemon of Deep Discovery Web Inspector while other traffic bypasses scanning and traverses straight through the appliance to the endpoint.

Note

Bypass/redirect policies work only in bridge mode. In proxy mode, bypass/redirect policies do not work.

Types of Policies

You can configure the following types of policies:

- **Bypass**

Bypass traffic based on source IP addresses, destination IP addresses, or HTTPS domains.

All traffic is scanned according to scan and HTTPS inspection policies except for traffic that matches source IP addresses, destination IP addresses, or HTTPS domains configured in the bypass policy.

You can use a bypass policy to exclude traffic from certain devices that do not require scanning (such as printers) or that you do not want scanned.

- **Redirect**

  Redirect traffic based on source or destination IP addresses or source or destination MAC addresses.

  Traffic is scanned only for traffic that matches source or destination IP addresses or sources or destination MAC addresses configured in the redirect policy. All other traffic is bypassed with no scanning.

  You can use a redirect policy when most traffic that you want scanned comes only from or is destined to certain devices (such as gateways and routers).

Bypass/Redirect Policies Priorities and Precedence

You can configure policies to control how traffic is managed as it traverses the Deep Discovery Web Inspector appliance. You can have one bypass policy with multiple entries and one redirect policy with multiple entries. You should understand Deep Discovery Web Inspector priorities and precedence in evaluating bypass/redirect policies.

- Bypass policies are higher priority than redirect policies. If traffic matches both a bypass policy and a redirect policy, the bypass policy takes precedence and is used to evaluate the traffic.
- The bypass entries are evaluated in order. When a network packet is evaluated, the first matched entry is applied without evaluating following bypass entries.
- The redirect entries are evaluated in order. When a network packet is evaluated, the first matched entry is applied without evaluating following redirect entries.

Example: Deep Discovery Web Inspector is configured with both a bypass policy and a redirect policy. Traffic enters Deep Discovery Web Inspector from source IP address 10.10.10.10:

Bypass policy:

```
Source IP:
10.10.10.10
10.10.10.0/24
```

Redirect policy:

```
Source IP:
10.10.10.0/24
```

The source IP address matches the first entry in the bypass policy and is used for evaluation. The source address also matches the entry in the redirect policy. Since the bypass policy takes priority, traffic from 10.10.10.10 bypasses scanning.

Managing Bypass/Redirect Policies

Go to **Administration** > **System Maintenance** > **Bypass/Redirect Policy** to perform any of the following tasks to manage policies.

Procedure

- Click on the **Bypass** tab to view information about the existing bypass policy configuration.
- Click on the **Redirect** tab to view information about the existing redirect policy configuration.
- Add entries to the bypass or redirect policies.
- Delete existing entries from the bypass or redirect policies.
- Click **Import/Export Bypass** or **Import/Export Redirect** to export or import a copy of the defined bypass/redirect policies.

Configuring a Redirect Policy

When a redirect policy is configured and traffic matches an entry in the policy, Deep Discovery Web Inspector scans the matching network traffic for a match to scan policies and HTTPS inspection policies. You can configure redirect policies to match traffic based on the following:

- Source IP addresses
- Source MAC addresses
- Destination IP addresses
- Destination MAC addresses

Note

If both a redirect policy and a bypass policy are configured, you should understand the priority and precedence rules that Deep Discovery Web Inspector uses for evaluating traffic. See *Bypass/Redirect Policies Priorities and Precedence on page 9-99*.

Procedure

1. Go to **Administration** > **System Maintenance** > **Bypass/Redirect Policy** > **Redirect**.

2. Specify the redirect settings.

Option	Description

Add Source IP Address	Add one or more source IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Source IP Address**.
	You can add an IP address entry using any of the following formats:
	`10.10.10.10`
	`10.1.1.0/24`
	`192.168.1.1-192.168.1.5`

Option	Description

Add Destination IP Address	Add one or more destination IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Destination IP Address**.
	You can add an IP address entry using any of the following formats:
	`10.10.10.10`
	`10.1.1.0/24`
	`192.168.1.1-192.168.1.5`

Add Source MAC Address	Add one or more source MAC address entries, one entry at a time, by adding an MAC address entry and then clicking **Add Source MAC Address**.
	You can add a MAC address entry using any of the following formats:
	`01-23-45-67-89-ab`
	`01:23:45:67:89:ac`
	`0123.4567.89ad`

Add Destination MAC Address	Add one or more destination MAC address entries, one entry at a time, by adding an MAC address entry and then clicking **Add Destination MAC Address**.
	`01-23-45-67-89-ab`
	`01:23:45:67:89:ac`
	`0123.4567.89ad`

3. Click **Save**.

Configuring a Bypass Policy

When a bypass policy is configured and traffic matches an entry in the policy, Deep Discovery Web Inspector bypasses network traffic scanning of that traffic and sends the traffic straight to the end point. You can configure bypass policies to match traffic based on the following:

- Source IP addresses

- Destination IP addresses
- HTTPS domains

Note

Deep Discovery Web Inspector first evaluates matches in the Source IP address and Destination IP address bypass lists, then evaluates matches in the HTTPS domain bypass list (by comparing destination IP addresses of traffic with all IP addresses of this domain name), if any of the entries in the bypass lists are matched, traffic is bypassed.

An IP address might be associated with multiple domain names. In this case, Deep Discovery Web Inspector bypasses all the matching domains.

Note

If both a redirect policy and a bypass policy are configured, you should understand the priority and precedence rules that Deep Discovery Web Inspector uses for evaluating traffic. See *Bypass/Redirect Policies Priorities and Precedence on page 9-99*.

Procedure

1. Go to **Administration** > **System Maintenance** > **Bypass/Redirect Policy** > **Bypass**.
2. Specify the bypass settings.

Option	Description

Add Source IP Address	Add one or more source IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Source IP Address**.
	You can add an IP address entry using any of the following formats:
	`10.10.10.10`
	`10.1.1.0/24`
	`192.168.1.1-192.168.1.5`

OPTION	DESCRIPTION

Add Destination IP Address	Add one or more destination IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Destination IP Address**.
	You can add an IP address entry using any of the following formats:
	`10.10.10.10`
	`10.1.1.0/24`
	`192.168.1.1-192.168.1.5`

Add HTTPS Domain	Add one or more HTTPS domain entries, one entry at a time, by adding a domain name entry and then clicking **Add HTTPS Domain**.
	You can use wildcards when adding entries (* and ?). The domain prefix `https://` is insensitive and should not be included in the input for matching.
	`test?.example.com`
	`example.com`
	`*.example2.com`

3. Click **Save**.

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 9-7. 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)

Screen	Tab
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
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 9-105*.

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 9-105*.

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.

Power Off / Restart

The **Power Off / Restart** screen provides options to power off or restart the Deep Discovery Web Inspector appliance and its associated services.

Restarting Deep Discovery Web Inspector

Procedure

1. Go to **Administration** > **System Maintenance** > **Power Off/Restart**.
2. Click **Restart**.
3. Click **Proceed**.
4. At the confirmation dialog box, choose the appropriate action.

OPTION	DESCRIPTION
Restart	Click to restart the appliance.
Cancel	Click to cancel the restart operation.

Powering Off Deep Discovery Web Inspector

Procedure

1. Go to **Administration** > **System Maintenance** > **Power Off/Restart**.

2. Click **Power off**.

3. Click **Proceed**.

4. At the confirmation dialog box, choose the appropriate action.

OPTION	DESCRIPTION
Power Off	Click to power off the appliance.
Cancel	Click to cancel the power off operation.

Audit Logs

You can view details about configuration changes made under the **Policy**, **Administration**, and **Alerts/Reports** menus. Additionally, all export operations are recorded in the audit log, such as exporting all detections on **Detections** > **All Detections** > **Export All**. You can also view information about user access and other events, such as user log on and password changes, that occurred when using the Deep Discovery Web Inspector management console.

Note

Deep Discovery Web Inspector records the behavior, even if the behavior is failed. For example, if a log on fails, it is recorded in one audit log.

Viewing Audit Logs

You can view details about user access, configuration changes, and other events that occurred when using the Deep Discovery Web Inspector management console.

See *Audit Logs on page 9-110*.

Procedure

1. Go to **Administration** > **Audit Log**.

2. (Optional) Select a time period from the drop-down list.

   Options: last 4 hours, last 24 hours, last 7 days, last 30 days, last 90 days

3. (Optional) Enter a value and click on the **Search** icon to filter the audit log results.

   You can search for values in the `Source`, `IP Address`, and `Description` display fields.

4. View the audit log results.

   The following table describes the information available in the audit log.

Field	Description
Log Date	The time the log entry was recorded.
Source	The user account who performed the task.
IP Address	The IP address of the end point used to access the management console.
Description	The log event description.

5. (Optional) Click **Export** to save the audit log records as a `csv` file to a local computer of network folder.

   You can export a maximum of 50,000 log entries.

Accounts / Contacts

Deep Discovery Web Inspector uses role-based administration to grant and control access to the management console where they can perform administrative tasks.

To use role-based administration, you create custom accounts and assign a specific role to each account. A role defines the level of access to the management console.

By creating custom accounts and assigning specific management console privileges to the accounts, you can present account users with only the tools and permissions necessary to perform specific tasks.

Additionally, as part of contacts administration, you can configure a list of recipients in the contact list. The contact list is used by default when sending alert notifications and reports.

Managing Accounts

Deep Discovery Web Inspector has a default administrator account (admin) that has full administrative access. The default administrator account can perform all tasks, including adding new administrator accounts.

Accounts assigned the administrative role can create additional accounts and assign these accounts the **Administrator** role or the **Operator** role. Administrators can delegate tasks to different administrators and operators to reduce bottlenecks in Deep Discovery Web Inspector administration.

Administrator accounts can additionally edit or delete existing accounts.

You can create local user accounts or you can add Active Directory users to Deep Discovery Web Inspector accounts.

Account Role Classifications

ROLE	DESCRIPTION
Administrator	Users have complete administrative access to the features and settings contained in the menu items. • **Dashboard**: Full access • **Detections**: Full access • **Policy**: Full access • **Alerts / Reports**: Full access • **Administration**: Full access

Role	Description
Operator	Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications. • **Dashboard**: Full access • **Detections**: Full access • **Policy**: No access • **Alerts / Reports**: Read-only • **Administration**: No access

Note

All account roles can access **Help**.

Adding Local User Accounts

You can add local user accounts to provide role-based access to the Deep Discovery Web Inspector management console and to receive reports or notifications from Deep Discovery Web Inspector.

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click **Add**.

   The **Add/Edit Account** screen appears.
3. Toggle the **Status** of this account.
4. Select **Local user** from the **User type** drop-down list.
5. Specify the account user name.
6. Enter the password and confirm it.
7. Under **Permission**, select a **Role** for this account.

The role determines the level of access this account has. Valid options are **Administrator** and **Operator**.

Account Role Classifications on page 9-112

8. Click **Save**.

   The new account is added to the **Accounts** list.

Adding Active Directory User Accounts

You can add Microsoft Active Directory user accounts to provide role-based access to the Deep Discovery Web Inspector management console and to check reports or notifications from Deep Discovery Web Inspector.

Note

You must configure Microsoft Active Directory Services settings on Deep Discovery Web Inspector before you can add an Active Directory user account.

See *Active Directory Services on page 9-44*.

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.

2. Click **Add**.

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

3. Toggle the **Status** of this account.

4. Select **Active Directory user** from the **User type** drop-down list.

5. Type a portion of the Common Name in **User name**.

   Search content should be four characters or longer.

   Use the following format for Active Directory input for **User name**: User Principal Name (username@domain)

When adding accounts, you can choose users from multiple Active Directory domains, provided those domains are added to the Deep Discovery Web Inspector appliance's Active Directory Services.

Do not press **Enter** before selecting the user account. Use the drop down menu to select the user.

Matching user accounts are displayed in the drop-down list.

Note

User accounts are not displayed in the results table under the following circumstances:

- The user account's User Principal Name (UPN) is not specified on the Active Directory server.
- The user account is disabled on the Active Directory server.

---

6. Select the Active Directory user account to add.

7. Under **Permission**, select a **Role** for this user.

   The role determines the level of access. Valid options are **Administrator** and **Operator**.

   Account Role Classifications on page 9-112

8. Click **Save**.

   The new user account is added to the **Accounts** list.

Editing Accounts

You can edit an account's settings, including the account name and password. You can also change the account's role if you need to adjust the permissions for that account because of organizational changes.

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

Deleting Accounts

Delete accounts to adjust settings for a role revision or other organizational changes.

> **Note**
>
> You can only delete custom accounts. You cannot delete the default Deep Discovery Web Inspector administrator account.

Procedure

1. Go to **Administration** > **Accounts / Contacts** > **Accounts**.
2. Select the account to remove.
3. Click 🗑 **Delete**.
4. At the confirmation message, click **OK**.

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**.

Managing Contacts

You can add or remove recipient email addresses on the contacts page. Contacts added to this list are sent emails 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**.

Related information

↳ *Configuring Alert Notifications*
↳ *Scheduling Reports*

License

For information about managing your product license, see:

Licensing and Maintenance on page 10-1

About Deep Discovery Web Inspector

You can use the **About** screen in **Help** > **About** to view the firmware version and other product details.

Chapter 10

Licensing and Maintenance

Topics include:

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

Typically, 90 days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

https://olr.trendmicro.com/registration/

Activation Codes

Use a valid Activation Code to enable your product. A product will not be operable until activation is complete. An Activation Code has 37 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

If you received a Registration Key instead of an Activation Code, use it to register the product at:

https://olr.trendmicro.com/registration/

A Registration Key has 22 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxx-xxxx-xxxx

After registration, your Activation Code is sent via email.

Product License Description

The following table describes your product license. For information about viewing the product license, see *Viewing Your Product License on page 10-4*.

ITEM	DESCRIPTION
Product Details	
Product	The product name is Deep Discovery Web Inspector-<module name>. The value for <module name> can be either 510 or 1100. For example: Deep Discovery Web Inspector-510
Version	The product version is associated with the Activation Code and product license. Knowing the product version is helpful for troubleshooting issues.
License Details	
Activation code	The Activation Code has 37 characters (including the hyphens) and appears as follows: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx For details, see *Activation Codes on page 10-2*.
Type	The license type includes full and evaluation licenses. The Maintenance Agreement defines the available license type.
Seats number	The number of license seats purchased with this product.
Status	The current state of your product license. For information about the product license statuses, see *Product License Status on page 10-3*.
Expires on	The date that the license expires.

Product License Status

Your product license status changes from when you first acquire the product to when you must renew the license. Some of these statuses require intervention in order to maintain all product functionality. You can evaluate the product without activating a product license.

Status	Description
Activated	Deep Discovery Web Inspector has full product functionality and component updates for the license period. Technical Support is available based on the Maintenance Agreement.
In Grace Period	Deep Discovery Web Inspector is activated and has full product functionality for a limited time during the grace period.
Inactivated	Technical support and component updates are not available. All other Deep Discovery Web Inspector functionality is available.
Expired	The license is no longer valid. After the grace period lapses, product functionality is limited. • For evaluation licenses, component updates are not available. Scanning is maintained with outdated components. • For full licenses, technical support and component updates are not available. Scanning is maintained with outdated components. ⚠ **WARNING!** Outdated components significantly reduce product detection capabilities.

Viewing Your Product License

Procedure

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

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 10-4*.

Chapter 11

Technical Support

Learn about the following topics:

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

Appendices

Appendices

Appendix A

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 A-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 A-3*.

configure deploy reset

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-7. configure network

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

configure network basic

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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>

<table>
<tr><td><b>View</b></td><td>Privileged</td></tr>
<tr><td><b>Parameters</b></td><td><b>&lt;ip&gt;</b>: Destination IP address or network ID
<b>&lt;mask&gt;</b>: Network mask</td></tr>
<tr><td colspan="2"><b>Example</b>:</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

configure network redirect scan ip destination del

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

<table>
<tr><td colspan="2">Deletes a redirect scan policy by specifying a destination IP address or network ID.</td></tr>
<tr><td colspan="2"><b>Syntax</b>:
configure network redirect scan ip destination del <ip> <mask&gt;</td></tr>
<tr><td><b>View</b></td><td>Privileged</td></tr>
<tr><td><b>Parameters</b></td><td><b>&lt;ip&gt;</b>: Destination IP address or network ID
<b>&lt;mask&gt;</b>: Network mask</td></tr>
<tr><td colspan="2"><b>Example</b>:</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

configure network redirect scan mac

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-48. enable

Enters privileged mode where privileged commands are run.	
Syntax: `enable`	
View	Normal
Parameters	None
Example:	
To enter privileged mode: `enable`	

exit

Table A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-56. restart service

Command family restarts system services for the Deep Discovery Web Inspector appliance.	
Syntax: `restart service`	
View	Privileged

restart service product

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-70. show network

Command family displays various Deep Discovery Web Inspector network information.	
Syntax: `show network`	
View	Normal

show network arp

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-97. show system

Command family displays system information for the Deep Discovery Web Inspector appliance.	
Syntax: `show system`	
View	Normal

show system date

TABLE A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-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 A-107. start service

Command family starts system services for the Deep Discovery Web Inspector appliance.	
Syntax: `start service`	
View	Privileged

start service product

TABLE A-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 A-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 A-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 A-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 A-112. stop service

Command family stops system services for the Deep Discovery Web Inspector appliance.	
Syntax: `stop service`	
View	Privileged

stop service product

TABLE A-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 A-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 A-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`

Appendix B

SNMP Object Identifiers

Topics include:

SNMP Query Objects

TABLE B-1. productVersion

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.1.1
Object name	productVersion
Description	Returns the Deep Discovery Web Inspector version.

TABLE B-2. productBuild

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.1.2
Object name	productBuild
Description	Returns the Deep Discovery Web Inspector build number.

TABLE B-3. Product hotfix

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.1.3
Object name	productHotfix
Description	Returns the Deep Discovery Web Inspector hotfix number.

TABLE B-4. patternIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.2.1.1
Object name	patternIndex
Description	Returns the pattern index.

TABLE B-5. patternID

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.2.1.2
Object name	patternID
Description	Returns the pattern ID.

TABLE B-6. patternName

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.2.1.3
Object name	patternName
Description	Returns the pattern name.

TABLE B-7. patternVersion

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.2.1.4
Object name	patternVersion
Description	Returns the pattern version.

TABLE B-8. virtualAnalyzerQueue

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.3.1
Object name	virtualAnalyzerQueue
Description	Returns the Virtual Analyzer queue number.

TABLE B-9. ifIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.4.1.1

ITEM	DESCRIPTION
Object name	ifIndex
Description	Returns the interface index.

TABLE B-10. ifDescr

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.4.1.2
Object name	ifDescr
Description	Returns the interface description.

TABLE B-11. ifReceiveThroughput

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.4.1.3
Object name	ifReceiveThroughput
Description	Returns the interface receiving throughput.

TABLE B-12. ifTransmitThroughput

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.1.4.1.4
Object name	ifTransmitThroughput
Description	Returns the interface transmitting throughput.

TABLE B-13. hwMonitorNumber

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.3.1.1
Object name	hwMonitorNumber
Description	Count of number of conceptual rows in hwMonitorTable

Table B-14. hwMonitorLastChange

Item	Description
OID	.1.3.6.1.4.1.6101.3006.3.1.2
Object name	hwMonitorLastChange
Description	The value of system time when a conceptual row was added or deleted from this table

Table B-15. hwMonitorIndex

Item	Description
OID	.1.3.6.1.4.1.6101.3006.3.1.3.1.1
Object name	hwMonitorIndex
Description	A unique identifier that does not persist across management restarts

Table B-16. tmSubsystemType

Item	Description
OID	.1.3.6.1.4.1.6101.3006.3.1.3.1.2
Object name	tmSubsystemType
Description	Hardware component reporting environmental state

Table B-17. tmHardwareStatus

Item	Description
OID	.1.3.6.1.4.1.6101.3006.3.1.3.1.3
Object name	tmHardwareStatus
Description	Last reported state of this component

TABLE B-18. tmMonitorDescription

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.3.1.3.1.4
Object name	tmMonitorDescription
Description	Human readable description of this event

TABLE B-19. tmHardwareTime

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.3.1.3.1.5
Object name	tmHardwareTime
Description	Value of system time when tmHardwareStatus was obtained

SNMP Traps

TABLE B-20. updateSuccessNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.1
Object name	updateSuccessNotification
Description	Notification to indicate that a component update or roll back was successful.

TABLE B-21. updateFailedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.2
Object name	updateFailedNotification
Description	Notification to indicate that a component update or roll back was unsuccessful.

TABLE B-22. cpuUsageNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.3
Object name	cpuUsageNotification
Description	Notification to indicate that the CPU usage level has reached the maximum threshold.

TABLE B-23. memUsageNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.4
Object name	memUsageNotification
Description	Notification to indicate that the memory usage level has reached the maximum threshold.

TABLE B-24. diskSpaceNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.5
Object name	diskSpaceNotification
Description	Notification to indicate that the available disk space is less than the minimum threshold.

TABLE B-25. serviceStoppedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.6
Object name	serviceStoppedNotification
Description	Notification to indicate that a service has stopped and cannot be restarted.

TABLE B-26. atpDetectNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.7
Object name	atpDetectNotification
Description	Notification to indicate that the number of advanced threat detections on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-27. ransomwareDetectNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.8
Object name	ransomwareDetectNotification
Description	Notification to indicate that the number of ransomware detections on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-28. cccDetectNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.9
Object name	cccDetectNotification
Description	Notification to indicate that the number of C&C callbacks on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-29. licenseExpireNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.10
Object name	licenseExpireNotification
Description	Notification to indicate that the product license is about to expire or has expired.

TABLE B-30. ntpFailedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.0.11
Object name	ntpFailedNotification
Description	Notification to indicate that time synchronization with an NTP server is not successful.

TABLE B-31. updateSuccessMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.1
Object name	updateSuccessMsg
Description	Message to indicate that a component update or roll back was successful.

TABLE B-32. updateFailedMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.2
Object name	updateFailedMsg
Description	Message to indicate that a component update or roll back was unsuccessful.

TABLE B-33. cpuUsageMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.3
Object name	cpuUsageMsg
Description	Message to indicate that the CPU usage level has reached the maximum threshold.

TABLE B-34. memUsageMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.4
Object name	memUsageMsg
Description	Message to indicate that the memory usage level has reached the maximum threshold.

TABLE B-35. diskSpaceMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.5
Object name	diskSpaceMsg
Description	Message to indicate that the available disk space is less than the minimum threshold.

TABLE B-36. serviceStoppedMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.6
Object name	serviceStoppedMsg
Description	Message to indicate that a service has stopped and cannot be restarted.

TABLE B-37. atpDetectMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.7
Object name	atpDetectMsg
Description	Message to indicate that the number of advanced threat detections on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-38. ransomwareDetectMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.8
Object name	ransomwareDetectMsg
Description	Message to indicate that the number of ransomware detections on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-39. cccDetectMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.9
Object name	cccDetectMsg
Description	Message to indicate that the number of C&C callbacks on hosts in the specified network groups reaches the threshold during the specified time period.

TABLE B-40. licenseExpireMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.10
Object name	licenseExpireMsg
Description	Message to indicate that the product license is about to expire or has expired.

TABLE B-41. ntpFailedMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.11
Object name	ntpFailedMsg
Description	Message to indicate that time synchronization with an NTP server is not successful.

TABLE B-42. coinMinersDetectMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3006.2.1.12
Object name	coinMinersDetectMsg
Description	Message to indicate that the number of coin miner detections on hosts in the specified network groups reaches the threshold during the specified time period.

SNMP Registration Objects

OID	DESCRIPTION
.1.3.6.1.4.1.2021	UC Davis
.1.3.6.1.4.1.6101	Trend Micro, Inc.
.1.3.6.1.6.3.1.1.5.1	SNMPv2-MIB MIB
.1.3.6.1.4.1.8072	NET-SNMP-AGENT-MIB
.1.3.6.1.4.1.6101.999	TMCM
.1.3.6.1.4.1.6101.3001	TMTM
.1.3.6.1.4.1.6101.3006	Deep Discovery Web Inspector

Index

TREND MICRO™

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: APEM28796/190819