Trend Micro™

Deep Discovery Inspector

6.8 Service Pack 2

Administrator's Guide

Breakthrough Protection Against APTs and Targeted Attacks

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

Trend Micro, the Trend Micro t-ball logo, Deep Discovery, Apex Central, and Trend Vision One are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2025. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM6810069/251027

Release Date: November 2025

Protected by U.S. Patent No.: 8595840; 8925074; 7707635; 8505094

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.

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 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 Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 1: Introduction

About Deep Discovery Inspector 1-2

What's new 1-2

Features and benefits 1-3

- Threat management capabilities 1-3
- APT Attack Sequence 1-4
- Host Severity 1-5
- Advanced threat scan engine 1-8
- Virtual analyzer 1-8

Chapter 2: Get started

Preconfiguration console 2-2

Get started tasks 2-2

Management console 2-3

- Management console requirements 2-4
- Opening the management console 2-5
- Management console account passwords 2-6
  - Changing an administrator account password 2-7
  - Changing a viewer account password 2-8
- Logging on with single sign-on 2-9

Network 2-9

- Configuring the appliance IP settings 2-9
  - Network format rules 2-12
- Managing network interface ports 2-14

Chapter 3: Dashboard

Dashboard overview 3-2

Tabs 3-2

- Tab tasks 3-3

Adding/modifying tabs 3-3
Moving tabs 3-4
Closing/deleting tabs 3-4

Widgets 3-5

Widget tasks 3-5
Adding widgets to the dashboard 3-6

About Deep Discovery Inspector widgets 3-6

Deep Discovery Inspector widgets 3-7

Deep Discovery Inspector default widget tabs 3-10

Summary 3-10
Threats at a glance 3-10
Top affected hosts 3-12
Threat summary 3-12
Malicious scanned network traffic 3-12
Scanned traffic by protocol type 3-13
Threat monitoring 3-13
Threat geographic map 3-13
Viewing information on the threat geographic map 3-14
Monitored network traffic in past 30 days 3-15
Virtual analyzer status 3-15
Top hosts with virtual analyzer detections 3-15
Top malicious sites analyzed by virtual analyzer 3-16
Top suspicious files 3-16
Virtual analyzer 3-17
Top trends 3-19
Top disruptive applications 3-19
Top malicious urls detected 3-19
System status 3-20
CPU usage 3-20
Disk usage 3-20
Memory usage 3-20

Optional widgets 3-20

All scanned traffic 3-21
Malicious real-time network traffic 3-21

Real-time scanned traffic 3-21
Top exploited hosts 3-22
Top grayware-infected hosts 3-22
Top malicious content detected 3-22
Top malware-infected hosts 3-23
Top suspicious behaviors detected 3-23

Chapter 4: Detections

About the detections screen 4-2

Affected hosts 4-3

Display options and search filters 4-3
Viewing affected hosts 4-5
Viewing affected hosts - host details 4-9
Viewing affected hosts - detection details 4-12
Affected hosts - detection details 4-14
Connection details 4-14
Affected Hosts - Detection Details - File Analysis Result 4-21
Affected Hosts - Detection Details - Suspicious Object and Related File Analysis Result 4-24
Affected Hosts - Detection Details - Suspicious Object Information 4-24
Affected Hosts - Detection Details - Related Analyzed File Information 4-25
Mitigation suggestions 4-26
Affected hosts advanced search filter 4-27
About affected hosts advanced search filter 4-27
Adding an affected hosts advanced search filter 4-29
Editing an affected hosts saved search 4-30
Deleting an affected hosts saved search 4-32
Importing affected hosts saved searches 4-32
Exporting affected hosts saved searches 4-33
About affected hosts - host details advanced search filter 4-34
Adding an affected hosts - host details advanced search filter 4-40

Editing an affected hosts - host details saved search 4-42
Deleting an affected hosts - host details saved search 4-44
Importing affected hosts - host details saved searches 4-44
Exporting affected hosts - host details saved searches 4-45
C&C callback addresses 4-46
Viewing C&C callback addresses 4-46
Virtual analyzer suspicious objects 4-47
User-defined suspicious objects 4-49
Retro scan 4-50
Retro scan and the Smart Protection Network 4-51
Enabling retro scan 4-51
Retro scan screen 4-52
Retro scan report details screen 4-53
Disable retro scan 4-54
Disabling retro scan 4-54
All detections 4-55
Display options and search filters 4-55
Viewing all detections 4-57
Viewing all detections - detection details 4-61
All detections - detection details 4-63
All detections - detection details - connection details 4-63
All detections - detection details - detection information 4-65
All detections - detection details - connection summary 4-67
All detections - detection details - protocol information 4-67
All detections - detection details - file information 4-69

All detections - detection details - additional information 4-69
All detections - detection details - file analysis result 4-69
All detections - detection details - file analysis result - file information 4-70
All detections - detection details - file analysis result - YARA detections 4-71
All detections - detection details - file analysis result - notable characteristics 4-72
All detections - detection details - suspicious object and related file analysis result 4-72
All detections - detection details - suspicious object information 4-72
All detections - detection details - related analyzed file information 4-73
All detections - detection details - mitigation suggestions 4-74
All detections advanced search filter 4-75
Adding an all detections advanced search filter 4-81
Editing an all detections saved search 4-83
Deleting an all detections saved search 4-85
Importing all detections saved searches 4-85
Exporting all detections saved searches 4-86

Chapter 5: Reports

About reports 5-2
Scheduled reports 5-4
Schedules 5-5
Scheduling a report 5-6
Deleting a report schedule 5-7
On-demand reports 5-8
Generating an on-demand report 5-9
Deleting an on-demand report 5-11

Customization 5-11
Customizing reports 5-11

Chapter 6: Administration

Updates 6-2
Component updates 6-2
Components to update 6-2
Component update methods 6-4
Component update tasks 6-5
Manual updates 6-5
Performing manual updates 6-6
Scheduled updates 6-6
Update source 6-7
Configuring the update source 6-7
Product updates 6-8
Hot fixes / patches 6-9
Applying a hotfix or patch 6-9
Rolling back a hotfix or patch 6-11
Service packs / version upgrade 6-12
Applying a service pack or version upgrade 6-12
Clearing the browser cache 6-14
Notifications 6-15
Threat detection notifications 6-16
High risk hosts detections notifications 6-18
Adding to the high risk hosts detections notification exclusion list 6-20
Suspicious hosts detections notifications 6-21
High network traffic notifications 6-22
Unanalyzed sample detections notifications 6-24
Virtual analyzer detections notifications 6-26
Deny list notifications 6-27
Retro scan detections notifications 6-29
High tunneled domains notifications 6-30
Low network traffic notifications 6-31
Delivery options 6-33
Configuring email notification settings 6-33

Monitoring / scanning 6-34
Hosts / ports 6-34
Configuring hosts and ports 6-35
Threat detections 6-36
Configuring threat detections 6-36
Smart Protection 6-38
About Smart Protection Server 6-40
Setting up Smart Protection server 6-40
Managing the Smart Protection server list 6-41
Web Reputation 6-42
Configuring web reputation settings 6-42
Application filters 6-45
Configuring application filter settings 6-46
Deny list / allow list 6-47
Deny list / allow list format rules 6-48
Configure deny lists and allow lists 6-51
Configure deny lists and allow lists 6-52
Format rules for importing deny lists / allow lists 6-54
Exporting custom deny lists / allow lists 6-54
Importing custom deny lists / allow lists 6-55
Detection rules 6-56
Packet capture 6-58
Adding a packet capture rule 6-59
Detection exceptions 6-60
TLS traffic inspection 6-63
Inspection settings 6-65
Configuring tunneled domains 6-65
Certificate management 6-66
Trusted CA certificates 6-66
Signing certificate 6-67
Decryption policy 6-68
Virtual Analyzer 6-72
Types of virtual analyzer 6-72
Internal Virtual Analyzer configuration 6-73
External Virtual Analyzer Configuration 6-75
Sandbox as a Service Configuration 6-75

Trend Vision One — Sandbox Analysis configuration 6-76
File submissions 6-77
Certified safe software service 6-77
File submission rules 6-78
File submission rule types and criteria 6-79
File submission rules screen 6-83
Adding a file submission rule 6-83
Internal Virtual Analyzer 6-86
Sandbox management 6-86
Virtual Analyzer status 6-86
Virtual Analyzer images 6-87
Image preparation 6-87
Importing an image 6-88
Import an image using the Virtual Analyzer Image Import Tool 6-90
Modify instances 6-91
Modifying instances 6-91
Deleting instances 6-92
Archive passwords 6-92
Adding an archive password 6-93
Sandbox for macOS 6-93
YARA rules 6-94
Creating a YARA rule file 6-95
Adding a YARA rule file 6-97
Editing a YARA rule file 6-97
Deleting a YARA rule file 6-98
Exporting a YARA rule file 6-98
Network groups and assets 6-98
Adding network groups 6-99
Adding registered domains 6-101
Adding registered services 6-103
Synchronize network groups and assets from Trend Vision One 6-106
Importing/exporting configuration settings 6-107
Integrated products/services 6-108
Integrated Trend Micro products and services 6-108

Trend Vision One 6-109
Direct connection to Trend Vision One 6-110
Connection to Trend Vision One using a Service Gateway as a proxy 6-112
Disconnect Deep Discovery Inspector from Trend Vision One using Network Inventory 6-114
Service Gateway connection 6-114
Service Gateway services 6-116
Viewing enabled Service Gateway services 6-116
Smart Protection services 6-117
Component service updates 6-118
Disconnecting a Service Gateway 6-118
Apex Central 6-119
Apex Central components 6-120
Registering to Apex Central 6-121
Unregistering from Apex Central 6-123
Managing the connection with Apex Central 6-123
Deep Discovery Director 6-124
Connecting to Deep Discovery Director 6-124
Unregistering from Deep Discovery Director 6-126
Threat investigation center 6-127
Integrating threat investigation center 6-127
TXOne OT Defense Console 6-128
Configuring TXOne OT Defense Console 6-129
Threat intelligence sharing 6-130
Threat intelligence sharing configuration 6-130
Inline products and services 6-132
Trend Micro TippingPoint Security Management System (SMS) 6-132
Configure Trend Micro TippingPoint Security Management System (SMS) 6-133
Check Point Open Platform for Security (OPSEC) ... 6-136
Configuring Check Point Open Platform for Security (OPSEC) 6-137
Preconfiguring a security gateway 6-145
Configuring a secured connection 6-147

IBM Security Network Protection 6-151
Configuring IBM security network protection . 6-151
Palo alto panorama or firewalls 6-156
Configuring Palo Alto Panorama or firewalls ... 6-157
SAML Authentication 6-161
Service Provider Metadata and Certificate 6-162
Configuring Identity Provider Settings 6-163
Configuring Okta 6-164
Configuring Active Directory Federation Services .. 6-167
Configuring Endpoints for Single Sign-on through AD FS 6-169
Microsoft Active Directory 6-170
Configuring Microsoft Active Directory integration 6-171
Syslog 6-172
Adding a syslog server 6-173
System settings 6-175
Network 6-176
Network interface 6-176
Data and management ports 6-176
Inline ports 6-177
Proxy 6-178
Configure a proxy server 6-178
SMTP 6-179
Configuring SMTP settings 6-179
SNMP 6-180
Configuring SNMP trap mode 6-180
Configuring SNMP agent mode 6-181
HTTPS certificate 6-183
Generating an HTTPS certificate 6-183
Importing an HTTPS certificate 6-184
Time 6-185
Configuring time options 6-185
Session timeout 6-186
Configuring session timeout 6-186
Accounts 6-187
About accounts 6-187

User roles and menu item permissions 6-188
Adding a local account 6-191
Adding an Active Directory account 6-193
Adding a SAML account 6-194
Editing an account 6-196
Resetting an account password 6-197
Deleting an account 6-198
Unlocking an account 6-199

System logs 6-199

System maintenance 6-201

Storage maintenance 6-201
Performing storage maintenance 6-202
Performing product database maintenance 6-202
Configuring file size settings 6-202
Backup / restore 6-203
Back up file settings 6-204
Importing file settings 6-205
Restoring default settings 6-206
Power off / restart 6-207
Restarting Deep Discovery Inspector 6-207
Powering off Deep Discovery Inspector 6-208

Licenses 6-208

Activation codes 6-208
Product version 6-209
Deep Discovery Inspector license expiry 6-209
Activating or renewing licenses 6-210

Chapter 7: Troubleshoot

Frequently asked questions (FAQs) 7-2

FAQs - appliance rescue 7-2
FAQs - configuration 7-3
FAQs - detections 7-3
FAQs - installation 7-3
FAQs - upgrade 7-4
FAQs - virtual analyzer image 7-4

Troubleshooting 7-5
Slow management console response 7-5
Detections 7-6
No detections on all detections screen 7-6
"unregistered service" server displays in all detections query 7-7
Unknown IP addresses display on a screen 7-7
Known safe objects flagged as malicious 7-7
"database is corrupt" alert displays 7-8
Virtual analyzer 7-8
Cannot upload OVA 7-8
No virtual analyzer response to file submissions 7-8
Virtual analyzer images 7-9
The installation media does not start 7-9
"found new hardware" wizard 7-10
An image displays a blue screen 7-10
Cannot connect to network services 7-11
Diagnostics 7-11
Inline deployment and TLS inspection 7-12
Network connectivity issue 7-13
TLS connection issue 7-14

Chapter 8: Technical support

Troubleshooting resources 8-2
Using the support portal 8-2
Threat encyclopedia 8-2
Contacting Trend Micro 8-3
Speeding up the support call 8-3
Sending suspicious content to Trend Micro 8-4
Email Reputation Services 8-4
File Reputation Services 8-4
Web Reputation Services 8-5
Other resources 8-5
Download center 8-5

Appendices

Appendix A: Virtual analyzer supported file types

Appendix B: Settings replicated by Deep Discovery Director and Trend Vision One

Appendix C: TLS support for integrated products/services

Appendix D: Service addresses and ports

Index

Index IN-1

Preface

Preface

Learn more about the following topics:

- *Documentation on page 2*
- *Audience on page 3*
- *Document Conventions on page 3*

Documentation

The documentation set for Deep Discovery Inspector includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Inspector, and explanations on Deep Discovery Inspector concepts and features.
AWS Deployment Guide	The AWS Deployment Guide contains information about requirements and procedures for planning deployment, deploying, and troubleshooting Deep Discovery Inspector deployment on AWS.
Inline (LAN bypass) Network Interface Card Installation Guide	The Inline (LAN bypass) Network Interface Card Installation Guide contains information about requirements and procedures for installing an additional bypass network interface card on supported Deep Discovery Inspector appliances.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery 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.

Document	Description
Online Help	Web-based documentation that is accessible from the Deep Discovery Inspector management console. The Online Help contains explanations of Deep Discovery Inspector components and features, as well as procedures needed to configure Deep Discovery Inspector.
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: https://success.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

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

Audience

The Deep Discovery 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
- Database management
- Antivirus and content security protection

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
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

Chapter 1

Introduction

Learn about product features, capabilities, and security technology in the following topics:

- *About Deep Discovery Inspector on page 1-2*
- *Features and benefits on page 1-3*
- *Threat management capabilities on page 1-3*
- *APT Attack Sequence on page 1-4*
- *Host Severity on page 1-5*
- *Advanced threat scan engine on page 1-8*
- *Virtual analyzer on page 1-8*

About Deep Discovery Inspector

Deep Discovery Inspector is a third-generation threat management solution designed and architected to deliver breakthrough targeted attack and advanced threat visibility, insight, and control. Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports.

Trend Micro developed Deep Discovery Inspector to meet the requirements of G1000 organizations and government around the world. Deep Discovery Inspector integrates global intelligence and scanning technology to catch traditional signature-based threats and more sophisticated threats requiring heuristic analysis.

What's new

The following table describes the new features in Deep Discovery Inspector 6.8 Service Pack 2.

Feature	Description
New Deep Discover Inspector model	The new 550/1500 Deep Discovery Inspector hardware appliance models are now available.
Support for HASSH fingerprint identification	Deep Discovery Inspector can now identify HASSH fingerprints in SSH traffic for anomaly detection. The information is also sent to Trend Vision One as part of the telemetry data.
Centralized management from Trend Vision One	You can now use Network Inventory on Trend Vision One to configure the VLAN awareness setting on Deep Discovery Inspector.
Virtual Analyzer enhancements	Virtual Analyzer now supports Office 2024, allowing for threat analysis in a simulated Office 2024 environment.

Features and benefits

Deep Discovery Inspector offers sophisticated detection capabilities using multiple advanced detection engines to present detailed information about custom and signature-based threats passing through various network protocols. Deep Discovery Inspector detects targeted attacks and advanced threats, and helps remediate targeted attacks with automated processes.

Deep Discovery Inspector includes the following features:

- *Threat management capabilities on page 1-3*
- *APT Attack Sequence on page 1-4*
- *Host Severity on page 1-5*
- *Advanced threat scan engine on page 1-8*
- *Virtual analyzer on page 1-8*

Threat management capabilities

Deep Discovery Inspector detects and identifies evasive threats in real-time, and provides in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

TABLE 1-1. Threat Management Capabilities

CAPABILITY	DESCRIPTION
Expanded APT and targeted attack detection	Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom sandbox analysis. New discovery and correlation rules detect malicious content, communication, and behavior across every stage of an attack sequence.
Visibility, analysis, and action	Using an intuitive multi-level format, the Deep Discovery Inspector management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.

Capability	Description
High capacity platforms	Deep Discovery Inspector features a high-performance architecture that meets the demanding and diverse capacity requirements of large organizations. Deep Discovery Inspector features are useful for a company of any size, and are vital to larger organizations needing to reduce the risk of targeted attacks.

APT Attack Sequence

Targeted attacks and advanced persistent threats (APTs) are organized, focused efforts that are custom-created to penetrate enterprises and government agencies for access to internal systems, data, and other 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 1-2. 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.

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

Host Severity

In Deep Discovery Inspector, host severity is the impact on a host as determined from aggregated detections by Trend Micro products and services.

Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows you to prioritize and quickly respond.

Host severity is based on the aggregation and correlation of the severity of the events that affect a host. If several events affect a host and have no detected connection, the host severity will be based on the highest event severity of those events. However, if the events have a detected correlation, the host severity level will increase accordingly.

For example: Of five events affecting a host, the highest risk level is moderate. If the events have no correlation, the host severity level will be based on the moderate risk level of that event. However, if the events are

correlated, then the host severity level will increase based on the detected correlation.

The host severity scale consolidates threat information from multiple detection technologies and simplifies the interpretation of overall severity. You can prioritize your responses based on this information and your related threat response policies.

TABLE 1-3. Host Severity Scale

CATEGORY	LEVEL	DESCRIPTION
Critical Host exhibits behavior that **definitely** indicates host is compromised	10	Host shows evidence of compromise including but not limited to the following: • Data exfiltration • Multiple compromised hosts/servers
	9	Host exhibits an indication of compromise from APTs including but not limited to the following: • Connection to an IP address associated with a known APT • Access to a URL associated with a known APT • A downloaded file associated with a known APT • Evidence of lateral movement
	8	Host may exhibit the following: • A high severity network event • Connection to a C&C Server detected by Web Reputation Services • A downloaded file rated as high risk by Virtual Analyzer
Major Host is targeted by a known malicious behavior or attack and exhibits behavior that	7	Host may exhibit the following: • Inbound malware downloads; no evidence of user infection • An inbound Exploit detection

Category	Level	Description
likely indicates host is compromised	6	Host may exhibit the following: • Connection to a dangerous site detected by Web Reputation Services
	5	Host may exhibit the following: • A downloaded medium- or low-risk potentially malicious file with no evidence of user infection
	4	Host may exhibit the following: • A medium severity network event • A downloaded file rated as medium risk by Virtual Analyzer
Minor Host exhibits anomalous or suspicious behavior that may be benign or indicate a threat	3	Host may exhibit the following: • Repeated unsuccessful logon attempts or abnormal patterns of usage • A downloaded or propagated packed executable or suspicious file • Evidence of running IRC, TOR, or outbound tunneling software
	2	Host may exhibit the following: • A low severity network event • Evidence of receiving an email message that contains a dangerous URL • A downloaded file rated as low risk by Virtual Analyzer

Category	Level	Description
Trivial Host exhibits normal behavior that may be benign or indicate a threat in future identification of malicious activities	1	Host may exhibit the following: • An informational severity network event • Connection to a site rated as untested or to a new domain detected by Web Reputation Services • Evidence of a running disruptive application such as P2P

Advanced threat scan engine

Advanced Threat Scan Engine uses a combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks.

Major features include the following:

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

Virtual analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. 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 and STIX files that can be used in investigations.

Chapter 2

Get started

Learn about the Deep Discovery Inspector management console and basic appliance settings in the following topics:

- *Preconfiguration console on page 2-2*
- *Get started tasks on page 2-2*
- *Management console on page 2-3*
- *Network on page 2-9*

Preconfiguration console

The Deep Discovery Inspector Preconfiguration Console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Inspector management console.

For details, see the *Deep Discovery Inspector Installation and Deployment Guide*.

Get started tasks

Customize threat detection by configuring the following settings.

For information on the settings you need to configure, refer to the help topics for each step below.

Tip

In the management console, go to **Help** > **Setup Guide** to access an on-screen setup guide to help you through the steps below.

Procedure

1. Add **Network Groups**.

   For details, see *Adding network groups on page 6-99*.

2. Configure **Registered Domains**.

   For details, see *Adding registered domains on page 6-101*.

3. Configure **Registered Services**.

   For details, see *Adding registered services on page 6-103*.

4. (Optional) Configure **Proxy Settings**.

   For details, see *Configure a proxy server on page 6-178*.

5. Update components.

   For details, see *Performing manual updates on page 6-6*.

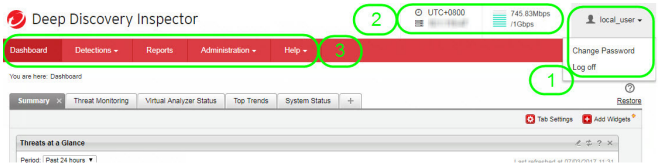
6. (Optional) Configure **TLS Traffic Inspetion**

   For details, see *Inspection settings on page 6-65*

Management console

Deep Discovery Inspector provides a built-in online management console for viewing system status, configuring and viewing threat detections and logs, running reports, administering Deep Discovery Inspector, updating components, and obtaining help.

The management console includes the following user interface elements:



#	UI Element	Description
1.	Account name and basic user account operations	Basic user account operations are located under the account name in the upper right corner of the management console screen and include the following: • Change Password **Note** The passwords of non-local accounts cannot be changed from the management console. • Log Off
2.	Appliance information at a glance	Appliance information at a glance includes the following: • Time zone • Appliance FQDN or IP address • Network traffic • Decrypted traffic (when TLS traffic inspection is enabled)
3.	Main screen tabs	The management console includes the following tabs: • Dashboard • Detections • Reports • Administration • Help

Management console requirements

The Deep Discovery Inspector management console supports the following web browsers:

- Google™ Chrome™

- Mozilla™ Firefox™
- Microsoft™ Edge

Recommended resolution: 1280x800 or higher

Opening the management console

Procedure

1. From a network workstation, open a supported browser.
2. Set the Internet security level to `Medium` and enable ActiveX Binary and Script Behaviors to make sure that tool tips and reports appear.
3. Type the management console IP address:
   - If using the default Deep Discovery Inspector IP address, type the following:

     ```
     https://192.168.252.1/index.html
     ```

     Note
     The URL is case sensitive.
   - If using a unique IP address, type that IP address.
4. Type the default user name:

   ```
   admin
   ```
5. Type the default password:

   ```
   admin
   ```
6. Click **Log on**.

   Important
   After changing the Deep Discovery Inspector appliance IP address, update browser bookmarks to reflect the new IP address.

7. Change the default password.

   See *Management console account passwords on page 2-6*.

8. Set system time.

   See *Configuring time options on page 6-185*.

9. Activate Deep Discovery Inspector.

   See *Activating or renewing licenses on page 6-210*.

Management console account passwords

Note

The passwords of non-local accounts cannot be changed from the management console.

Deep Discovery Inspector grants access to the management console by user accounts. The built-in administrator account can create a maximum of 127 local accounts. To access the management console, each user account requires a logon password.

The management console accepts passwords that contain the following:

- 8 to 32 characters
- At least one uppercase character (A-Z)
- At least one lowercase character (a-z)
- At least one numeric character (0-9)
- At least one special character: ` ~ ! @ # $ % ^ & * ( ) - _ + = [ ] { } \ | < > , . / ? : ; '"

Observe the following guidelines for creating a strong password:

- Avoid words found in the dictionary
- Intentionally misspell words

- Use phrases or combine words
- Use both uppercase and lowercase letters

Changing an administrator account password

Note

The passwords of non-local accounts cannot be changed from the management console.

The default management console password for the system administrator account is `admin`.

Tip

For added security, change the Deep Discovery Inspector password periodically.

Tip

An administrator password can also be reset on the **Accounts** screen.

Procedure

1. On any Deep Discovery Inspector main screen, at the top-right corner, open the drop-down menu under your account name.
2. Click **Change Password**.
3. Type the old password.
4. Type the new password and confirm it.
5. Click **Save**.

   Deep Discovery Inspector automatically logs off.

6. Log on to Deep Discovery Inspector with the new password.

Changing a viewer account password

Note

The passwords of non-local accounts cannot be changed from the management console.

Deep Discovery Inspector generates a default management console password when a new viewer account is created.

The new user must obtain this default password from the administrator and change the account password after logging on for the first time.

Tip

For added security, change the Deep Discovery Inspector password periodically.

Procedure

1. On any Deep Discovery Inspector main screen, at the top-right corner, open the drop-down menu under your account name.
2. Click **Change Password**.
3. Type the old password.
4. Type the new password and confirm it.
5. Click **Save**.

   Deep Discovery Inspector automatically logs off.
6. Log on to Deep Discovery Inspector with the new password.

Logging on with single sign-on

If you configure the required settings for SAML integration on Deep Discovery Inspector, users can access the Deep Discovery Inspector management console using their existing identity provider credentials.

For more information, see *SAML Authentication on page 6-161*.

Procedure

1. On the **Log On** screen, select a service name from the drop-down list.
2. Click **Single Sign-on (SSO)**.

   The system automatically navigates to the logon page for your organization.
3. Follow the on-screen instructions and provide your account credentials to access the Deep Discovery Inspector management console.

Network

Go to **Administration** > **System Settings** > **Network** to manage the Deep Discovery Inspector appliance network settings.

Deep Discovery Inspector uses a management port and several data ports. Go to **Administration** > **System Settings** > **Network Interface** to do the view the status of these ports.

Configuring the appliance IP settings

Procedure

1. Go to **Administration** > **System Settings** > **Network**.
2. In **Host name or FQDN**, specify a host name or FQDN.

Note

If you are using SAML authentication, the **Host name or FQDN** must contain the domain name. Changing the **Host name or FQDN** affects SAML authentication.

3. (Optional) Select the option to use the host name instead of the IP address as the identity of this appliance.

Important

The host name must be resolvable within your network.

4. Select the **IPv4 type**.
   - **Static IP address**
   - **Dynamic IP address (DHCP)**

Note

Deep Discovery Inspector requires its own IP address to ensure that the management port can access the management console. To enable a DHCP server on your network to dynamically assign an IP address to Deep Discovery Inspector, select **Dynamic IP address (DHCP)**. Otherwise, select **Static IP address**.

5. If **Static IP address** is selected, specify the following:
   a. **IPv4 address**: The numeric address specifically for Deep Discovery Inspector.
   b. **IPv4 subnet mask**: Indicates the subnet mask for the network that includes the Deep Discovery Inspector IP address.
   c. **IPv4 gateway**: The IP address of the network gateway.
   d. **IPv4 DNS server 1**: The IP address of the primary server that resolves host names to an IP address.
   e. **IPv4 DNS server 2** (optional): The IP address of the secondary server that resolves host names to an IP address.

6. (Optional) Configure an IPv6 address.

   a. Select **Enable IPv6 address**.

      The IPv6 address settings appear.

   b. Specify the following IPv6 address settings:

      - **IPv6 address**: The alphanumeric address specifically for Deep Discovery Inspector.
      - **IPv6 subnet prefix length**: Indicates the prefix length for the network that includes the Deep Discovery Inspector IP address.
      - **IPv6 gateway**: The IP address of the network gateway.
      - (Optional) **IPv6 DNS server**: The IP address of the server that resolves host names to an IP address.

7. (Optional) Enable **Always use TLS 1.2 or above**.

Important

The appliance must be restarted after **Always use TLS 1.2 or above** is enabled or disabled.

When enabled, Deep Discovery Inspector cannot connect to products/services that do not support TLS 1.2 and above.

Note

To be compliant with the Payment Card Industry Data Security Standard (PCI-DSS) v3.2, the appliance should use TLS 1.2 or above for all inbound and outbound connections.

Ensure that the integrated products and services are using the latest version that support TLS 1.2 or above. For details, see *TLS support for integrated products/services on page C-1*.

Verify that the following products/services are configured to use TLS 1.2 or above.

- The ActiveUpdate server source at **Administration** > **Updates** > **Component Updates** > **Source** must use HTTPS.
- The Apex Central server address at **Administration** > **Integrated Products/Services** > **Apex Central** must use HTTPS.
- The syslog servers at **Administration** > **Integrated Products/Services** > **Syslog** must use SSL.
- The SMTP server at **Administration** > **System Settings** > **SMTP** must use SSL/TLS or STARTTLS.
- The Threat Intelligence Sharing service at **Administration** > **Integrated Products/Services** > **Threat Intelligence Sharing** must use only HTTPS (disable **Share information using HTTP**).

8. Click **Save**.

Network format rules

Go to **Administration** > **System Settings** > **Network**.

The following format rules apply to Deep Discovery Inspector network settings.

TABLE 2-1. Network Setting Format Rules

FORMAT SETTING	DESCRIPTION
Appliance Host Name Format	The host name can contain alphanumeric characters and dashes ("A-Z", "a-z", "0-9", "-").
Dynamic IP Address	Obtain a dynamic IP address from a DHCP server on your network. Verify that the Preconfiguration Console has been changed accordingly. For details, see the *Deep Discovery Inspector 6.8 Service Pack 2 Installation and Deployment Guide*.
Static IP Address Format	**Note** The IP address cannot be the broadcast or network address. IP addresses must be in the format: XXX.XXX.XXX.XXX, where X is a decimal value between 0 and 255. The IPv4 address cannot be in any of the following formats: • `AAA.XXX.XXX.XXX`, where AAA is in the range 223 to 240 [Multicast Address] • `0.0.0.0` [Local Host name] • `255.255.255.255` [Broadcast Address] • `127.0.0.1` [Loopback Address] The IPv6 address cannot be in any of the following formats: • `ff00::/8` [Multicast Address] • `fe80::/10` [Link-local Address] • `::0` [Unicast route Address] • `::1/128` [Loopback Address]

Format Setting	Description
Subnet Mask Format	**Note** The subnet mask cannot be the broadcast or network address. The binary format of a subnet mask starts with a sequence of continuous 1s and ends with a sequence of continuous 0s. IPv4 address subnet mask example: • For `255.255.255.0`, the binary format is `11111111.11111111.11111111.00000000`.
Subnet Prefix Format	IPv6 addresses convert groups of bits into groups of hexadecimal digits, separated by colons. The high-order bits on the left of an IPv6 address specify the network, the rest specify particular addresses in that network. All the addresses in one network have the same first N bits, called the "prefix". Use "/N" to denote a prefix N bits long. IPv6 address subnet prefix example: • For `2001:db8::/32`, the prefix is `/32` and is 32 bits long. This example means all addresses where the first 32 bits are `2001:db8`.
Default Gateway Address Format	The gateway must be in the same subnet as the IP address.
DNS	IPv4 or IPv6 address

Managing network interface ports

Procedure

1. Go to **Administration** > **System Settings** > **Network Interface**.
2. View the status for each port.
3. Select **VLAN awareness** if you want to Deep Discovery Inspector to recognize and identify VLANs operating on the same network.

Important

Before enabling VLAN awareness, make sure that the inbound and outbound traffic for the same connection in your network use the same VLAN ID. Otherwise, Deep Discovery Inspector may not be able to identify the two directions as being the same network flow, causing incomplete telemetry and less accurate detection.

4. (Optional) If using an SSL inspection product, specify how Deep Discovery Inspector identifies decrypted SSL traffic .
   a. Click the right arrow (▶) at the beginning of the row to open the **Interface details** panel.
   b. In the **Interface details** panel, check **SSL identification**.

      The **Edit criteria** option appears when **SSL identification** is selected.
   c. Click **Edit criteria**.

      The **Identification for Decrypted SSL Traffic** window appears.
   d. Configure the **Marker VLAN tag** or **TCP port** that decrypted SSL traffic uses.
   e. Click **OK**.
   f. Repeat the above steps for each interface that receives decrypted SSL traffic.
5. (Optional) If receiving traffic via encapsulated remote mirroring, configure the receiving port on Deep Discovery Inspector.
   a. Click the right arrow (▶) at the beginning of the row to open the **Interface details** panel.
   b. In the **Interface details** panel, check **Encapsulated Remote Mirroring**.
   c. In the text box next to **Encapsulated Remote Mirroring**, type an IPv4 address.

d. Repeat the above steps for each interface that receives encapsulated mirrored traffic.

6. Click **Save**.

Chapter 3

Dashboard

Learn about the information that displays on the **Dashboard** tab in the following sections:

- *Dashboard overview on page 3-2*
- *Tabs on page 3-2*
- *Widgets on page 3-5*
- *About Deep Discovery Inspector widgets on page 3-6*
- *Deep Discovery Inspector widgets on page 3-7*
- *Deep Discovery Inspector default widget tabs on page 3-10*
- *Optional widgets on page 3-20*

Dashboard overview

Monitor your network integrity with the dashboard.

Each management console user account is provided a partially independent dashboard. Changes to a user account's dashboard affect the dashboards of other user accounts.

Customize the Deep Discovery Inspector dashboard with available widgets to provide timely and accurate system status and threat information about your network.

The Deep Discovery Inspector dashboard displays the following information on customizable and user-selected widgets:

- System data and status
- Threat data and analysis
- Summary graphs

The dashboard also monitors real-time network traffic volumes scanned by Deep Discovery Inspector.

The dashboard includes the following user interface elements:

- *Tabs on page 3-2*
- *Widgets on page 3-5*

Tabs

Tabs provide a container for widgets.

The dashboard supports up to 30 tabs. Each tab on the dashboard can contain up to 20 widgets.

Tab tasks

TABLE 3-1. Tab Tasks

TASK	STEPS
Add a tab	Click the plus icon at the top of the dashboard. For details, see *Adding/modifying tabs on page 3-3*.
Edit tab settings	Click **Tab Settings**. For details, see *Adding/modifying tabs on page 3-3*.
Move tab	Drag-and-drop to change a tab's position. For details, see *Moving tabs on page 3-4*.
Close/delete tab	Default tabs can be closed but not deleted. Customized tabs can be deleted but not closed. **Important** Deleting a tab deletes all the widgets contained in the tab. For details, see *Closing/deleting tabs on page 3-4*

Adding/modifying tabs

Procedure

1. To add a new tab or modify an existing tab, perform one of the following tasks:

   - To add a new tab, go to the **Dashboard** screen and click the tab with the + icon.

     The **New Tab** window appears.

   - To modify an existing tab, go to **Dashboard** > **Tab Settings**.

     The **Tab Settings** window appears.

2. Change the tab title, layout, and auto-fit options.

   Note

   The auto-fit function is affected by the selected layout and the amount of widgets added in the tab. Deep Discovery Inspector applies auto-fit only when auto-fit is enabled and the widgets are arranged one widget per row.

3. Click **Save**.

   The updated tab appears on the **Dashboard** screen.

Moving tabs

Procedure

1. Go to **Dashboard**.
2. Left-click and drag the tab to the desired location.

   Note

   All widgets contained by a tab move with the tab.

Closing/deleting tabs

On the dashboard, select the tab you wish to close or delete.

- Default tabs can be closed but not deleted.
- Customized tabs can be deleted but not closed.

Important

Deleting a tab deletes all the widgets contained in the tab.

Procedure

1. To close or delete a tab, click the icon beside the tab title.
   - Default tabs are closed and removed from view.
   - Customized tabs are deleted.

Widgets

Widgets are the core components of the dashboard. Widgets contain visual charts and graphs that allow you to track threats and associate them with the logs accumulated from one or several sources.

Widgets can be customized to provide a clear snapshot of network health and vulnerabilities. For details, see *Widget tasks on page 3-5*.

Widget tasks

TABLE 3-2. Widget Tasks

TASK	STEPS
Close	Close a widget and remove it from view.
Edit	• Rename a widget. • Modify display options. • Modify data options.
Export	Download a `.csv` file containing information about widget data.
Help	View information about a widget, widget data, and configuration or editable options.
Refresh	Display the latest information on the screen. **Note** Widget views refresh automatically. Different widgets have different refresh times.

Adding widgets to the dashboard

Procedure

1. Go to the **Dashboard** screen and click **Add Widgets**.
2. To find a widget to add, do any of the following:
   - To reduce the number of widgets displayed, click a category from the left navigation panel.
   - To search for a widget, specify the widget name or partial widget name in the search text box at the top of the screen.
3. (Optional) To change the widget count per page, select a number from the **Records** drop-down menu.
4. (Optional) To switch between Detailed and Summary views, click the display icons at the top of the page.
5. To select a widget, click the check box next to the widget's title.
6. Click **Add**.

   The widget is added to the tab.

About Deep Discovery Inspector widgets

Deep Discovery Inspector allows administrators to view system threat data displayed on various widgets.

By default, widgets are displayed on five tabs:

TABLE 3-3. Default Tabs

TAB	DESCRIPTION
Summary	This tab contains widgets that display hosts requiring priority attention and other detailed, actionable information. For details, see *Summary on page 3-10*.

Tab	Description
Threat Monitoring	This tab contains widgets that display real-time threat data to help administrators identify affected hosts and network threat distribution. For details, see *Threat monitoring on page 3-13*.
Virtual Analyzer Status	This tab contains widgets that display the top suspicious files, top hosts with Virtual Analyzer detections, top malicious sites analyzed by Virtual Analyzer, and Virtual Analyzer status and detections. For details, see *Virtual analyzer status on page 3-15*.
Top Trends	This tab contains widgets that display summary information for eight predefined threat types. For details, see *Top trends on page 3-19*.
System Status	This tab contains widgets that display basic Deep Discovery Inspector statuses including: CPU usage, disk usage, and memory usage. For details, see *System status on page 3-20*.

Optional, undisplayed widgets may be added to any widget tab. For details, see *Adding widgets to the dashboard on page 3-6*.

For widgets that display threat data, see *All detections - detection details - detection information on page 4-65* to view a list of displayed threat types.

Deep Discovery Inspector widgets

Deep Discovery Inspector includes the following widgets:

Table 3-4. Summary Widgets

Widget	Description
Threats at a Glance	This widget displays actionable information about six key metrics and links to the corresponding detection logs.
Top Affected Hosts	This widget displays hosts with the highest severity rating by severity in the past 1 hour/24 hours/7 days/30 days.
Threat Summary	This widget displays the threat count of various threat types within the past 24 hours/7 days/30 days.
Malicious Scanned Network Traffic	This widget displays real-time total and malicious scanned traffic volume detected by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in hours.

Widget	Description
Scanned Traffic by Protocol Type	This widget displays total traffic volume by protocol, in the past 1 hour/24 hours/7 days/30 days.

Table 3-5. Threat Monitoring Widgets

Widget	Description
Threat Geographic Map	This widget displays a graphical representation of the affected hosts on a virtual world map within the past hour/current day/past 7 days/ past 30 days.
Monitored Network Traffic in Past 30 Days	This widget displays the throughput of network traffic monitored by the Deep Discovery Inspector in the past 30 days.

Table 3-6. Virtual Analyzer Status Widgets

Widget	Description
Top Hosts with Virtual Analyzer Detections	This widget displays the top affected hosts analyzed by Virtual Analyzer based on the number of detections, in the past 1 hour/24 hours/7 days/30 days.
Top Malicious Sites Analyzed by Virtual Analyzer	This widget displays top malicious sites analyzed by Virtual Analyzer by detection and affected host count, in the past 1 hour/24 hours/7 days/30 days.
Top Suspicious Files	This widget displays top suspicious files analyzed by Virtual Analyzer by detection and affected host count, in the past 1 hour/24 hours/7 days/30 days.
Virtual Analyzer	This widget displays the status of Virtual Analyzer, including Virtual Analyzer threat analysis results within the past 1 hour/24 hours/7 days/30 days.

Table 3-7. Top Trends Widgets

Widget	Description
Top Disruptive Applications	This widget displays the most detected disruptive applications within the past 1 hour/24 hours/7 days/30 days.
Top Malicious URLs Detected	This widget displays the most detected malicious URLs within the past 1 hour/24 hours/7 days/30 days.

TABLE 3-8. System Status Widgets

WIDGET	DESCRIPTION
CPU Usage	This widget displays real-time CPU consumption for each CPU used by Deep Discovery Inspector. The indicator color is green if CPU usage is 85% or less. It turns yellow when CPU usage is between 85% and 95%, and red if more than 95%.
Disk Usage	This widget displays real-time disk usage for all disks. Green indicates the amount of disk space (in GB) being used. Blue indicates the amount of available disk space (in GB).
Memory Usage	This widget displays real-time memory usage. Green indicates the amount (in GB) of memory being used. Blue indicates the amount (in GB) of available memory. Memory usage information is also available on the Preconfiguration Console.

TABLE 3-9. Optional Widgets

WIDGET	DESCRIPTION
All Scanned Traffic	This widget displays total scanned traffic volume for the past 24 hours by HTTP, SMTP, and other traffic, in seconds.
Malicious Real-time Network Traffic	This widget displays real-time total and malicious traffic volume detected by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in seconds.
Real-time Scanned Traffic	This widget displays real-time total traffic volume scanned by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in seconds.
Top Exploited Hosts	This widget displays the most detected exploited hosts within the past 1 hour/24 hours/7 days/30 days.
Top Grayware-infected Hosts	This widget displays the most grayware-infected hosts within the past 1 hour/24 hours/7 days/30 days.
Top Malicious Content Detected	This widget displays the most detected threats within the past 1 hour/24 hours/7 days/30 days.

Widget	Description
Top Malware-infected Hosts	This widget displays the hosts most affected by malware within the past 1 hour/24 hours/7 days/30 days.
Top Suspicious Behaviors Detected	This widget displays the most detected suspicious behaviors within the past 1 hour/24 hours/7 days/30 days.

Optional widgets may be added to any widget tab.

Deep Discovery Inspector default widget tabs

Summary

The **Summary** tab contains widgets that display hosts requiring priority attention and other detailed actionable information.

By default, this tab displays the following widgets:

- *Threats at a glance on page 3-10*
- *Top affected hosts on page 3-12*
- *Threat summary on page 3-12*
- *Malicious scanned network traffic on page 3-12*
- *Scanned traffic by protocol type on page 3-13*

Threats at a glance

This widget displays actionable information about six key metrics and links to the corresponding detection logs.

TABLE 3-10. Threats at a Glance

METRIC	SOURCE	DESCRIPTION
Targeted Attack detections	Affected Hosts	• Counts Affected Hosts • Associated with the **Hosts with Targeted Attack detections** preset search Click a value to drill down to the **Affected Hosts** screen.
C&C Communication detections	Affected Hosts	• Counts Affected Hosts • Associated with the **Hosts with C&C Communication detections** preset search Click a value to drill down to the **Affected Hosts** screen.
Lateral Movement detections	Affected Hosts	• Counts Affected Hosts • Associated with the **Hosts with Lateral Movement detections** preset search Click a value to drill down to the **Affected Hosts** screen.
Ransomware	All Detections	• Counts detections • Associated with the **Ransomware** preset search Click a value to drill down to the **All Detections** screen.
Potential threats	All Detections	• Counts detections • Associated with the **Potential Threats** preset search Click a value to drill down to the **All Detections** screen.

Metric	Source	Description
Email threats	All Detections	• Counts detections • Associated with the **Email Threats** preset search Click a value to drill down to the **All Detections** screen.

The default time period is **Past 24 hours**.

Click **Edit** to change the title of the widget.

Top affected hosts

This widget displays hosts with the highest severity rating by severity level in the past 1 hour/24 hours/7 days/30 days.

Click **Edit** to change the number of affected hosts displayed (up to 20).

For details about the Host Severity scale, see *Host Severity on page 1-5*.

Threat summary

This widget displays total threats within the past 24 hours, 7 days, or 30 days. Information is displayed in a graph relating time and total threats. The type of threat is distinguishable by color.

The time range is editable from the top left drop-down.

Click a bar to open the **All Detections** screen with the **Detection type: Malicious Behavior** filter applied for that time period.

Click **Edit** to filter the types of threats displayed in the graph.

Malicious scanned network traffic

This widget displays real-time total and malicious scanned traffic volume detected by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in hours. This data can be filtered by traffic type:

- All traffic
- HTTP
- SMTP
- Other

Scanned traffic by protocol type

This widget displays total traffic volume by protocol, in the past 1 hour/24 hours/7 days/30 days.

Click **Edit** to change whether data is displayed in a bar, pie, or line chart. Select up to 10 protocols to display.

Threat monitoring

The **Threat Monitoring** tab contains widgets that display real-time threat data to help administrators identify affected hosts and network threat distribution.

By default, this tab displays the following widgets:

- *Threat geographic map on page 3-13*
- *Monitored network traffic in past 30 days on page 3-15*

Threat geographic map

The **Threat Geographic Map** widget is a graphical representation of affected hosts on a virtual world map. All affected hosts in different countries within a selected time frame are displayed in the following categories:

- Malware sources
- Network exploits sources
- Document exploit sources
- Malicious email sources
- Malware callback (C&C) destinations

The **Threat Geographic Map** displays regions with affected hosts as a solid red circle and the Deep Discovery Inspector location being analyzed as a red pinpoint.

Viewing information on the threat geographic map

Procedure

1. Select one of the following time frames:
   - **Past 1 hour**
   - **Today**
   - **Past 7 days**
   - **Past 30 days**
2. Modify the location.
   a. On the **Threat Geographic Map**, click the **Edit** icon.

      An edit screen appears.

   b. On the edit screen, select a location.

   c. Click **Apply**.

      The **Threat Geographic Map** is updated to reflect the new location.
3. Click any location to display relevant information in a pop-up window.

   Note

   The right pane displays information about affected hosts organized by country.
4. Click the total number of events for any threat in the pop-up window.

   A table populated with details about all threats (related to the indicated threat, country, and time period) appears.
5. In the table, click **Show** to display more details about a detection.

Monitored network traffic in past 30 days

This widget displays a graph of the total traffic monitored by Deep Discovery Inspector in the past 30 days, including decrypted TLS traffic. Hover over a point on the graph to learn about the traffic size and type. When Deep Discovery Inspector has exceeded or is close to exceeding the maximum bandwidth capacity, a red line appears to indicate the maximum bandwidth capacity.

Click, drag, and then release the mouse over a section of the timeline to zoom in. After zooming in, click **Reset** to reset the zoom level.

Use this widget to evaluate whether or not Deep Discovery Inspector has had sufficient bandwidth to scan all the network traffic it has received in the past 30 days.

Virtual analyzer status

Virtual Analyzer widgets are designed to show any Advanced Persistent Threats detected by Deep Discovery Inspector and analyzed by Virtual Analyzer.

By default, this tab displays the following widgets:

- *Top hosts with virtual analyzer detections on page 3-15*
- *Top malicious sites analyzed by virtual analyzer on page 3-16*
- *Top suspicious files on page 3-16*
- *Virtual analyzer on page 3-17*

Using this summary data gives administrators insight into what type of threat file types are affecting the network, which hosts are affected, and which malicious sites are attempting network access.

Top hosts with virtual analyzer detections

This widget displays the top affected hosts analyzed by Virtual Analyzer based on the number of detections.

Viewing hosts attacked in the past 1 hour, 24 hours, 7 days, or 30 days and the type of detected attack allows users (typically system or

network administrators) to take appropriate action (blocking network access, isolating computers according to IP address) to prevent malicious operations from affecting hosts.

Click a bar to open the **Filtered Detections** screen for that host with the selected time period.

Click **Edit** to change whether data displays in a chart, graph or table. You can also control the total number of affected hosts displayed (up to 20).

Top malicious sites analyzed by virtual analyzer

This widget displays the top malicious sites analyzed by Virtual Analyzer as detections per affected host. Deep Discovery Inspector, combined with Trend Micro Smart Protection Network, queries the level of security of destinations.

Viewing the top malicious sites mounting attacks against system hosts within the past 1 hour, 24 hours, 7 days, or 30 days allows users (typically system or network administrators) to take appropriate action (blocking network access to these malicious destinations by proxy or DNS server) in order to prevent malicious operations from affecting hosts.

All malicious sites within a chosen time frame are shown in a table.

Click a row to open the **Filtered Detections** screen for that malicious site with the selected time period.

Top suspicious files

This widget displays top suspicious files analyzed by Virtual Analyzer, along with the following information:

- The file count as detected by Deep Discovery Inspector
- The hosts affected by the suspicious file

Viewing suspicious files affecting hosts in the past 1 hour, 24 hours, 7 days or 30 days in a graphical format allows users (typically system or network administrators) to take appropriate action by adding email block lists, changing HTTP or FTP servers, modifying system files, or writing registry keys) to remove malicious operations from affecting hosts.

Data gathered about the affected hosts includes:

TABLE 3-11. Top Suspicious Files Data

COLUMN NAME	DESCRIPTION
File Name/SHA-1	The suspicious file name or SHA-1
Detections	Any event detected by Deep Discovery Inspector within a certain time frame
Affected Hosts	Any host that was affected by a suspicious file
Malware Name	The name of the known malware
Severity	The level of threat by suspicious files

Click **Edit** to change whether data displays in a chart, graph or table. You can also control the total number of top suspicious files displayed (up to 20).

Click the download icon ( ) beside a file name to download the suspicious file in a password-protected .zip archive.

Click a row to open the **Filtered Detections** screen for that malicious file with the selected time period.

Virtual analyzer

This widget displays information about files analyzed by Virtual Analyzer.

Use this widget to:

- Discover information about Virtual Analyzer
- View the overall analysis results from Virtual Analyzer

The widget also lets you do the following actions:

- Filter the information based on a defined **Period** (Past 30 days, 7 days, 24 hours, or 1 hour).
- Hover over a section of the chart to view the percentage of Malicious or Not Malicious analyzed files.

The widget displays a table with the following information:

VIRTUAL ANALYZER TYPE	DISPLAYED INFORMATION
Internal	• Analysis Module: Internal • Virtual Analyzer Status: Enabled • Last file analyzed: last scanned file name or SHA-1 • Last file analysis date • # of files to be analyzed • Average files count per hour
External	• Analysis Module: External • Last file analyzed: last scanned file name or SHA-1 • Last file analysis date: • # of files to be analyzed • Average files count per hour
Sandbox as a Service	• Analysis Module: Sandbox as a Service • Virtual Analyzer Status: Enabled • Last file analyzed: last scanned file name or SHA-1 • Last file analysis date • # of files to be analyzed • Average files count per hour
Trend Vision One — Sandbox Analysis	• Analysis Module: Trend Vision One — Sandbox Analysis • Virtual Analyzer Status: Enabled • Last file analyzed: last scanned file name or SHA-1 • Last file analysis date • # of files to be analyzed • Average files count per hour

Top trends

The **Top Trends** tab displays threat summary information from various perspectives. Administrators can use top threats data to identify the most dangerous hosts or the most severe threats in order to take appropriate action. Several Deep Discovery Inspector widgets identify the most affected hosts along with the most severe threats within certain time frames. For each widget, a detailed threat log can be exported for further analysis.

By default, this tab displays the following widgets:

- *Top disruptive applications on page 3-19*
- *Top malicious urls detected on page 3-19*

Top disruptive applications

This widget displays disruptive applications within the past 1 hour, 24 hours, 7 days, or 30 days.

Click a bar to open the **All Detections** screen with the **Protocol** and **Detection type: Disruptive Application** filters applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of top disruptive applications displayed (up to 20).

Top malicious urls detected

This widget displays the most malicious URL detections within the past 1 hour, 24 hours, 7 days, or 30 days.

By default, all detections within the selected time frame are shown in a table containing the URL and total detections.

Click a row to open the **All Detections** screen with the **IP address/ Domain/URL** and **Detection type: Malicious URL** filters applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of hosts displayed (up to 20).

System status

The **System Status** tab shows administrators whether Deep Discovery Inspector is operating within specifications; insufficient resources may cause a system failure. These widgets display real-time system resource data to ensure that all Deep Discovery Inspector resources are operating within specifications.

By default, this tab displays the following widgets:

- *CPU usage on page 3-20*
- *Disk usage on page 3-20*
- *Memory usage on page 3-20*

CPU usage

This widget displays what percent of each CPU is being used.

Disk usage

This widget displays how much disk space is available for your appliance.

Memory usage

This widget displays how much memory is available on your appliance.

Optional widgets

By default, the following widgets are not displayed in Deep Discovery Inspector 6.8 Service Pack 2, but may be added to any widget tab.

- *All scanned traffic on page 3-21*
- *Malicious real-time network traffic on page 3-21*
- *Real-time scanned traffic on page 3-21*
- *Top exploited hosts on page 3-22*
- *Top grayware-infected hosts on page 3-22*

- *Top malicious content detected on page 3-22*
- *Top malware-infected hosts on page 3-23*
- *Top suspicious behaviors detected on page 3-23*

All scanned traffic

This widget displays all scanned traffic for the past 24 hours and can be filtered by traffic type:

- All traffic
- HTTP
- SMTP
- Other

Malicious real-time network traffic

This widget displays all malicious traffic detected by Deep Discovery Inspector, in a line graph format, filtered by traffic type:

- All traffic
- HTTP
- SMTP
- Other

Traffic size is displayed with the time scale moving from right to left in seconds. Hover over a point on the graph to learn about the traffic size.

Click **Edit** to control whether data is displayed using traffic size or percent. You can also choose whether to display all scanned traffic data.

Real-time scanned traffic

This widget displays scanned traffic in a line graph based on all real-time HTTP, SMTP, or other traffic information. The time scale moves from right to left in seconds. Hover over a point on the graph to learn about the traffic size.

Top exploited hosts

This widget shows which hosts on your networks have been most affected by exploit attempts within the past 1 hour, 24 hours, 7 days, or 30 days. By default, all exploited hosts within the selected time frame are shown in a table showing the IP addresses of the top exploited hosts and total detections.

Click a row to open the **Host Details** screen for that host with the **Detection type: Exploit** filter applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number to exploited hosts displayed (up to 20).

Top grayware-infected hosts

This widget displays the most detected grayware on your networks within the past 1 hour, 24 hours, 7 days, or 30 days.

Note

This widget shows only those hosts with threats categorized as "High" severity.

By default, all grayware detections within the selected time frame are shown in a table.

Click a row to open the **Host Details** screen for that host with the **Detection type: Grayware** filter applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of grayware-infected hosts displayed (up to 20).

Top malicious content detected

This widget displays the most-detected known malware on your networks within the past 1 hour, 24 hours, 7 days, or 30 days.

By default, all known malware detections within the selected time frame are shown in a table.

Click a row to open the **All Detections** screen with the **Threat/Detection/ Reference** filter applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of exploited hosts displayed (up to 20).

Top malware-infected hosts

This widget displays the most malware-infected hosts on your networks within the past 1 hour, 24 hours, 7 days, or 30 days.

By default, all malware-infected hosts within the selected time frame are shown in a table showing the IP addresses of the infected hosts and total detections.

Click a row to open the **Host Details** screen for that host with the **Detection type: Malicious Behavior** filter applied.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number to malware-infected hosts displayed (up to 20).

Top suspicious behaviors detected

This widget displays the most detected suspicious behavior on your networks within the past 1 hour, 24 hours, 7 days, or 30 days.

By default, all suspicious behaviors within the selected time frame are shown in a table containing the description of the top suspicious behaviors and total detections.

Click a row to open the **All Detections** screen with the **Threat/Detection/ Reference** filter applied and only high detection severity .

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number to suspicious behaviors displayed (up to 20).

Chapter 4

Detections

Learn about information that displays on the **Detections** tab in the following topics:

- *About the detections screen on page 4-2*
- *Affected hosts on page 4-3*
- *C&C callback addresses on page 4-46*
- *Virtual analyzer suspicious objects on page 4-47*
- *User-defined suspicious objects on page 4-49*
- *Retro scan on page 4-50*
- *All detections on page 4-55*

About the detections screen

FIGURE 4-1. Detections Categories

The **Detections** tab provides access to real-time information about the following detection categories.

DETECTION CATEGORIES	DESCRIPTION
Affected Hosts	Hosts that have been involved in one or more phases of a targeted attack For details, see *Affected hosts on page 4-3*. For details about the Host Severity scale, see *Host Severity on page 1-5*.
C&C Callback Addresses	C&C addresses of callback attempts to known C&C addresses For details, see *C&C callback addresses on page 4-46*.
Virtual Analyzer Suspicious Objects	Suspicious objects identified by Virtual Analyzer or retrieved from an external source For details, see *Virtual analyzer suspicious objects on page 4-47*.
User-Defined Suspicious Objects	Suspicious objects and exceptions retrieved from external sources. For details, see *User-defined suspicious objects on page 4-49*
Retro Scan	A cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network For details, see *Retro scan on page 4-50*.
All Detections	Hosts with detections from all event logs, including global intelligence, user-defined lists, and other sources For details, see *All detections on page 4-55*.

Affected hosts

The **Affected Hosts** screens display information about hosts that have been involved in one or more phases of a targeted attack.

Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows you to prioritize and quickly respond. For details about the Host Severity scale, see *Host Severity on page 1-5*.

Access different information about Affected Hosts on the following views:

1. Affected Hosts view:
   - Displays a summary of affected hosts by attack phase
   - Provides access to Host Details views

     By default, Deep Discovery Inspector searches the Affected Hosts view by **IP Address** and **Host Name**.
2. Host Details view:
   - Displays host event details in chronological order
   - Provides access to Detection Details views

     By default, Deep Discovery Inspector searches the Affected Hosts - Host Details view by **Peer Host**.
3. Detection Details view:
   - Displays details of each detected threat
   - Provides access to different information panels, depending on search and other filter criteria and settings

Display options and search filters

To customize the display of targeted attack detections, apply the following display options and search filters:

TABLE 4-1. Display Options and Search Filters: Affected Hosts

FILTER OPTIONS	DESCRIPTION	
Detection severity	Filter options include the following detection severity settings:	
	High only	Displays `High severity detections only`
		Displays `High and medium severity detections`
		Displays `High, medium, and low severity detections`
	All	Displays `All detections, including informational detections`
Period	**Past 1 hour**	
	Past 24 hours (default)	
	Past 7 days	
	Past 30 days	
	Custom range Specify a custom range from the current day to the past 31 days.	
Customize Columns	Display optional columns.	

Filter Options	Description
Basic Search	Search for an IP address or host name. **Tip** Type a case-insensitive keyword in the basic search field to search a partial host match.

Preset Search Filters	Search by preset search criteria.
	• Affected Hosts view includes the following preset searches:
	  • Hosts with Targeted Attack detections
	  • Hosts with C&C Communications detections
	  • Hosts with Lateral Movement detections
	• Affected Hosts - Host Details view includes the following preset searches:
	  • Threats
	  • Known Threats
	  • Potential Threats
	  • Ransomware

Advanced Search Filter	Search by user-defined criteria sets. Each set includes one or more of the following: • Attributes • Operators • Associated values For details, see *Affected hosts advanced search filter on page 4-27*.

Viewing affected hosts

Procedure

1. Go to **Detections** > **Affected Hosts**.

2. Set the detection severity level by dragging the **Detection severity** slider to the desired rating.
3. Select a time period.
4. Click **Customize Columns**, select one or more optional columns for display and click **Apply** to return to the modified **Affected Hosts** screen.

FIGURE 4-2. Customize Columns

TABLE 4-2. Host Information Columns

COLUMN NAME	PRESELECTED	DESCRIPTION
IP Address	X	IP address of the affected host
Host Name	X	Computer name of the host
MAC Address		Media Access Control address of a network node
Network Group	X	Network group that an IP address/host is assigned
Host Severity	X	Highest impact on a host determined from aggregated detections by Trend Micro products and services For details about the Host Severity scale, see *Host Severity on page 1-5*.
Most Notable Threat	X	Threat description of the highest severity detection
Latest Detection	X	Most recent detection, based on timestamp

Note

The default **IP Address**, **Host Severity** and **Latest Detection** columns cannot be removed.

TABLE 4-3. Notable Statistics Columns

COLUMN NAME	PRESELECTED	DESCRIPTION
Targeted Attack		A threat that aims to exfiltrate data from a target system For details, see *APT Attack Sequence on page 1-4*

TABLE 4-4. Attack Phase Columns

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

Columns	Preselected	Description
Data Exfiltration	X	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.
Unknown Attack Phase	X	Detection is triggered by a rule that is not associated with an attack phase.

5. To run a basic search, do one of the following:

   - Type an IP address or host name in the search text box and press **Enter**.
   - Click the icon.

   By default, Deep Discovery Inspector searches **Affected Hosts** by **IP Address** and **Host Name**.

6. To run a saved search, go to **Detections** > **Affected Hosts**, open the drop-down menu of the search box, and click a saved search.

   Deep Discovery Inspector provides the following preset saved searches.

Table 4-5. Preset Saved Searches

Name	Filter Options
Hosts with Targeted Attack detections	Notable events in Targeted Attack
Hosts with C&C Communication detections	Notable events in C&C Communication
Hosts with Lateral Movement detections	Notable events in Lateral Movement

7. To create and apply an advanced search filter, click **Advanced**.

   For details, see *Affected hosts advanced search filter on page 4-27*.

8. Click **Export**.

   The following file downloads:

   - affected_host.csv

Viewing affected hosts - host details

Procedure

1. Go to **Detections** > **Affected Hosts**.
2. To display Affected Hosts - Host Details, do one of the following:
   - Click any detection link associated with an affected host.
   - Click the IP address of an affected host.

   Details about the host are displayed.

FIGURE 4-3. Affected Hosts - Host Details

3. Set the detection severity level by dragging the **Detection severity** slider.
4. Select a time period.
5. To select columns for display, click **Customize Columns**, select one or more columns, then click **Apply** to return to the modified **Affected Hosts** screen.

TABLE 4-6. Affected Hosts - Host Details Columns

COLUMNS	PRESELECTED
Status	X
Timestamp	X
Source Host	
Destination Host	
Interested Host	

Columns	Preselected
Peer Host	X
Sender	
Recipients	
Email Subject	
User Account	
Threat Description	X
Detection Name	X
Detection Type	
Protocol	X
Detection Severity	X
Attack Phase	X
Direction	X
Notable Object	X

Note

The default **Timestamp** and **Threat Description** columns cannot be removed.

6. (Optional) Click **Mark Displayed as Resolved** to mark all the detections displayed on the current page as resolved.

   In the Status column, the icon changes to .

Note

After marking all displayed detections as resolved, detections can only be individually marked as unresolved.

7. To run a basic search, do one of the following:

   - Type an IP address or host name in the search text box and press **Enter**.
   - Click the icon.

   By default, Deep Discovery Inspector searches Affected Hosts - Host Details by **Peer Host**.

8. Mark the affected peer host as one of the following:

   - Network Group
   - Registered Domains
   - Registered Services

   Do one of the following to open the drop-down menu and mark the host:

   - Beside the IP address, click the icon.
   - In the **Peer Host** column, click the icon.

9. To run a saved search, open the drop-down menu of the search box, and click a saved search.

   Deep Discovery Inspector provides the following preset saved searches on the Affected Host - Host Details screen.

TABLE 4-7. Preset Saved Searches

NAME	FILTER OPTIONS
Threats	Detection type options include the following: • Malicious Content • Malicious Behavior • Suspicious Behavior • Exploit • Grayware • Malicious URL

Name	Filter Options
Known Threats	File Detection Types: Known Malware

Potential Threats	• Virtual Analyzer Result: Has analysis results
	• File Detection type options include the following:
	  • Highly Suspicious File
	  • Heuristic Detection

Ransomware	Detection name options include the following: • Ransomware-related detections

10. To create and apply an advanced search filter, click **Advanced**.

    For details, see *About affected hosts - host details advanced search filter on page 4-34*.

11. Click **Export**.

    A zip archive with the following files downloads:

    - threats.csv
    - malicious_urls.csv
    - application_filters.csv
    - correlated_incidents.csv

Viewing affected hosts - detection details

Procedure

1. To view **Affected Hosts** detection details for any event, click the icon under the **Details** column on the **Affected Hosts - Hosts Details** screen.

   Detection details about the event are displayed.

Figure 4-4. Affected Hosts - Detection Details

2. In the **Connection Details** section, you may do the following:

   - Click **View in Threat Connect** to connect with **Threat Connect**, where you can search for current information about the threat.
   - Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.
   - Click **Download** and then select **Connection Details** to download a CSV file of the connection details.
   - If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file.

     In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

     For details about packet capture, see *Packet capture on page 6-58*.
   - Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the packet capture file, and the connection details.

   Important

   Suspicious files must always be handled with caution. Extract the detected file and pcap file at your own risk.

   The password for the zip archive is "virus".

3. In the **File Analysis Result** section, you may do the following:

   - Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.
   - Click **Download** and then select **Virtual Analyzer Report** to download the Virtual Analyzer report.
   - Click **Download** and then select **Investigation Package** to download a password protected ZIP archive containing the investigation package.

- Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.
- Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the Virtual Analyzer report, and the investigation package.

Important

Suspicious files must always be handled with caution. Extract the detected file at your own risk.

The password for the zip archive is "virus".

4. In the **Suspicious Object and Related File Analysis Result** section, view suspicious object and related analyzed file information.
5. In the **Mitigation Suggestions** section, view a description of the threat, its impact on the host, and the recommended actions to protect against the threat.

Affected hosts - detection details

Deep Discovery Inspector logs the details of each threat it detects. The **Detection Details** screen may contain the following information, depending on search and other filter criteria and settings.

- *Connection details on page 4-14*
- *Affected Hosts - Detection Details - File Analysis Result on page 4-21*
- *Affected Hosts - Detection Details - Suspicious Object and Related File Analysis Result on page 4-24*
- *Mitigation suggestions on page 4-26*

Connection details

The **Connection Details** section of the **Affected Hosts - Detection Details** screen contains the following information:

- *Affected Hosts - Detection Details - Detection Information on page 4-17*
- *Affected Hosts - Detection Details - Connection Summary on page 4-19*
- *Affected Hosts - Detection Details - Protocol Information on page 4-19*
- *Affected Hosts - Detection Details - File Information on page 4-21*
- *Affected Hosts - Detection Details - Additional Information on page 4-21*

Click **View in Threat Connect** to connect with Threat Connect, where you can search for current information about the threat.

Click **Download** and then select **Connection Details** to download a CSV file of the connection details.

Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.

If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file. In the pcap file,

the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

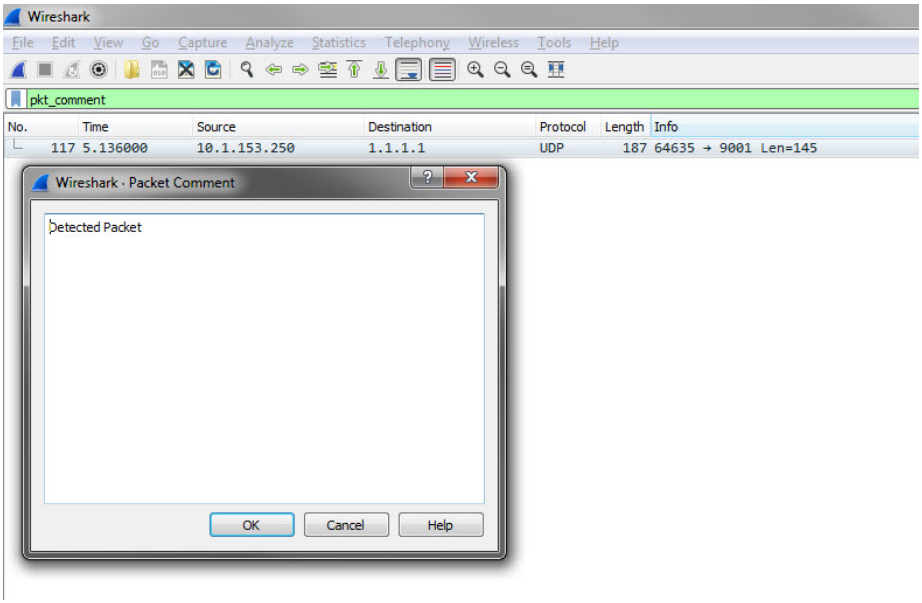


FIGURE 4-5. Detected Packet Example

For details about packet capture, see *Packet capture on page 6-58*.

Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the packet capture file, and the connection details.

Important

Suspicious files and pcap files must always be handled with caution. Extract the detected file and pcap file at your own risk. Trend Micro recommends analyzing the files in an isolated environment.

The password for the zip archive is "virus".

Affected Hosts - Detection Details - Detection Information

Information provided in the **Detection Information** section may include the following:

- Activity detected
- Attack phase
- Correlation Rule ID (ICID)
- Detection name
- Detection rule ID

Tip

Click the detection rule number to view more details about the rule in the Threat Encyclopedia.

- Detection severity
- Detection type
- Event class
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

Tip

Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Notable Object
- Protocol
- Reference

- Targeted attack campaign
- Targeted attack related
- Threat
- Threat description
- Timestamp
- URL category
- Virtual Analyzer risk level

Note

Additional information may appear for specific correlated incidents.

TABLE 4-8. Detection Types

DETECTION TYPES	DESCRIPTION
Correlated Incident	Events/detections that occur in a sequence or reach a threshold and define a pattern of activity
Disruptive Application	Any peer-to-peer, instant messaging, or streaming media applications considered to be disruptive because they may do the following: • Affect network performance • Create security risks • Distract employees
Exploit	Network and file-based attempts to access information
Grayware	Adware/grayware detections of all types and confidence levels
Malicious Behavior	Behavior that definitely indicates compromise with no further correlation needed, including the following: • Positively-identified malware communications • Known malicious destination contacted • Malicious behavioral patterns and strings

Detection Types	Description
Malicious Content	File signature detections
Malicious URL	Websites that try to perform malicious activities
Suspicious Behavior	Behavior that could indicate compromise but requires further correlation to confirm, including the following: • Anomalous behavior • False or misleading data • Suspicious and malicious behavioral patterns and strings

Affected Hosts - Detection Details - Connection Summary

Information provided in the **Connection Summary** section may include the following:

- A graphical display that includes the direction of the event and other information. The **Client** in the diagram is the host that initiated the connection.
- Host details may include the following:
  - Host name
  - IP address and port
  - Last logon user
  - MAC address
  - Network group
  - Network zone
  - Operating system

Affected Hosts - Detection Details - Protocol Information

Information provided in the **Protocol Information** section may include the following:

- BOT command

- BOT URL
- Certificate Information
  - Issued To
    - Common name
    - Organization
    - Organizational unit
  - Issued By
    - Common name
    - Organization
    - Organizational unit
- Domain name
- Host name
- HTTP referer
- ICMP code
- ICMP type
- IRC channel name
- IRC nick name
- Message ID
- Protocol
- Queried domain
- Recipients
- Sender
- SNI host name
- Subject

- Target share
- Transport Layer Security (TLS)
- URL
- User agent
- User name

Affected Hosts - Detection Details - File Information

Information provided in the **File Information** section may include the following:

- File name
- File SHA-1
- File SHA-256
- File size

Affected Hosts - Detection Details - Additional Information

Information provided in the **Additional Information** section may include the following:

- Attempted to disrupt connection
- Detected by
- Mitigation
- Fingerprinting
  - JA3 hash value
  - JA3S hash value
- VLAN ID

Affected Hosts - Detection Details - File Analysis Result

The **File Analysis Result** section of the **Affected Hosts - Detection Details** screen contains the following information:

- *Affected Hosts - Detection Details - File Analysis Result - File Information on page 4-22*
- *Affected Hosts - Detection Details - File Analysis Result - YARA Detections on page 4-23*
- *Affected Hosts - Detection Details - File Analysis Result - Notable Characteristics on page 4-24*

Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.

Click **Download** and then select **Virtual Analyzer Report** to download the Virtual Analyzer report.

Tip

Viewing or downloading the Virtual Analyzer report may take longer than the other options. Allocate more time for the Virtual Analyzer report to appear or download.

Click **Download** and then select **Investigation Package** to download a password protected ZIP archive containing the investigation package.

Important

Suspicious files must always be handled with caution. Extract the detected file at your own risk.

The password for the zip archive is "virus".

Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.

Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the Virtual Analyzer report, and the investigation package.

Affected Hosts - Detection Details - File Analysis Result - File Information

Information provided in the **File Analysis Result** - **File Information** section of the **Detection Details** window may include the following:

- Child files
  - File name / URL
  - File size (bytes)
  - Type
  - File SHA-1
  - File SHA-256
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

Tip

Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Threat
- Virual Analyzer risk level

Affected Hosts - Detection Details - File Analysis Result - YARA Detections

Information provided in the **File Analysis Result** - **YARA Detections** section of the Detection Details window may include the following:

- YARA Rule File

- YARA Rules

Affected Hosts - Detection Details - File Analysis Result - Notable Characteristics

Information provided in the **File Analysis Result** - **Notable Characteristics** section of the **Detection Details** window may include characteristics that are commonly associated with malware. Characteristics are grouped into the following categories:

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformation or other known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity
- Other notable characteristic

Affected Hosts - Detection Details - Suspicious Object and Related File Analysis Result

The **Suspicious Object and Related File Analysis Result** section of the **Affected Hosts - Detection Details** screen contains the following information:

- *Affected Hosts - Detection Details - Suspicious Object Information on page 4-24*
- *Affected Hosts - Detection Details - Related Analyzed File Information on page 4-25*

Affected Hosts - Detection Details - Suspicious Object Information

Information provided in the **Suspicious Object Information** section may include the following:

- Expiration date
- Related analyzed file
- Suspicious object
- Type
- Virtual Analyzer risk level

Affected Hosts - Detection Details - Related Analyzed File Information

Information provided in the **Related Analyzed File Information** section of the **Detection Details** window may include the following:

- Child files
  - File name
  - File size (bytes)
  - File type
  - File SHA-1
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

Tip

Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Threat
- Virtual Analyzer risk level

YARA Detections

- YARA Rule File
- YARA Rules

Notable characteristics that are commonly associated with malware. Characteristics are grouped into the following categories:

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformation or other known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity
- Other notable characteristic

Mitigation suggestions

Information provided in the **Mitigation Suggestions** section may include the following:

- Description
- Detailed description
- Impact
- Immediate action

Affected hosts advanced search filter

Use the advanced search filter to create and apply customized searches on detections displayed on the following screens:

- Affected Hosts view

  For details, see *About affected hosts advanced search filter on page 4-27*.

- Affected Hosts - Host Details view

  For details, see *About affected hosts - host details advanced search filter on page 4-34*.

Note

Include the following in each advanced search filter:

- A maximum of 20 criteria sets
- A maximum of 1024 characters in each text-based value field

Save up to 50 advanced search filters.

About affected hosts advanced search filter

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

TABLE 4-9. Search Filter Criteria: Affected Hosts

ATTRIBUTE	OPERATOR	ACTION
Host Name	**Contains/Does not contain**	Type a value
IP Address	**Contains/Does not contain** **In range/Not in range**	Type a value Type a range
MAC Address	**In/Not in**	Type a value

Attribute	Operator	Action
Network Group	**In/Not in**	Select one or more of the following: • **All groups** • **Default**
Notable Events	**In**	Select one or more of the following: • **Targeted Attack** • **C&C Communication** • **Lateral Movement**
Registered Services	**In/Not in**	Select one or more of the following: • **Active Directory** • **Authentication Servers - Kerberos** • **Content Management Server** • **Database Server** • **DNS** • **Domain Controller** • **File Server** • **FTP** • **HTTP Proxy** • **Radius Server** • **Security Audit Server** • **SMTP** • **SMTP Open Relay** • **Software Update Server** • **Web Server**

For details, see the following:

- *Adding an affected hosts advanced search filter on page 4-29*

- *Editing an affected hosts saved search on page 4-30*
- *Importing affected hosts saved searches on page 4-32*

Adding an affected hosts advanced search filter

Procedure

1. To create an advanced search filter, go to **Detections** > **Affected Hosts** and click **Advanced**.
2. Open the **Filter** drop-down menu and select an **Interested Host Information** attribute and an operator.
3. Do one of the following to provide an action:
   - Type a value in the text box.
   - Click an action from the drop-down menu.

Tip

Type a keyword to search a partial match.

For details, see *About affected hosts advanced search filter on page 4-27*.

Note

You can add multiple criteria entries separated by a comma.

4. (Optional) Click **Add new** to include other criteria sets in the search filter.

   Include the following in each advanced search filter:

   - A maximum of 20 criteria sets
   - A maximum of 1024 characters in each text-based value field

   Save up to 50 advanced search filters.
5. Click **Search**.

The **Affected Hosts** screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

6. (Optional) To save a search, do the following:

   a. Click the **Save** icon and click **Save as ...** .

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

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

   Note

   A saved search includes any search filter you create and the current customized column settings.

7. (Optional) Click **Cancel** to exit the advanced search feature and return to the previous screen.

Editing an affected hosts saved search

Procedure

1. To edit an Affected Hosts saved search, go to **Detections** > **Affected Hosts** and open the **Saved Searches** drop-down menu.
2. Select a saved search to edit and click the icon.
3. Select an attribute and an operator.
4. Do one of the following to provide an action:
   - Type a value in the text box.
   - Click an action from the drop-down menu.

Tip

Type a keyword to search a partial match.

For details, see *About affected hosts advanced search filter on page 4-27*.

Note

You can add multiple criteria entries separated by a comma.

5. (Optional) Click **Add new** to include other criteria sets.

   Include the following in each advanced search filter:

   - A maximum of 20 criteria sets
   - A maximum of 1024 characters in each text-based value field

6. Click **Search**.

   The **Affected Hosts** screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

7. (Optional) To save an edited saved search, click the **Save** icon and do one of the following:

   - To save the edited saved search with the same name, click **Save**.
   - To save the edited saved search with a new name, do the following:

   a. Click **Save As ...**.

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

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

      Note

      A saved search includes any search filter you create and the current customized column settings.

8. (Optional) To exit the advanced search feature, do one of the following:
   - Click **Cancel** to return to the previous screen.
   - Click on a saved search to run a basic search.

Deleting an affected hosts saved search

Important

Deleting a saved search will also permanently delete any report schedule associated with that saved search. However, any generated reports will not be deleted.

Procedure

1. To delete a saved search, go to **Detections** > **Affected Hosts**, and open the **Saved Searches** drop-down menu.
2. Click the **Delete** icon beside the saved search to be deleted.

Note

Preset filters cannot be deleted.

Importing affected hosts saved searches

Procedure

1. To import one or more saved searches, go to **Detections** > **Affected Hosts** and open the **Saved Searches** drop-down menu.
2. Click **Import** at the top of the **Saved Searches** drop-down menu.

   The **Import to Saved Searches** window appears.
3. Click **Browse** and select the file containing the saved searches.

The file is uploaded and validated. By default, all valid saved searches are selected for import.

Deep Discovery Inspector disables saved searches that are not compatible with the current product version.

4. (Optional) Hover over a saved search's name and then click the edit icon to rename the saved search before importing.

Note

Saved searches that have a duplicate name must be renamed before importing. Saved searches with a duplicate name are highlighted by a red box.

5. Mark the check box next to each saved search that you want to import or mark the check box at the top of the column to mark all the saved searches.

6. Click **Import**.

   The imported saved searches appear in the **Saved Searches** drop-down menu.

Exporting affected hosts saved searches

Procedure

1. To export one or more saved searches, go to **Detections** > **Affected Hosts** and open the **Saved Searches** drop-down menu.

2. Click **Export** at the top of the **Saved Searches** drop-down menu.

   The **Export Saved Searches** window appears. By default, all saved searches are selected for export.

3. Mark the check box next to each saved search that you want to export or mark the check box at the top of the column to mark all the saved searches.

Note

Deep Discovery Inspector cannot export preset filters.

4. Click **Export**.

   The saved searches file download begins.

About affected hosts - host details advanced search filter

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

TABLE 4-10. Search Filter Criteria: Affected Hosts - Host Details

ATTRIBUTE	OPERATOR	ACTION	EXAMPLES
Host Name	**Contains/Does not contain**	Type a value	computer.example.com
IP address	**Contains/Does not contain** **In range/Not in range**	Type a value Type a range	10.1.1.2
MAC address	**In/Not in**	Type a value	AA:AA:AA:AA:AA:AA
Network Group	**In/Not in**	Select one or more of the following: • **All groups** • **Default**	

Attribute	Operator	Action	Examples
Registered Services	**In/Not in**	Select one or more of the following: • **Active Directory** • **Authentication Servers - Kerberos** • **Content Management Server** • **Database Server** • **DNS** • **Domain Controller** • **File Server** • **FTP** • **HTTP Proxy** • **Radius Server** • **Security Audit Server** • **SMTP** • **SMTP Open Relay** • **Software Update Server** • **Web Server**	
Protocol	**In/Not in**	Select one or more of the following: • **All protocol types** • **Desired protocol type(s)** • **Other**	
Transport Layer Security (TLS)	**Over SSL/TLS/Not over SSL/TLS**		

Attribute	Operator	Action	Examples
Direction	**Equals**	Select one of the following: • **Internal** • **External**	
Status	**Equals**	Select one of the following: • **Resolved** • **Unresolved**	
Threat/ Detection/ Reference	**Contains**/**Does not contain**/ **Equals**	Type a value	VAN_RANSOMWARE.UMXX
Detection Rule ID	**In**/**Not in**	Type a value	707-710, 721-727
Correlation Rule ID (ICID)	**In**/**Not in**	Type a value	707-710, 721-727
Detection Type	**In**/**Not in**	Select one or more of the following: • **Malicious Content** • **Malicious Behavior** • **Suspicious Behavior** • **Exploit** • **Grayware** • **Malicious URL** • **Disruptive Application** • **Correlated Incident**	

Attribute	Operator	Action	Examples
Attack Phase	**In**/**Not in**	Select one or more of the following: • **Intelligence Gathering** • **Point of Entry** • **C&C Communication** • **Lateral Movement** • **Asset/Data Discovery** • **Data Exfiltration** • **Unknown Attack Phase**	
YARA Rule File/YARA Rule	**Contains**/**Equals**	Type a value	myYARAFile
	Has YARA detection		
C&C List Source	**In**/**Not in**	Select one or more of the following: • **Global Intelligence** • **Virtual Analyzer** • **User-defined**	
C&C Callback Address	**Contains**/**Does not contain**/**Equals**	Type a value	computer.example.com
C&C Risk Level	**In**/**Not in**	Select one or more of the following: • **High** • **Medium** • **Low**	

Attribute	Operator	Action	Examples
Virtual Analyzer Result	**Has analysis results/No analysis results**		
PCAP File	**Has PCAP file/No PCAP file**		
Is Targeted Attack Related	**Yes/No**		
File Detection Type	**In**	Select one or more of the following: • **Highly Suspicious File** • **Heuristic Detection** • **Known Malware**	
File Name	**Has file name/No file name**		
	Contains/Does not contain	Type a value	myFile
File SHA-1	**Has file SHA-1/No file SHA-1**		
	Contains/Does not contain	Type a value	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
File SHA-256	**Has file SHA-256/No file SHA-256**		

Attribute	Operator	Action	Examples
	Contains/Does not contain	Type a value	8b7df143d91c716ecfa5fc1730022f6b421b05ceedee8fd52b1fc65a96030ad52
IP Address/ Domain/URL	**Has network object/No network object**		
	Contains/Does not contain/ Equals	Type a value	10.1.1.2
Suspicious Object/Deny List Entity	**Contains/Does not contain/ Equals**	Type a value	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
Email Address	**Has email address/No email address**		example@example.com
	Contains/Does not contain	Type a value	
Message ID (Email)	**Has message ID/No message ID**		

Attribute	Operator	Action	Examples
	Contains/Does not contain	Type a value	950124.162336@example.com
Subject (Email)	**Has subject/No subject**		
	Contains/Does not contain	Type a value	mySubject

For details, see the following:

- *Adding an affected hosts - host details advanced search filter on page 4-40*
- *Editing an affected hosts - host details saved search on page 4-42*
- *Importing affected hosts - host details saved searches on page 4-44*

Adding an affected hosts - host details advanced search filter

Procedure

1. To create an Affected Hosts - Host Details advanced search filter, go to **Detections** > **Affected Hosts** and click any detection link.

   Details about the host are displayed.

2. Click **Advanced**.

3. Open the **Filter** drop-down menu and select an attribute and an associated operator.

4. Do one of the following to provide an action:

   - Type a value in the text box.
   - Click an action from the drop-down menu.

Tip

Type a keyword to search a partial match.

For details, see *About affected hosts advanced search filter on page 4-27*.

Note

You can add multiple criteria entries separated by a comma.

5. (Optional) Click **Add new** to include other criteria sets in the search filter.

   Include the following in each advanced search filter:

   - A maximum of 20 criteria sets
   - A maximum of 1024 characters in each text-based value field

   Save up to 50 advanced search filters.

6. Click **Search**.

   The Affected Hosts - Host Details screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

7. (Optional) To save a search, do the following:

   a. Click the **Save** icon and click **Save as ...** .

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

      The name of the new saved search adds to the list of saved searches.

      Note

      A saved search includes any search filter you create and the current customized column settings.

8. (Optional) Click **Cancel** to exit the advanced search feature.

Editing an affected hosts - host details saved search

Procedure

1. To edit an advanced Affected Hosts - Host Details saved search, go to **Detections** > **Affected Hosts** and click any detection link.
2. Open the **Saved Searches** drop-down menu.
3. Select a saved search to edit.
4. To edit a saved search, do one of the following:
   - Click the icon.
   - Click **Advanced**.
5. Select an attribute and an associated operator.
6. Do one of the following to provide an action:
   - Type a value in the text box.
   - Click an action from the drop-down menu.

   Tip

   Type a keyword to search a partial match.

   For details, see *About affected hosts advanced search filter on page 4-27*.

   Note

   Add multiple criteria entries separated by a comma.
7. (Optional) Click **Add new** to include other criteria sets in the search filter.

Note

Include the following in each advanced search filter:

- A maximum of 20 criteria sets
- A maximum of 1024 characters in each text-based value field

Save up to 50 advanced search filters.

8. Click **Search**.

   The Affected Hosts - Host Details screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

9. (Optional) To save an edited saved search, click the **Save** icon and do one of the following:

   - To save the edited saved search with the same name, click **Save**.

     The edited saved search is saved with the original name.

   - To save the edited saved search with a new name, do the following:

   a. Click **Save As ...**.

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

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

Note

A saved search includes any search filter you create and the current customized column settings.

10. (Optional) To exit the advanced search feature, do one of the following:

    - Click **Cancel** to return to the previous screen.

- Click on a saved search to run a basic search.

Deleting an affected hosts - host details saved search

Procedure

1. To drill down to Affected Hosts - Host Details from the **Affected Hosts** screen, do one of the following:
   - Click any detection link associated with an affected host.
   - Click the IP address of an affected host.
2. To delete a saved search, open the **Saved Searches** drop-down menu.
3. Click the **Delete** icon beside the saved search to be deleted.

Note

Preset filters cannot be deleted.

Importing affected hosts - host details saved searches

Procedure

1. To import one or more saved searches, go to **Detections** > **Affected Hosts** and click any detection link.
2. Open the **Saved Searches** drop-down menu.
3. Click **Import** at the top of the **Saved Searches** drop-down menu.

   The **Import to Saved Searches** window appears.
4. Click **Browse** and select the file containing the saved searches.

   The file is uploaded and validated. By default, all valid saved searches are selected for import.

Deep Discovery Inspector disables saved searches that are not compatible with the current product version.

5. (Optional) Hover over a saved search's name and then click the edit icon to rename the saved search before importing.

Note

Saved searches that have a duplicate name must be renamed before importing. Saved searches with a duplicate name are highlighted by a red box.

6. Mark the check box next to each saved search that you want to import or mark the check box at the top of the column to mark all the saved searches.
7. Click **Import**.

   The imported saved searches appear in the **Saved Searches** drop-down menu.

Exporting affected hosts - host details saved searches

Procedure

1. To import one or more saved searches, go to **Detections** > **Affected Hosts** and and click any detection link.
2. Open the **Saved Searches** drop-down menu.
3. Click **Export** at the top of the **Saved Searches** drop-down menu.

   The **Export Saved Searches** window appears. By default, all saved searches are selected for export.
4. Mark the check box next to each saved search that you want to export or mark the check box at the top of the column to mark all the saved searches.

Note

Deep Discovery Inspector cannot export preset filters.

5. Click **Export**.

   The saved searches file download begins.

C&C callback addresses

The **C&C Callback Addresses** screen displays a list of C&C callback addresses identified by scan engine pattern and rule matches.

C&C callback address detections can be sorted by **Callback Address**, **C&C Risk Level**, **Type**, **Latest Callback**, or **Callbacks**.

FIGURE 4-6. C&C Callback Addresses

Viewing C&C callback addresses

Procedure

1. Go to **Detections** > **C&C Callback Addresses**.
2. Click the drop-down for detection type and then select one of the following detection types:
   - **All** (default)
   - **IP Addresses/Domains**
   - **URLs**
3. (Optional) Copy a callback address to the Deny List or the Allow List.
   a. Select a callback address detection.
   b. Click **Copy to Deny List** or **Copy to Allow List**.

      A window appears to copy to the Deny List or Allow List.
   c. Specify the options and click **Save**.

A notification that asks to reload the lists appears .

d. Click **Reload**.

4. (Optional) Click a number in the **Callbacks** column to drill-down to the **All Detections** screen with filters applied.
5. (Optional) To sort the list of C&C callback addresses, click the column titles.

Note

Only one column can be sorted at a time.

- **Callback Address**: Ascending/descending alphanumeric
- **C&C Risk Level**: Ascending/descending alphabetical
- **Type**: Ascending/descending alphabetical
- **Latest Callback**: Earliest/latest date
- **Callbacks**: Ascending/descending numerical

Virtual analyzer suspicious objects

The **Virtual Analyzer Suspicious Objects** screen (**Detections** > **Virtual Analyzer Suspicious Objects**) displays a list of suspicious files, IP addresses, URLs, and domains identified by the Virtual Analyzer or synchronized from external sources.

The following table outlines actions available in the **Virtual Analyzer Suspicious Objects** screen.

Action	Description
Filter object data	Use the search field or object type list to filter objects. **Tip** The search field is not case-sensitive and allows partial matches.
View number of detections during a time period	Specify a time period to see the number of detections for all objects during the selected period. **Important** • The table contains all Virtual Analyzer suspicious objects regardless of the selected period. • If a Virtual Analyzer suspicious object was not detected during the selected time period, the total detections displayed is "0".
Manage Virtual Analyzer suspicious objects	Manage one or multiple Virtual Analyzer suspicious objects. Options include: • **Move object to deny list**: Select one or more objects, then click **Move to Deny List** to move the selected objects to the deny list. • **Move object to allow list**: Select one or more objects, then click **Move to Allow List** to move the selected objects to the allow list. • **Delete object**: Select one or more objects, then click **Delete** to delete the selected objects.
View details about detections	Click a number under the **Detections** column to drill-down to the **All Detections** screen with filters applied.
Sort list	Click any of the column titles to sort the Virtual Analyzer suspicious objects list. **Note** Only one column can be sorted at a time.

User-defined suspicious objects

Consolidate suspicious object information based on input from different sources.

The **User-Defined Suspicious Objects** screen (**Detections** > **User-Defined Suspicious Objects**) contains the **User-Defined Suspicious Objects** list and the **Exception** list.

"Suspicious objects" are known malicious or potentially malicious domains, file SHA-1, file SHA-256, IP addresses, or URLs. "Exceptions" are objects that are considered safe.

Note

Deep Discovery Inspector retrieves the User-Defined Suspicious Objects list and the Exception list from Trend Vision One, Deep Discovery Director, and Apex Central.

The following table outlines the actions available on the **User-Defined Suspicious Objects** screen.

Action	Description
Display the User-Defined Suspicious Objects list	Click on the **Suspicious Objects** tab to display the User-Defined Suspicious Objects list.
Display the Exceptions list	Click on the **Exceptions** tab to display the Exceptions list.
Filter object data	Use the search field or object type list to filter objects. **Tip** The search field is not case-sensitive and allows partial matches.

Action	Description
Sort list	Click any of the column titles to sort the User-Defined Suspicious Objects list or the Exceptions list. **Note** You can sort only one column at a time.
Export all synchronized data	On the **Suspicious Objects** tab, click **Export All** to export all synchronized suspicious object data into a CSV file. On the **Exceptions** tab, click **Export All** to export all synchronized exceptions data into a CSV file.

Retro scan

Retro Scan is a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network. Web access logs may include undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations to determine if your network is affected by attacks.

Retro Scan stores the following log information in the Smart Protection Network:

- IP addresses of endpoints monitored by Deep Discovery Inspector
- URLs accessed by endpoints
- GUID of this server

Retro Scan then periodically scans the stored log entries to check for callback attempts to C&C servers in the following lists:

- Trend Micro Global Intelligence List: Trend Micro compiles the list from multiple sources and evaluates the risk level of each C&C callback address. The C&C list is updated and delivered to enabled products daily.
- User-defined list: Retro Scan can also scan logs against your own C&C server list. Addresses must be stored in a text file.

Important

The Retro Scan screen in Deep Discovery Inspector only displays information for scans that use the Trend Micro Global Intelligence List.

Retro scan and the Smart Protection Network

C&C communication is generally associated with large botnets, but is also a significant component of targeted attacks. Targeted attacks are often remotely orchestrated through C&C communication between the compromised hosts and the attackers. Malware call back to C&C servers for additional downloads or instructions, and can be used by attackers to access the compromised hosts.

C&C-related traffic in targeted attacks is often difficult to locate. Attackers change and redirect addresses, use legitimate sites, and even set up C&C servers inside a company's network. Moreover, most security technologies focus solely on detecting and blocking addresses that are known to be malicious at that point in time. This is problematic because reputation scores constantly change. Addresses that are considered safe today can easily become malicious within the next hour or day.

In response to these issues, Retro Scan integrates the Trend Micro Smart Protection Network to discover threats. This cloud-based protection system combines advanced threat research with intelligence from customers to provide better protection and minimize the impact of targeted attacks.

Retro Scan examines historical web access logs to help you discover suspicious connections regardless of when the address is identified as malicious.

Enabling retro scan

Retro Scan functions independently from Deep Discovery Inspector and is disabled by default.

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Web Reputation**.

2. Click **Enable Web Reputation**.
3. Under **Smart Protection Settings**, select **Trend Micro Smart Protection Network**.
4. Select **Enable Retro Scan**.

   The **Service and Terms** window appears.
5. Read the information and click **Accept**.
6. Click **Save**.

After Retro Scan is enabled, Deep Discovery Inspector periodically checks Retro Scan for scan reports. If scan reports are available, Deep Discovery Inspector displays summary information on the **Retro Scan** screen.

Retro scan screen

The **Retro Scan** screen displays the following information:

- Date and time of latest scan
- Link to the Retro Scan **Report Repository**

  Note

  Clicking the link opens the **Report Repository** in a new browser tab.
- Summary of the results of all scans

Column	Description
Report Generated	Date and time the scan report was completed
Compromised Hosts	Number of hosts that attempted to connect to C&C callback addresses during the scan period
Callback Attempts	Number of C&C callback attempts found in the logs during the scan period

Note

Click the number to display the details for a specific report. For details, see *Retro scan report details screen on page 4-53*.

The **Retro Scan** screen also allows you to export the summary information to a .csv file.

Retro scan report details screen

Clicking a number under the **Callback Attempts** column on the **Retro Scan** screen opens a new screen with the following information:

- Number of callback attempts
- Link to the Retro Scan report

Note

Clicking the link opens the online version of the report in a new browser tab.

- Summary of the Standard Scan report

Column	Description
Callback Attempted	Date and time of each C&C callback attempt
Monitored Network Group	Monitored network group to which the compromised host belongs
Compromised Hosts	Name of the compromised host
IP Address	IP address of the compromised host
Callback Address	URL or IP address of the C&C server

Column	Description
Related Malware Families	Malware families associated with the C&C callback address
Related Attacker Groups	Attacker groups associated with the C&C callback address

Disable retro scan

Retro Scan is automatically disabled when you do any of the following:

- Disable Web Reputation

  Optionally disable Web Reputation only if you use other security products to block URLs or use Deep Discovery Inspector specifically for sandbox analysis.

- Change Smart Protection source to a local Smart Protection server

  Retro Scan is based on queries to the web reputation technology in the Smart Protection Network. Retro Scan cannot store and scan logs for queries to a local Smart Protection server.

Disabling retro scan

WARNING!

Disabling Retro Scan deletes all Retro Scan detection logs received and displayed by Deep Discovery Inspector.

Procedure

1. To disable Retro Scan service, go to **Administration** > **Monitoring / Scanning** > **Web Reputation**.
2. Under Smart Protection Settings, deselect **Enable Retro Scan**.

3. In the confirmation message window, click **OK** to disable Retro Scan and delete all Retro Scan detection logs.

All detections

The **All Detections** screen displays a list of hosts that have experienced an event in a user-defined time period. Detections are displayed from global intelligence, user-defined lists, and other sources.

By default, Deep Discovery Inspector searches **All Detections** by **Source Host**, **Destination Host** and **Interested Host**.

Display options and search filters

To customize the display, apply the following display options and search filters:

TABLE 4-11. Display Options and Search Filters: All Detections

FILTER OPTIONS	DESCRIPTION	
Filter by Severity	Filter options include the following severity settings:	
	High only	Displays `High severity detections only`
		Displays `High and medium severity detections`
		Displays `High, medium, and low severity detections`

Filter Options	Description	
	All	Displays `All detections, including informational detections`
Period	**Past 1 hour** **Past 24 hours** (default) **Past 7 days** **Past 30 days** **Custom Range** Specify a custom range from the current day to the past 31 days.	
Customize Columns	Display optional columns.	
Basic Search	Search an IP address or host name. **Tip** Type a case-insensitive keyword in the basic search field to search a partial host match.	
Preset Search Filters	Search by preset search criteria. All Detections view includes the following preset searches: • Threats • Known Threats • Potential Threats • Email Threats • Ransomware	

Filter Options	Description
Advanced Search Filter	Search by user-defined criteria sets, including the following: Each set includes one or more of the following: • Attributes • Operators • Associated values For details, see *All Detections Advanced Search Filter on page 4-75*.

Viewing all detections

Procedure

1. Go to **Detections** > **All Detections**.
2. Set the detection severity level by dragging the **Detection severity** slider.
3. Select a time period.
4. To select columns for display, click **Customize Columns**, select one or more columns, then click **Apply** to return to the modified **All Detections** screen.

Table 4-12. All Detections Columns

Columns	Preselected
Status	X
Timestamp	X
Source Host	X
Destination Host	X
Interested Host	X
Peer Host	
Sender	

Columns	Preselected
Recipients	
Email Subject	
User Account	
Threat Description	X
Detection Name	X
Threat (Virtual Analyzer)	
Reference	
Detection Type	
Protocol	X
Transport Layer Security (TLS)	
Detection Severity	X
Attack Phase	X
Direction	
Notable Object	X

Note

The default **Timestamp** and **Threat Description** columns cannot be removed.

The default **Details** column cannot not be removed and does not appear in the **Customize Columns** option.

5. (Optional) Click **Mark Displayed as Resolved** to mark all the detections displayed on the current page as resolved.

   In the Status column, the icon changes to .

Note

After marking all displayed detections as resolved, detections can only be individually marked as unresolved.

6. To run a basic search, do one of the following:

   - Type an IP address or host name in the search text box and press **Enter**.
   - Click the icon.

   By default, Deep Discovery Inspector searches **All Detections** by **Source Host**, **Destination Host**, and **Interested Host**.

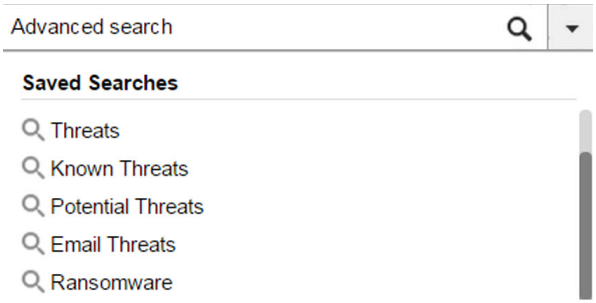


FIGURE 4-7. All Detections Basic Search

7. To run a saved search, go to **Detections**>**All Detections**, open the drop-down menu of the search box, and click a saved search.

   Deep Discovery Inspector provides the following preset saved searches.

TABLE 4-13. Preset Saved Searches

NAME	FILTER OPTIONS
Threats	Detection type options include the following: • Malicious Content • Malicious Behavior • Suspicious Behavior • Exploit • Grayware • Malicious URL
Known Threats	File Detection Types: Known Malware

Potential Threats	• Virtual Analyzer Result: Has analysis results
	• File Detection type options include the following:
	  • Highly Suspicious File
	  • Heuristic Detection

Email Threats	Protocol options include the following: • IMAP4 • POP3 • SMTP
Ransomware	Detection name options include the following: • Ransomware-related detections

8. To create and apply an advanced search filter, click **Advanced**.

   For details, see *All detections advanced search filter on page 4-75*.

9. Click **Export**.

   A zip folder with the following files downloads:

   - threats.csv
   - malicious_urls.csv

- application_filters.csv
- correlated_incidents.csv

Viewing all detections - detection details

Procedure

1. To view **All Detections** detection details for any event, click the icon under the **Details** column on the **All Detections** screen.

   Detection details about the event are displayed.

   FIGURE 4-8. All Detections - Detection Details

2. In the **Connection Details** section, you may do the following:

   - Click **View in Threat Connect** to connect with **Threat Connect**, where you can search for current information about the threat.
   - Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.
   - Click **Download** and then select **Connection Details** to download a CSV file of the connection details.
   - If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file.

     In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

     For details about packet capture, see *Packet capture on page 6-58*.
   - Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the packet capture file, and the connection details.

Important

Suspicious files must always be handled with caution. Extract the detected file and pcap file at your own risk.

The password for the zip archive is "virus".

3. In the **File Analysis Result** section, you may do the following:
   - Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.
   - Click **Download** and then select **Virtual Analyzer Report** to download the Virtual Analyzer report.
   - Click **Download** and then select **Investigation Package** to download a password protected ZIP archive containing the investigation package.
   - Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.
   - Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the Virtual Analyzer report, and the investigation package.

Important

Suspicious files must always be handled with caution. Extract the detected file at your own risk.

The password for the zip archive is "virus".

4. In the **Suspicious Object and Related File Analysis Result** section, view suspicious object and related analyzed file information.
5. In the **Mitigation Suggestions** section, view a description of the threat, its impact on the host, and the recommended actions to protect against the threat.

All detections - detection details

Deep Discovery Inspector logs the details of each threat it detects. The **Detection Details** screen may contain any of the following information, depending on search and other filter criteria and settings.

- *All detections - detection details - connection details on page 4-63*
- *All detections - detection details - file analysis result on page 4-69*
- *All detections - detection details - suspicious object and related file analysis result on page 4-72*
- *All detections - detection details - mitigation suggestions on page 4-74*

All detections - detection details - connection details

The **Connection Details** section of the **All Detection - Detection Details** screen contains the following information:

- *All detections - detection details - detection information on page 4-65*
- *All detections - detection details - connection summary on page 4-67*
- *All detections - detection details - protocol information on page 4-67*
- *All detections - detection details - file information on page 4-69*
- *All detections - detection details - additional information on page 4-69*

Click **View in Threat Connect** to connect with Threat Connect, where you can search for current information about the threat.

Click **Download** and then select **Connection Details** to download a CSV file of the connection details.

Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.

If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file. In the pcap file,

the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

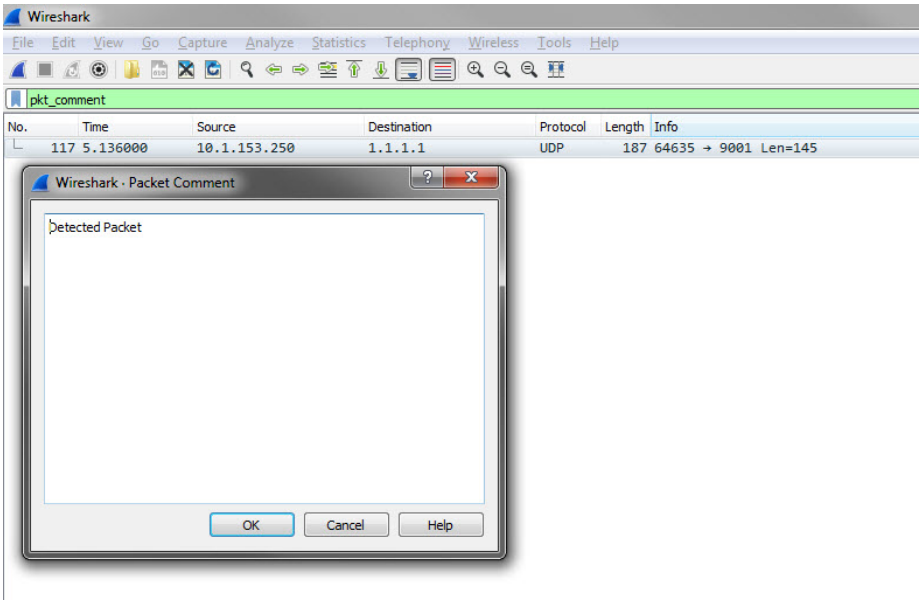


FIGURE 4-9. Detected Packet Example

For details about packet capture, see *Packet capture on page 6-58*.

Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the packet capture file, and the connection details.

Important

Suspicious files and pcap files must always be handled with caution. Extract the detected file and pcap file at your own risk. Trend Micro recommends analyzing the files in an isolated environment.

The password for the zip archive is "virus".

All detections - detection details - detection information

Information provided in the **Detection Information** section may include the following:

- Activity detected
- Attack phase
- Correlation Rule ID (ICID)
- Detection name
- Detection rule ID

> **Tip**
> Click the detection rule number to view more details about the rule in the Threat Encyclopedia.

- Detection severity
- Detection type
- Event class
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

> **Tip**
> Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Notable Object
- Protocol
- Reference

- Targeted attack campaign
- Targeted attack related
- Threat
- Threat description
- Timestamp
- URL category
- Virtual Analyzer risk level

Note

Additional information may appear for specific correlated incidents.

TABLE 4-14. Detection Types

DETECTION TYPES	DESCRIPTION
Correlated Incident	Events/detections that occur in a sequence or reach a threshold and define a pattern of activity
Disruptive Application	Any peer-to-peer, instant messaging, or streaming media applications considered to be disruptive because they may do the following: • Affect network performance • Create security risks • Distract employees
Exploit	Network and file-based attempts to access information
Grayware	Adware/grayware detections of all types and confidence levels
Malicious Behavior	Behavior that definitely indicates compromise with no further correlation needed, including the following: • Positively-identified malware communications • Known malicious destination contacted • Malicious behavioral patterns and strings

Detection Types	Description
Malicious Content	File signature detections
Malicious URL	Websites that try to perform malicious activities
Suspicious Behavior	Behavior that could indicate compromise but requires further correlation to confirm, including the following: • Anomalous behavior • False or misleading data • Suspicious and malicious behavioral patterns and strings

All detections - detection details - connection summary

Information provided in the **Connection Summary** section may include the following:

- A graphical display that includes the direction of the event and other information. The **Client** in the diagram is the host that initiated the connection.
- Host details may include the following:
  - Host name
  - IP address and port
  - Last logon user
  - MAC address
  - Network group
  - Network zone
  - Operating system

All detections - detection details - protocol information

Information provided in the **Protocol Information** section may include the following:

- BOT command

- BOT URL
- Certificate Information
  - Issued To
    - Common name
    - Organization
    - Organizational unit
  - Issued By
    - Common name
    - Organization
    - Organizational unit
- Domain name
- Host name
- HTTP referer
- ICMP code
- ICMP type
- IRC channel name
- IRC nick name
- Message ID
- Protocol
- Queried domain
- Recipients
- Sender
- SNI host name
- Subject

- Target share
- Transport Layer Security (TLS)
- URL
- User agent
- User name
- Miscellaneous

All detections - detection details - file information

Information provided in the **File Information** section may include the following:

- File name
- File SHA-1
- File SHA-256
- File size

All detections - detection details - additional information

Information provided in the **Additional Information** section may include the following:

- Attempted to disrupt connection
- Detected by
- Mitigation
- Fingerprinting
  - JA3 hash value
  - JA3S hash value
- VLAN ID

All detections - detection details - file analysis result

The **File Analysis Result** section of the **All Detections - Detection Details** screen contains the following information:

- *All detections - detection details - file analysis result - file information on page 4-70*
- *All detections - detection details - file analysis result - YARA detections on page 4-71*
- *All detections - detection details - file analysis result - notable characteristics on page 4-72*

Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.

Click **Download** and then select **Virtual Analyzer Report** to download the Virtual Analyzer report.

Tip

Viewing or downloading the Virtual Analyzer report may take longer than the other options. Allocate more time for the Virtual Analyzer report to appear or download.

Click **Download** and then select **Investigation Package** to download a password protected ZIP archive containing the investigation package.

Important

Suspicious files must always be handled with caution. Extract the detected file at your own risk.

The password for the zip archive is "virus".

Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.

Click **Download** and then select **All** to download a password protected ZIP archive containing the detected file, the Virtual Analyzer report, and the investigation package.

All detections - detection details - file analysis result - file information

Information provided in the **File Analysis Result** - **File Information** section of the **Detection Details** window may include the following:

- Child files
  - File name / URL
  - File size (bytes)
  - Type
  - File SHA-1
  - File SHA-256
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

Tip

Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Threat
- Virual Analyzer risk level

All detections - detection details - file analysis result - YARA detections

Information provided in the **File Analysis Result** - **YARA Detections** section of the Detection Details window may include the following:

- YARA Rule File

- YARA Rules

All detections - detection details - file analysis result - notable characteristics

Information provided in the **File Analysis Result** - **Notable Characteristics** section of the **Detection Details** window may include characteristics that are commonly associated with malware. Characteristics are grouped into the following categories:

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformation or other known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity
- Other notable characteristic

All detections - detection details - suspicious object and related file analysis result

The **Suspicious Object and Related File Analysis Result** section of the **All Detection - Detection Details** screen contains the following information:

- *All detections - detection details - suspicious object information on page 4-72*
- *All detections - detection details - related analyzed file information on page 4-73*

All detections - detection details - suspicious object information

Information provided in the **Suspicious Object Information** section may include the following:

- Expiration date
- Related analyzed file
- Suspicious object
- Type
- Virtual Analyzer risk level

All detections - detection details - related analyzed file information

Information provided in the **Related Analyzed File Information** section of the **Detection Details** window may include the following:

- Child files
  - File name
  - File size (bytes)
  - File type
  - File SHA-1
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

Tip

Click the tactic or technique to view more details on the MITRE website.

© ATT&CK™ is a trademark of the MITRE Corporation.

- Threat
- Virtual Analyzer risk level

YARA Detections

- YARA Rule File
- YARA Rules

Notable characteristics that are commonly associated with malware. Characteristics are grouped into the following categories:

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformation or other known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity
- Other notable characteristic

All detections - detection details - mitigation suggestions

Information provided in the **Mitigation Suggestions** section may include the following:

- Description
- Detailed description
- Impact
- Immediate action

All detections advanced search filter

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

Note

Include the following in each advanced search filter:

- A maximum of 20 criteria sets
- A maximum of 1024 characters in each text-based value field

Save up to 50 advanced search filters.

For details, see the following:

- *Adding an All Detections Advanced Search Filter on page 4-81*
- *Editing an All Detections Advanced Search Filter on page 4-83*
- *Importing all detections saved searches on page 4-85*

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

TABLE 4-15. Search Filter Criteria: All Detections

ATTRIBUTE	OPERATOR	ACTION	EXAMPLES
Host Name	**Contains/Does not contain**	Type a value	computer.example.com
IP address	**Contains/Does not contain** **In range/Not in range**	Type a value Type a range	10.1.1.2
MAC address	**In/Not in**	Type a value	AA:AA:AA:AA:AA:AA

Attribute	Operator	Action	Examples
Network Group	**In/Not in**	Select one or more of the following: • **All groups** • **Default**	
Registered Services	**In/Not in**	Select one or more of the following: • **Active Directory** • **Authentication Servers - Kerberos** • **Content Management Server** • **Database Server** • **DNS** • **Domain Controller** • **File Server** • **FTP** • **HTTP Proxy** • **Radius Server** • **Security Audit Server** • **SMTP** • **SMTP Open Relay** • **Software Update Server** • **Web Server**	
Protocol	**In/Not in**	Select one or more of the following: • **All protocol types** • **Desired protocol type(s)** • **Other**	

Attribute	Operator	Action	Examples
Transport Layer Security (TLS)	**Over SSL/TLS/Not over SSL/TLS**		
Direction	**Equals**	Select one of the following: • **Internal** • **External**	
Status	**Equals**	Select one of the following: • **Resolved** • **Unresolved**	
Threat/ Detection/ Reference	**Contains/Does not contain/ Equals**	Type a value	VAN_RANSOMWARE.UMXX
Detection Rule ID	**In/Not in**	Type a value	707-710, 721-727
Correlation Rule ID (ICID)	**In/Not in**	Type a value	707-710, 721-727

Attribute	Operator	Action	Examples
Detection Type	**In/Not in**	Select one or more of the following: • **Malicious Content** • **Malicious Behavior** • **Suspicious Behavior** • **Exploit** • **Grayware** • **Malicious URL** • **Disruptive Application** • **Correlated Incident**	
Attack Phase	**In/Not in**	Select one or more of the following: • **Intelligence Gathering** • **Point of Entry** • **C&C Communication** • **Lateral Movement** • **Asset/Data Discovery** • **Data Exfiltration** • **Unknown Attack Phase**	
YARA Rule File/YARA Rule	**Contains/Equals**	Type a value	myYARAFile
	Has YARA detection		

Attribute	Operator	Action	Examples
C&C List Source	**In/Not in**	Select one or more of the following: • **Global Intelligence** • **Virtual Analyzer** • **User-defined** • **Relevance Rule**	
C&C Callback Address	**Contains/Does not contain/ Equals**	Type a value	computer.example.com
C&C Risk Level	**In/Not in**	Select one or more of the following: • **High** • **Medium** • **Low**	
Virtual Analyzer Result	**Has analysis results/No analysis results**		
PCAP File	**Has PCAP file/No PCAP file**		
Is Targeted Attack Related	**Yes/No**		
File Detection Type	**In**	Select one or more of the following: • **Highly Suspicious File** • **Heuristic Detection** • **Known Malware**	
File Name	**Has file name/No file name**		

Attribute	Operator	Action	Examples
	Contains/**Does not contain**	Type a value	myFile
File SHA-1	**Has file SHA-1**/**No file SHA-1**		
	Contains/**Does not contain**	Type a value	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
File SHA-256	**Has file SHA-256**/**No file SHA-256**		
	Contains/**Does not contain**	Type a value	8b7df143d91c716ecfa5fc1730022f6b421b05ceedee8fd52b1fc65a96030ad52
IP Address/ Domain/URL	**Has network object**/**No network object**		
	Contains/**Does not contain** / **Equals**	Type a value	10.1.1.2

Attribute	Operator	Action	Examples
Suspicious Object/Deny List Entity	**Contains/Does not contain/ Equals**	Type a value	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
Email Address	**Has email address/No email address**		example@example.com
	Contains/Does not contain	Type a value	
Message ID (Email)	**Has message ID/No message ID**		
	Contains/Does not contain	Type a value	950124.162336@example.com
Subject (Email)	**Has subject/No subject**		
	Contains/Does not contain	Type a value	mySubject

Adding an all detections advanced search filter

Procedure

1. To create an advanced search filter, go to **Detections** > **All Detections** and click **Advanced**.
2. Open the **Filter** drop-down menu and select an attribute and an associated operator.

3. Do one of the following to provide an action:
   - Type a value in the text box.
   - Click an action from the drop-down menu.

Tip

Type a keyword to search a partial match.

For details, see *All detections advanced search filter on page 4-75*.

Note

You can add multiple criteria entries separated by a comma.

4. (Optional) Click **Add new** to include other criteria sets in the search filter.

   Include the following in each advanced search filter:
   - A maximum of 20 criteria sets
   - A maximum of 1024 characters in each text-based value field

   Save up to 50 advanced search filters.

5. Click **Search**.

   The **All Detections** screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

6. (Optional) To save a search, do the following:

   a. Click the **Save** icon and select **Save as ...**.

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

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

Note

A saved search includes any search filter you create together with the current customized column settings.

7. (Optional) Click **Cancel** to exit the advanced search feature.

Editing an all detections saved search

Procedure

1. To edit an All Detections saved search, go to **Detections** > **All Detections** and open the **Saved Searches** drop-down menu.
2. Select a saved search to edit and click the icon.
3. Select an attribute and an associated operator.
4. Do one of the following to provide an action:
   - Type a value in the text box.
   - Click an action from the drop-down menu.

Tip

Type a keyword to search a partial match.

For details, see the Search Filter Criteria: All Detections table *All detections advanced search filter on page 4-75*.

Note

Add multiple criteria entries separated by a comma.

5. (Optional) Click **Add new** to include other criteria sets in the search filter.

Note

Include the following in each advanced search filter:

- A maximum of 20 criteria sets
- A maximum of 1024 characters in each text-based value field

Save up to 50 advanced search filters.

6. Click **Search**.

   The **All Detections** screen updates and displays data filtered by the search criteria. All search criteria sets are displayed in a summary.

7. (Optional) To save an edited saved search, click the **Save** icon and do one of the following:

   - To save the edited saved search with the same name, click **Save**.

     The edited saved search is saved with the original name.

   - To save the edited saved search with a new name, do the following:

   a. Click **Save as ...**.

      The **Saved Searches** window opens.

   b. Type a name and click **Save**.

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

      Note

      A saved search includes any search filter you create and the current customized column settings.

8. (Optional) To exit the advanced search feature, do one of the following:

   - Click **Cancel** to return to the previous screen.
   - Click on a saved search to run a basic search.

Deleting an all detections saved search

Procedure

1. To delete a saved search, go to **Detections** > **All Detections**, and open the **Saved Searches** drop-down menu.

2. Click the **Remove Filter** icon beside the saved search to be deleted.

Note

Preset filters cannot be deleted.

Importing all detections saved searches

Procedure

1. To import one or more saved searches, go to **Detections** > **All Detections** and open the **Saved Searches** drop-down menu.

2. Click **Import** at the top of the **Saved Searches** drop-down menu.

   The **Import to Saved Searches** window appears.

3. Click **Browse** and select the file containing the saved searches.

   The file is uploaded and validated. By default, all valid saved searches are selected for import.

   Deep Discovery Inspector disables saved searches that are not compatible with the current product version.

4. (Optional) Hover over a saved search's name and then click the edit icon to rename the saved search before importing.

Note

Saved searches that have a duplicate name must be renamed before importing. Saved searches with a duplicate name are highlighted by a red box.

5. Mark the check box next to each saved search that you want to import or mark the check box at the top of the column to mark all the saved searches.
6. Click **Import**.

   The imported saved searches appear in the **Saved Searches** drop-down menu.

Exporting all detections saved searches

Procedure

1. To export one or more saved searches, go to **Detections** > **All Detections** and open the **Saved Searches** drop-down menu.
2. Click **Export** at the top of the **Saved Searches** drop-down menu.

   The **Export Saved Searches** window appears. By default, all saved searches are selected for export.
3. Mark the check box next to each saved search that you want to export or mark the check box at the top of the column to mark all the saved searches.

   Note

   Deep Discovery Inspector cannot export preset filters.
4. Click **Export**.

   The saved searches file download begins.

Chapter 5

Reports

Learn how to generate and access Deep Discovery Inspector scheduled and on-demand reports in the following topics:

- *About Reports on page 5-2*
- *Scheduled Reports on page 5-4*
- *Schedules on page 5-5*
- *Scheduling a Report on page 5-6*
- *Deleting a Report Schedule on page 5-7*
- *On-demand Reports on page 5-8*
- *Generating On-demand Reports on page 5-9*
- *Deleting an On-demand Report on page 5-11*
- *Customization on page 5-11*
- *Customizing Reports on page 5-11*

About reports

Deep Discovery Inspector provides report templates for easy access to threat information. Reports help you better understand complex threat scenarios, prioritize responses, and plan containment and mitigation.

TABLE 5-1. Deep Discovery Inspector Reports

REPORT TYPE AND FORMAT	TABLE OF CONTENTS

Advanced Report
 	
Compressed archive with the following formats:
 	
1. PDF file
2. CSV files
	• Detection Overview
	  • Virtual Analyzer Summary
	  • Custom Deny List Events Summary
	• High Severity Hosts
	• High Severity Hosts Details
	• Virtual Analyzer Result Details
	• Deny List Detection Details
	• Threat Statistics
	  • Top 20 Hosts Visiting Malicious Sites
	  • Malicious Content Statistics
	• Informational Detections
	• Disruptive Application Usage
	• Recommendations
	• Glossary
	• Appendix A: Report Scope

Report Type and Format	Table of Contents

Executive Report
PDF
	• Highlights
	• Business Risk Profile
	• Affected Assets
	• Infection Sources
	• Detection Technology Used
	• Threat Statistics
	• Virtual Analyzer Statistics
	• Disruptive Applications
	• Deny List Entities
	• Potential Impact
	• Recommendations
	• Appendices
	  • Appendix A: Report Scope
	  • Appendix B: Most-affected Host Summary

Host Severity Report
PDF
	• Summary
	• Affected Hosts
	• C&C Communication
	• Potential Threats
	• Known Threats
	• Lateral Movement
	• Appendices
	  • Appendix A: Report Scope
	  • Appendix B: Host Severity of Affected Hosts

Report Type and Format	Table of Contents
Summary Report PDF	• Overview • Discovery Highlights • Recommendations • Appendix A: Report Scope

Threat Detection Report
PDF
	• Summary
	  • Top 10 Threats detected exclusively by Virtual Analyzer
	  • Top 10 Threats detected by Virtual Analyzer
	  • Detected Known Malware Types
	  • Infection Channels
	  • Top 10 Attack Sources Per Group
	  • Top 10 Cross Group Attacks
	  • Top 10 Attack Sources
	  • Top 10 Threat Types
	  • Threat Trends
	  • Virtual Analyzer Statistics
	• Appendices
	  • Appendix A: Report Scope
	  • Appendix B: Recommendations

Scheduled reports

The **Scheduled Reports** screen displays user-scheduled daily, weekly, and monthly reports on a calendar.

Table 5-2. Calendar Icons

Icon	Frequency	User	Purpose
D	Daily	Administrator	Track threat status

Icon	Frequency	User	Purpose
W	Weekly	Executive	Overview of organization's security posture
M	Monthly	Executive	Overview of organization's security posture

A list of scheduled reports by selected calendar day provides access to previous reports. Click a report to open or save it.

Schedules

Use the **Schedules** screen to do the following:

- Review the attributes of scheduled reports
- Add, modify, and delete report schedules

Table 5-3. Column Names: Schedules Tab

Column	Description
Frequency	Generic report period, including the following: • Daily • Weekly • Monthly
Name	Customized or default report name
Type	Report types, including the following: • Advanced • Executive • Host Severity • Summary • Threat Detection

Column	Description
Scope	Included hosts, including the following: • All monitored hosts • Filtered hosts
Notification	Status of the notifications option • On: Enabled • Off: Disabled
Period	Time range covered by the report
Created By	Name of the user account that scheduled the report

Scheduling a report

Reports can be scheduled to generate daily, weekly, and monthly.

Procedure

1. On the **Reports** > **Schedules** tab, click **Add**. The **Add Schedule** window opens.
2. (Optional) Type a report name.
3. Under **Schedule**, select a report frequency.

Table 5-4. Report Frequency

Frequency	Option	Description
Daily		Midnight to 23:59
Weekly	**Start week on:**	Default: Sunday Configurable: Sunday through Saturday
Monthly	**Start month on day:**	Default: Day 01 Configurable: 01 through 31

Next Report Period displays a time range for the report.

4. Select a report type.

   For details about available reports, see *About reports on page 5-2*.

   The **Table of Contents** of the selected report displays.

5. To select the report scope, click one of the following:

   - **All monitored hosts**
   - **Filtered hosts**

   Note

   Selectable saved filters include the preset Affected Hosts saved searches and any custom saved searches.

6. (Optional) Select **Send generated report to email recipients**.

   To edit the list of email recipients, go to **Administration** > **Notifications** > **Delivery Options** > **Email Settings**.

7. Click **Save**.

8. To modify a report schedule, click a report name and follow steps 2 to 7.

   Note

   Report schedules can only be edited by the user account that created the schedule. However, any user may delete any report schedule.

Deleting a report schedule

Procedure

1. On the **Reports** > **Schedules** tab, select a report schedule to delete.
2. Click **Delete**.

Note

This removes the report schedule. The report is not deleted.

Important

When a user account is deleted, any report schedule created by the account will also be deleted. However, any generated reports will not be deleted.

When a saved search is deleted, any report schedule associated with the search will also be deleted. However, any generated reports will not be deleted.

For details on how to remove scheduled reports that have previously generated, see *Storage Maintenance on page 6-201*.

On-demand reports

Generate one-time reports anytime you need them. Use the **On-demand Reports** screen to do the following:

- Review the attributes of generated on-demand reports
- Add, download, and delete on-demand reports

TABLE 5-5. Column Names: On-demand Reports Tab

COLUMN	DESCRIPTION
Generated	Date and time a report was generated
Name	Customized or default report name

Column	Description
Type	Report types, including the following: • Advanced • Executive • Host Severity • Summary • Threat Detection Report
Scope	Included hosts, including the following: • All monitored hosts • Filtered hosts
Period	Time range covered by the report
Created By	Name of the user account that generated the report
Download	Save or open a generated report

Note

On-demand reports are generated as soon as possible and are available for viewing immediately after they are generated. Email notifications are not provided for on-demand reports.

Generating an on-demand report

Procedure

1. Go to **Reports** > **On-demand Reports**.
2. Click **Add**.

   The **Add On-demand Report** window opens.
3. Set a report period. Options include the following:
   - Click a preset period:

- **Past 7 days**
- **Past 2 weeks**
- **Past 4 weeks**

- Click on the calendars to select a date range.

Note

When you click a preset period, the **From**/**To** field automatically adds the correct dates.

4. Select a report type.

   For details about available reports, see *About reports on page 5-2*.

   The **Table of Contents** of the selected report displays.

5. To select the report scope, click one of the following:

   - **All monitored hosts**
   - **Filtered hosts**

     Choose a saved search from **Affected Hosts**.

     Note

     Selectable saved searches include preset Affected Hosts saved searches and any custom saved searches. To configure a saved search for application to a report, go to **Detections** > **Affected Hosts** > **Advanced** and select a host attribute and associated criteria.

6. Click **Generate** to create the report.

   The new on-demand report appears in the list.

Deleting an on-demand report

Important

This procedure removes the report from Deep Discovery Inspector. Once deleted, the report cannot be recovered.

Any user may delete any report.

Procedure

1. On the **Reports** > **On-demand Reports** tab, select a report to delete.
2. Click **Delete**.

Customization

Use the **Customization** screen to configure report cover options. For details, see *Customizing Reports on page 5-11*.

Customizing reports

Procedure

1. Go to **Reports** > **Customization**.
2. Type a **company name**.
3. To display a company logo, click **Display** and browse to select an image.

   Important

   Image files must be in JPG or PNG file format. The maximum file size is 200 KB.

4. (Optional) Deselect the **Display Trend Micro logo** check box.

Note

The **Display Trend Micro logo** is preselected by default.

5. Click **Save**.

Chapter 6

Administration

Learn how to administer Deep Discovery Inspector operations in the following sections:

- *Updates on page 6-2*
- *Notifications on page 6-15*
- *Monitoring / scanning on page 6-34*
- *Virtual Analyzer on page 6-72*
- *Network groups and assets on page 6-98*
- *Integrated products/services on page 6-108*
- *About accounts on page 6-187*
- *System settings on page 6-175*
- *System logs on page 6-199*
- *System maintenance on page 6-201*
- *Licenses on page 6-208*

Updates

Use the **Updates** screen to configure component and product update settings.

Component updates

Download and deploy product components used to scan for and detect network threats. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest threats.

Components to update

To help protect your network, Deep Discovery Inspector uses the components listed in the following table.

TABLE 6-1. Deep Discovery Inspector Components

COMPONENT	DESCRIPTION
Advanced Persistent Threat Information Pattern	Advanced Persistent Threat Information Pattern provides details about advanced persistent threats.
Advanced Threat Correlation Pattern	The Advanced Threat Correlation Pattern contains a list of file features that are not relevant to any known threats.
Advanced Threat Scan Engine for Deep Discovery (Linux, 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.
C&C Identification Pattern	C&C Identification Pattern contains a list of known C&C servers and callback addresses.
Common Threat Family Information Pattern	Common Threat Family Information Pattern provides the common threat family name for detections.
Common Vulnerabilities and Exposures Information Pattern	Common Vulnerability and Exposure Information Pattern provides CVE reference information for detections.

Component	Description
Contextual Intelligence Query Handler	The Contextual Intelligence Query Handler processes the behaviors identified by the Contextual Intelligence Engine and sends the report to the Predictive Machine Learning engine.
Deep Discovery Malware Pattern	The Trend Micro Virus Scan Engine protects against viruses and malware in files through heuristic, signature-based, and behavior-based detection. Trend Micro updates the virus pattern files as soon as detection routines for new threats are available.
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 (5.14, Kernel mode, 64-bit, Conf: 6500)	The Network Content Inspection Engine is used to perform network scanning.
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.
Script Analyzer Unified Pattern	The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.
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.
Threat Correlation Pattern	The Threat Correlation Pattern is used by Deep Discovery Inspector during threat correlation.

Component	Description
Threat Knowledgebase (EN)	The Threat Knowledge Base provides information for threat correlation.
Trend Micro Intelligence Agent v.2 (Deep Discovery Inspector, Linux, 64-bit)	Trend Micro Intelligence Agent v.2 retrieves additional information about detections.
Trusted Certificate Authorities Pattern	Trusted Certificate Authorities Pattern provides the trusted certificate authorities to verify PE signatures.
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.

Component update methods

Use one of the following methods to update components:

Table 6-2. Update Methods

Method	Description
Manual update	To check the availability of new components, go to **Administration** > **Updates** > **Component Updates** on the management console. For details, see *Manual updates on page 6-5*. **Note** Deep Discovery Inspector updates all components. You cannot update components individually. To update Deep Discovery Inspector components, go to **Administration** > **Updates** > **Component Updates** > **Source**. For details, see *Update source on page 6-7*.

Method	Description
Scheduled update	To configure an update schedule, go to **Administration** > **Updates** > **Component Updates** > **Scheduled**. Deep Discovery Inspector automatically checks the update source at the specified frequency. For details, see *Scheduled updates on page 6-6*.

Component update tasks

To update all components, review the following procedures:

- *Proxy on page 6-178*
- *Manual updates on page 6-5*
- *Scheduled updates on page 6-6*
- *Update source on page 6-7*
- *Service packs / version upgrade on page 6-12*

Manual updates

Deep Discovery Inspector allows on-demand component updates. Use this feature during outbreaks or when updates do not arrive according to a fixed schedule.

The following details appear in the **Manual** screen.

Table 6-3. Manual Update Screen Details

Details	Description
Component	Component name
Current Version	Version number of each component currently used by the product
Latest Version	Latest version available on the server
Last Updated	Date and time of the last update

Performing manual updates

Procedure

1. Go to **Administration** > **Updates** > **Component Updates** > **Manual**.
2. Deep Discovery Inspector automatically checks which components need updating.

   Any components that need updating appear in red.
3. Click the **Update** button.

   The Deep Discovery Inspector components update. When the update completes, the following confirmation message appears:

   All components are up-to-date.

Scheduled updates

Configure scheduled updates to ensure that Deep Discovery Inspector components are up-to-date.

Procedure

1. Go to **Administration** > **Updates** > **Component Updates** > **Scheduled**.
2. Select **Enable Scheduled Updates**.
3. Select the update schedule by **Hour**, **Day**, or **Week** and specify the time or day.

   Tip

   Trend Micro recommends setting the update schedule to every two hours.
4. Click **Save**.

Update source

Deep Discovery Inspector downloads components from the Trend Micro ActiveUpdate server, the default update source. Deep Discovery Inspector can be configured to download components from another update source in your organization.

When using the Trend Micro ActiveUpdate server or Trend Micro Apex Central as the update source, Deep Discovery Inspector always uses TLS 1.2 and verifies the package integrity.

When using the Trend Micro ActiveUpdate server as the update source, Deep Discovery Inspector performs an HTTPS server authentication check.

When using **Other update source** as the update source, you must enable **Always use TLS 1.2 or above** in **Administration** > **System Settings** > **Network** to use a TLS connection.

Note

You can configure Deep Discovery Inspector to download directly from Trend Micro Apex Central. For details on how the Apex Central server can act as an update source, see the *Trend Micro Apex Central Administrator's Guide*.

Configuring the update source

Procedure

1. Go to **Administration** > **Updates** > **Component Updates** > **Source**.
2. Under **Download updates from**, select one of the following update sources:
   - **Trend Micro ActiveUpdate Server**: The Trend Micro ActiveUpdate server is the default source for the latest components.
   - **Other update source**: Select this option to specify an alternative update source. The update source must begin with "http://" or "https://".

     For example:

- `http://activeupdate.example.com`
- `https://activeupdate.example.com`

Note

Update sources cannot be specified in UNC path format.

3. (Optional) Enable **Retry unsuccessful updates** and specify **Number of retry attempts** and **Retry interval**.

Product updates

Product updates include the following:

- Hot Fixes / Patches
- Service Packs / Version Upgrade

To update Deep Discovery Inspector, do any of the following:

- Upgrade the firmware from the management console or configure Deep Discovery Director to manage upgrades.

  Upgrading the firmware updates existing application files and enhances features.

  For details, see *Service packs / version upgrade on page 6-12* and *Deep Discovery Director on page 6-124*.

- Backup/restore appliance configurations.

  When backing up or restoring appliance configurations, optionally retain some previous configuration settings.

  However, data and logs are not backed up or restored, and no new features are installed. Back up existing configuration settings by exporting them to an encrypted file, and importing the file to restore settings. You can also reset Deep Discovery Inspector by restoring the default settings that shipped with the product.

  For details, see *Backup / restore on page 6-203*.

Hot fixes / patches

After an official product release, Deep Discovery Inspector may release hot fixes or patches to address issues or enhance product performance.

TABLE 6-4. Hot Fixes / Patches

SYSTEM UPDATE	DESCRIPTION
Hotfix	A hotfix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore are not released to all customers. For non-Windows hotfixes, applying a hotfix typically requires stopping program daemons, copying the hotfix file to overwrite its counterpart in your installation, and restarting the daemons.
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 hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Non-Windows patches commonly include a setup script.

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

https://downloadcenter.trendmicro.com/

Applying a hotfix or patch

The following procedure is for manual upgrades only. For more information about upgrading via Deep Discovery Director, see the Deep Discovery Director product documentation.

Procedure

1. Save the hot fix / patch file to any folder on a computer.

WARNING!

Save the hot fix / patch file with its original name to avoid problems applying it.

2. On the computer where you saved the file, access and then log on to the management console.
3. Go to **Administration** > **Updates** > **Product Updates** > **Hot Fixes / Patches**.
4. Browse to locate the hot fix / patch file.
5. Click **Upload**.

WARNING!

To avoid problems uploading the file, do not close the browser or navigate to other screens.

6. If the upload was successful, review the **Uploaded System Update Details** section.

   This section indicates the build number for the hot fix / patch that you just uploaded and if a restart is required.

Note

You will be redirected to the management console's logon screen after the update is applied.

7. If a restart is required, finish all tasks on the management console before proceeding.
8. Click **Continue** to apply the hot fix / patch.

WARNING!

To avoid problems applying the hot fix / patch, do not close the browser or navigate to other screens.

Note

If there are problems applying the system update, details will be available in the **Hot Fixes / Patches** screen, or in the system log if a restart is required.

9. If a restart is required:

   a. Log on to the management console.

   b. Go to **Administration** > **System Logs** to check for any problems encountered while applying the hot fix / patch.

   c. Go back to the **Hot Fixes / Patches** screen.

10. Clear the browser cache. For details, see *Clearing the browser cache on page 6-14*.

11. Verify that the hot fix / patch displays in the **History** section as the latest update.

    The system update also appears as the first entry in the **Hot fix / patch history** table. This table lists all the hot fixes / patches that you have applied or rolled back.

Rolling back a hotfix or patch

Deep Discovery Inspector has a rollback function to undo an update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular hot fix / patch is applied.

Only the latest hot fix / patch can be rolled back. After a rollback, no other existing hot fix / patch can be rolled back. The rollback function will only become available again when a new hot fix / patch is applied.

Note

The rollback process automatically restarts Deep Discovery Inspector, so make sure that all tasks on the management console have been completed before rollback.

Procedure

1. Go to **Administration** > **Updates** > **Product Updates** > **Hot Fixes / Patches**.

2. In the **History** section, click **Roll Back**.
3. Check the rollback result in the first row of the **Hot fix / patch history** table.

Service packs / version upgrade

Trend Micro may release new Deep Discovery Inspector firmware to enhance performance or upgrade to a new version.

Deep Discovery Inspector 6.8 and 6.8 Service Pack 1 can upgrade to version 6.8 Service Pack 2.

Deep Discovery Inspector retains existing data, logs, and configuration settings after the upgrade.

The following table outlines the available types system upgrades for Deep Discovery Inspector.

System Upgrade	Description
Service Pack	A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Non-Windows service packs include a setup program and setup script.
Version Upgrade	Upgrading the firmware updates existing application files and enhances features.

Applying a service pack or version upgrade

The following procedure is for manual upgrades only. For more information about upgrading via Deep Discovery Director, see the Deep Discovery Director product documentation.

Procedure

1. Back up appliance configuration settings. For details, see *Backup / restore on page 6-203*.
2. If you have registered Deep Discovery Inspector to Apex Central, record the Apex Central registration details.

Note

Deep Discovery Inspector migrates the current product settings after the service pack / version upgrade is complete so that you do not need to reconfigure settings. Deep Discovery Inspector re-registers to Apex Central automatically after the firmware update completes.

3. Download the Deep Discovery Inspector firmware image from the Trend Micro website or obtain the image from your Trend Micro reseller or support provider.
4. Save the image to any folder on a computer.
5. Go to **Administration** > **Updates** > **Product Updates** > **Service Packs / Version Upgrade**.
6. Browse to locate the folder where you saved the firmware image.

Tip

The image file has an `.R.tar` extension.

7. Click **Upload**.

WARNING!

Performing the next step restarts Deep Discovery Inspector. Make sure that you have finished all product console tasks before continuing.

8. Click **OK**.

   Deep Discovery Inspector upgrades the firmware and restarts.
9. Wait 5 minutes for the upgrade progress screen to load. Optionally, click **Refresh** in the browser to view the upgrade progress screen.
10. Wait for the mangement console **Log On** screen to load.
11. Clear the browser cache. For details, see *Clearing the browser cache on page 6-14*.

12. Log back on to the management console.
13. If Deep Discovery Inspector is registered to Apex Central, register the product again. For details, see *Registering to Apex Central on page 6-121*.

Clearing the browser cache

Procedure

1. On Chrome:
   a. On the browser, go to **Settings**.
   b. Click **Show advanced settings...**.
   c. Under **Privacy**, click **Clear browsing data...**.
   d. Select **Cookies and other site and plug-in data** and **Cached images and files**.
   e. Click **Clear browsing data**.
2. On Mozilla FireFox:
   a. Go to **Options** > **Privacy**.
   b. Click **Clear your recent history**.
   c. Select **Cookies** and **Cache**.
   d. Click **Clear now**.
3. On Microsoft Edge
   a. Click the Hub icon.
   b. Click the History icon.
   c. Click **Clear all history**.
   d. Select **Cookies and saved website data** and **Cached data and files**.
   e. Click **Clear**.

Notifications

Deep Discovery Inspector can send email notifications for threshold-based network events.

The following table describes the notifications available on Deep Discovery Inspector

Event	Description
Threat detections	The number of threat detections reached the specified threshold. For details, see *Threat detection notifications on page 6-16*.
High risk hosts detections	Deep Discovery Inspector identified a high-risk host on your network. For details, see *High risk hosts detections notifications on page 6-18*.
Suspicious hosts detections	The number of suspicious hosts reached the specified threshold. For details, see *Suspicious hosts detections notifications on page 6-21*.
High network traffic	Network traffic reached the specified threshold. For details, see *High network traffic notifications on page 6-22*.
Unanalyzed sample detections	Virtual Analyzer was unable to analyze samples. For details, see *Unanalyzed sample detections notifications on page 6-24*.
Virtual analyzer detections	Virtual Analyzer detected malicious content in a sample. For details, see *Virtual analyzer detections notifications on page 6-26*.
Deny list	A detection matched an object in the user-defined Deny List. For details, see *Deny list notifications on page 6-27*.
Retro Scan detections	Retro Scan detected historical callback attempts to C&C servers in the TM Global Intelligence List. For details, see *Retro scan detections notifications on page 6-29*

Event	Description
High tunneled domains	The tunneled domains list exceeds the specified threshold. For details, see *High tunneled domains notifications on page 6-30*
Low network traffic	Network traffic in the specified port fell below the configured threshold For details, see *Low network traffic notifications on page 6-31*

Threat detection notifications

Deep Discovery Inspector can send notifications when detections reach the specified threshold. Threat Detection notifications specify the number of detections for each threat type.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Threat Detections**.
2. Select **Notify Administrator if number of threat detections for:**.
3. Specify the threshold for outbound and inbound traffic.
   - **Outbound traffic**: Detections from monitored networks
   - **Inbound traffic**: Detections from outside the network
4. Select the types of threats to detect.
5. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.
6. (Optional) Modify the default subject and message body.

Important

- The message subject cannot exceed 256 characters.
- The message body cannot exceed 4,096 characters.

You can use any of the following message tokens when customizing the notification.

Message Token	Description
__LOOP_END__	End of message token loop
__LOOP_RISKS_COUNT__	Detection count
__LOOP_RISKS_DIRECTION__	Direction of network traffic
__LOOP_RISKS_NAME__	Detection type
__LOOP_RISKS_THRESHOLD__	Detection threshold
__LOOP_START__	Start of message token loop
__TIMESTAMP__	Notification date and time

Important

The following tokens repeat as needed inside message token loops:

- __LOOP_RISKS_COUNT__
- __LOOP_RISKS_DIRECTION__
- __LOOP_RISKS_NAME__
- __LOOP_RISKS_THRESHOLD__

7. Click **Save**.

High risk hosts detections notifications

Deep Discovery Inspector can send notifications when detecting high-risk hosts. A host is considered high-risk when a high severity event is detected.

Procedure

1. Add at least one monitored network group.

   For details, see *Adding network groups on page 6-99*.

2. Go to **Administration** > **Notifications** > **Notification Settings** > **High Risk Hosts Detections**.

3. Select **Notify Administrator for high risk hosts**.

4. Specify a sending interval.

   - Summarize notifications and send one notification according to a set interval.
   - Send immediately after each detection.

   Tip

   Trend Micro recommends sending summary notifications for better performance.

5. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.

6. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

   You can use any of the following message tokens when customizing the notification.

Message Token	Description
__AFFECTED_HOST__	Affected host
__BEHAVIOR__	Description of suspicious behavior
__DATE__	Threat detection date and time
__DIRECTION__	Network traffic direction
__DST_ACCOUNT__	Destination account
__DST_GROUP__	Destination group
__DST_IP_ADDR__	Destination IP
__DST_MAC_ADDR__	Destination MAC address
__DST_PORT__	Destination port
__DST_ZONE__	Destination zone
__HOSTNAME__	Host name
__HOST_IP__	High-risk host IP address
__INCIDENT_COUNT__	Number of high risk hosts
__LOG_QUERY_URL__	Link to the All Detections screen on the management console

Message Token	Description
__NETWORK_PROTOCOL__	Network protocol
__SRC_ACCOUNT__	Source account
__SRC_GROUP__	Source group
__SRC_IP_ADDR__	Source IP address
__SRC_MAC_ADDR__	Source MAC address
__SRC_PORT__	Source port
__SRC_ZONE__	Source zone
__TIMESTAMP__	Notification date and time

7. Click **Save**.

Adding to the high risk hosts detections notification exclusion list

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **High Risk Hosts Detections Notifications** > **Exclusion List**.

   The **Exclusion List** screen appears.

2. Type a host name to be excluded from notification.

3. Type an IP address or address range.

4. Click **Add**.

   The IP address or address range appears in the **Defined IP Addresses** list.

Suspicious hosts detections notifications

Deep Discovery Inspector can send notifications when detecting suspicious hosts. A host is considered suspicious when the number of detections associated with it reaches the configured threshold. Suspicious Hosts Detections notifications contain information that can help determine the cause of the increased detections.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Suspicious Hosts Detections**.
2. Select **Notify administrator if number of detections per IP address**.
3. Specify the detection threshold.

   Tip

   Trend Micro recommends using the default settings.

4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.

5. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

   You can use any of the following message tokens when customizing the notification.

Message Token	Description
__LOOP_END__	End of message token loop
__LOOP_HOST_IP__	Host IP address
__LOOP_INCIDENT_NUMBER__	Incident count
__LOOP_INCIDENT_THRESHOLD__	Incident threshold
__LOOP_START__	Start of message token loop
__TIMESTAMP__	Notification date and time

Note

The following tokens repeat as needed inside message token loops:

- __LOOP_HOST_IP__
- __LOOP_INCIDENT_NUMBER__
- __LOOP_INCIDENT_THRESHOLD__

6. Click **Save**.

High network traffic notifications

Deep Discovery Inspector can send notifications when network traffic reaches the specified threshold. Increased activity might indicate an attack on your network.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **High Network Traffic**.
2. Select **Notify Administrator if network traffic exceeds normal traffic pattern**.
3. Do one of the following:
   - Click **Auto-Detect** to allow Deep Discovery Inspector to define the normal traffic threshold.
   - Manually specify the traffic threshold for each hour of the day.

   Note

   The amount of network traffic is rounded up to the nearest whole number. For example, 1.2 GB displays as 2 GB and 2.6 GB displays as 3 GB.
4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.
5. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

   You can use any of the following message tokens when customizing the notification.

Message Tokens	Description
__TIMESTAMP__	Notification date and time
__ TRAFFIC_END_TIME__	Traffic monitoring end date and time

Message Tokens	Description
__ TRAFFIC_START_TIME__	Traffic monitoring start date and time
__ TRAFFIC_THRESHOLD__	Network traffic threshold

6. Click **Save**.

Unanalyzed sample detections notifications

Deep Discovery Inspector can send notifications when Virtual Analyzer is unable to analyze samples. Unanalyzed Sample Detections notifications provide information about each sample, the time of analysis, and the URL to be used in downloading the files.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Unanalyzed Sample Detections**.
2. Select **Notify Administrator for unanalyzed sample detections**.
3. Specify a sending interval.

   Tip

   Trend Micro recommends using the default settings.

4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.

5. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

You can use any of the following message tokens when customizing the notification.

Message Token	Description
__IP_ADDRESS__	Deep Discovery Inspector IP address
__LOOP_END__	End of message token loop
__LOOP_SAMPLE_FILE_ANALYZETIME__	Sample analysis date and time
__LOOP_SAMPLE_FILE_DOWNLOADURL__	Sample download URL
__LOOP_SAMPLE_FILE_SHA1__	File SHA-1
__LOOP_SAMPLE_FILE_SIZE__	File size
__LOOP_SAMPLE_FILE_TYPE__	File type
__LOOP_START__	Start of message token loop
__TIMESTAMP__	Notification date and time
__TOTAL_FAILED_COUNT__	Number of unanalyzed samples

Note

The following tokens repeat as needed inside message token loops:

- __LOOP_SAMPLE_FILE_ANALYZETIME__
- __LOOP_SAMPLE_FILE_DOWNLOADURL__
- __LOOP_SAMPLE_FILE_SHA1__
- __LOOP_SAMPLE_FILE_SIZE__
- __LOOP_SAMPLE_FILE_TYPE__

6. Click **Save**.

Virtual analyzer detections notifications

Deep Discovery Inspector can send notifications when a file does not match any pattern but is recognized as suspicious by Virtual Analyzer within the specified period.

Suspicious files must meet the following criteria:

- Virtual Analyzer Result: Has analysis results
- File Detection Type: Highly Suspicious File or Heuristic Detection
- Virtual Analyzer Risk Level: High, Medium, or Low

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Virtual Analyzer Detections**.
2. Select **Notify Administrator for malicious content (or threats) detected by Virtual Analyzer only**.
3. Specify a sending interval.
   - Summarize notifications and send according to a set interval.

     Select a value between 1 hour and 24 hours.

- Send immediately after each detection.

Tip

Trend Micro recommends sending summary notifications for better performance.

4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.

5. (Optional) Modify the default subject and message body.

Note

- The message body cannot exceed 4,096 characters.
- The message subject cannot exceed 256 characters.

You can use any of the following message tokens when customizing the notification.

VARIABLE	DESCRIPTION
__DETECTION_DETAIL__	Virtual Analyzer detection details
__HTTPURL__	Deep Discovery Inspector management console URL
__TIMESTAMP__	Notification date and time
__XHOURS__	Notification sending interval

6. Click **Save**.

Deny list notifications

Deep Discovery Inspector can send notifications when detecting a threat that matches any object in the Deny List within the specified period.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Deny List**.
2. Select **Notify Administrator of Deny List malicious content**.
3. Specify a sending interval.

   Select a value between 1 hour and 24 hours.

   Tip

   Trend Micro recommends using the default settings.

4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.

5. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

   You can use any of the following message tokens when customizing the notification.

Message Token	Description
__HTTPURL__	Deep Discovery Inspector management console URL
__TIMESTAMP__	Notification date and time
__XHOURS__	Notification sending interval

6. Click **Save**.

Retro scan detections notifications

Deep Discovery Inspector can send notifications when Retro Scan detects historical callback attempts to C&C servers included in the Trend Micro Global Intelligence List.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Retro Scan Detections**.
2. Select **Notify Administrator if Retro Scan detects previous callback attempts to known C&C servers**.
3. Specify a sending interval.

   Select a value between one and 30 days.

   Tip

   Trend Micro recommends using the default settings.

4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.
5. (Optional) Modify the default subject and message body.

   Note

   - The message body cannot exceed 4,096 characters.
   - The message subject cannot exceed 256 characters.

   You can use any of the following message tokens when customizing the notification.

Message Token	Description
__HTTPURL__	Deep Discovery Inspector management console URL

Message Token	Description
__RETRO_SCAN_COMPROMISED_HOST_NUM__	Number of compromised hosts
__RETRO_SCAN_C_AND_C_CALLBACK_NUM__	Number of C&C callback attempts found
__TIMESTAMP__	Retro Scan report run date and time

6. Click **Save**.

High tunneled domains notifications

Deep Discovery Inspector can send notifications when the tunneled domains list exceeds the specified threshold.

Important

High Tunneled Domains notifications are only available when Deep Discovery Inspector is in inline mode.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **High Tunneled Domains**.
2. Select **Notify administrator if the tunneled domains list exceeds the specified threshold**.
3. Specify a **Threshold** between 1 and 10,000.
4. Specify a **Notification frequency**.
5. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.
6. (Optional) Modify the default subject and message body.

Note

- The message body cannot exceed 4,096 characters.
- The message subject cannot exceed 256 characters.

You can use any of the following message tokens when customizing the notification.

Message Token	Description
__TIMESTAMP__	Notification date and time
__CURRENTNUMBER__	Number of items in the tunneled domains list
__THRESHOLDNUMBER__	Specified tunneled domains threshold
__CONSOLEURL__	Deep Discovery Inspector management console URL

7. Click **Save**.

Low network traffic notifications

Deep Discovery Inspector can send notifications when network traffic in the specified port falls below the configured threshold.

Important

Low Traffic Notifications are not available when Deep Discovery Inspector is in inline mode.

Procedure

1. Go to **Administration** > **Notifications** > **Notification Settings** > **Low Network Traffic**.
2. Select **Notify administrator if network traffic falls below the specified threshold**.

3. Configure the following settings:
   - **Threshold**: Specify a value between 1 and 10,000.
   - **Monitored ports**: Select the ports Deep Discovery Inspector monitors for low network traffic
   - **Notification frequency**: Specify how often you receive notifications when low network traffic is detected
4. (Optional) Configure the notification recipients.

   For details, see *Configuring email notification settings on page 6-33*.
5. (Optional) Modify the default subject and message body.

Note

- The message body cannot exceed 4,096 characters.
- The message subject cannot exceed 256 characters.

You can use any of the following message tokens when customizing the notification.

Message Tokens	Description
__LOOP_CURRENTNUMBER__	Network traffic of monitored port
__LOOP_END__	End of the monitored port list
__LOOP_PORTNUMBER__	Monitored port
__LOOP_START__	Start of the monitored port list

Message Tokens	Description
__THRESHOLD NUMBER__	Network traffic threshold
__TIMESTAMP__	Notification date and time

6. Click **Save**.

Delivery options

Use the **Email Settings** screen to configure the following for all notifications:

- Recipient email address
- Maximum notifications per time period
- Notification time period

Configuring email notification settings

Configure the SMTP server at **Administration** > **System Settings** > **SMTP**.

Procedure

1. Go to **Administration** > **Notifications** > **Delivery Options** > **Email Settings**.
2. Type at least one notification recipient email address.

   Use a semicolon ";" to separate multiple addresses.
3. Type the amount of maximum notifications that can be sent during the specified time period.

Tip

Trend Micro recommends using the default settings.

4. Type the amount of minutes for the notification time period.

   During every notification time period, the total amount of notifications are counted. If the total amount of notifications exceeds the specified amount of maximum notifications, then no more notifications are sent until the next time period.

   Tip

   Trend Micro recommends using the default settings.

5. Click **Save**.

Monitoring / scanning

Monitoring / Scanning settings establish filters and exclusions for the following Deep Discovery Inspector network detection features:

- *Hosts / ports on page 6-34*
- *Threat detections on page 6-36*
- *Web Reputation on page 6-42*

  For more information, see *Smart Protection on page 6-38*
- *Application filters on page 6-45*
- *Deny list / allow list on page 6-47*
- *Detection rules on page 6-56*
- *Packet capture on page 6-58*
- *Detection exceptions on page 6-60*

Hosts / ports

Configure **Hosts / Ports** to specify the network traffic that Deep Discovery Inspector monitors. Scan all traffic in your network or traffic through specified segments of your network.

Deep Discovery Inspector monitors all network traffic by default.

Monitoring specific network traffic on portions of a network can significantly reduce the number of threat- and event-related detections. For example, to scan inbound and outbound email traffic, select **Monitor specific IP ranges and/or ports** and then add a rule with the following settings:

- Source IP: **All**
- Destination IP: **All**
- Destination port: **25**

Tip

Trend Micro recommends using the default setting to monitor all network traffic.

Configuring hosts and ports

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Hosts / Ports**.
2. To monitor all traffic on a network, select **Monitor all network traffic**.
3. To monitor specific traffic on a network, select **Monitor specific IP ranges and ports** and configure the following:
   a. Under **Network Monitoring List**, click **Add**.

      The **Specify IP Ranges and Ports** screen appears.

   b. Specify the **Source IP**.
   c. Specify the **Destination IP**.
   d. Specify the **Port**.
   e. Click **Save**.

      A new entry appears in the **Network Monitoring List**.

Note

When **Source IP** or **Destination IP** is **Monitor all IP ranges and ports**, traffic initiated by reversed streams is also scanned.

Tip

For certain IP addresses, subnet prefix "/32" is required.

Threat detections

Enable or disable the following features:

- **Threat Detections**: Detects both known and potential threats. Deep Discovery Inspector enables this feature by default.
- **Outbreak Containment Service**: Enables Deep Discovery Inspector to record detection information in the logs and block network traffic.

Configuring threat detections

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Threat Detections**.
2. Select **Enable All Threat Detections**.
3. Under **Threat Detection**, select **Enable threat detections**.
4. (Optional) Select **Enable Mobile App Reputation Service (MARS) server query**.

   Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories.

Note

The MARS Service enables Deep Discovery Inspector to send detection information about mobile devices to the MARS server for analysis.

5. Under **Outbreak Containment Service**, select one of the following:

   - **Enable outbreak detection**: Does not block traffic
   - **Enable outbreak detection and block traffic**: Blocks traffic

   Outbreak Containment Service is a Trend Micro utility that detects both known and unknown malware that can potentially start an outbreak.

6. Click **Enable Smart Feedback** (recommended) to send protected threat information to the Trend Micro Smart Protection Network.

   When enabled, Trend Micro Smart Feedback shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats.

   Information from the following file types may be included in feedback:

   - class
   - cmd
   - hta
   - jar
   - js
   - lnk
   - macho
   - mov
   - ps1
   - svg
   - swf
   - vbe

- vbs
- wsf

Feedback may include product name/ID and version and detection information, including file types and SHA-1s, URLs, IP addresses, and domains.

7. Click **Save**.

Smart Protection

Trend Micro Smart Protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By integrating Web Reputation Services, Deep Discovery Inspector can obtain reputation data for websites that users attempt to access. Deep Discovery Inspector logs URLs that Smart Protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.

Note

Deep Discovery Inspector does not use the File Reputation Service that is part of Smart Protection technology.

Deep Discovery Inspector connects to a Smart Protection source to obtain web reputation data.

Reputation services are delivered through the Trend Micro Smart Protection Network and Smart Protection Server. The following table provides a comparison.

Note

For details about the supported versions of Smart Protection Server, see *Integrated Trend Micro products and services on page 6-108*.

TABLE 6-5. Smart Protection Sources

BASIS OF COMPARISON	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
Purpose	A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology	Localizes the File and Web Reputation Services to the corporate network to optimize efficiency. The Smart Protection Server also provides the following: • Certified Safe Software Service • Community Domain/IP Reputation Service • Community File Reputation • Mobile App Reputation Service • Predictive Machine Learning engine • Web Inspection Service • Web Reputation Service
Administration	Hosted and maintained by Trend Micro	Installed and managed by Trend Micro product administrators
Connection protocol	HTTPS	HTTPS
Usage	Use if you do not plan to install Smart Protection Server To configure Smart Protection Network as source, see *Configuring web reputation settings on page 6-42*.	Use as primary source and the Smart Protection Network as an alternative source For guidelines on setting up Smart Protection Server and configuring it as source, see *Setting up Smart Protection server on page 6-40*.

About Smart Protection Server

Consideration	Description
Deployment	If you have previously installed a Smart Protection Server for use with another Trend Micro product, you can use the same server for Deep Discovery Inspector. While several Trend Micro products can send queries simultaneously, the Smart Protection Server may become overloaded as the volume of queries increases. Make sure that the Smart Protection Server can handle queries coming from different products. Contact your support provider for sizing guidelines and recommendations.
IP Address	Smart Protection Server and the VMware ESX/ESXi server (which hosts the Smart Protection Server) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Deep Discovery Inspector to make sure that these IP addresses are not assigned to the Smart Protection Server.
Installation	For installation instructions and requirements, refer to the *Installation and Upgrade Guide* for Trend Micro Smart Protection Server at https://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx.

Setting up Smart Protection server

Procedure

1. Install Smart Protection Server (standalone) on a VMware ESX/ESXi server.
2. Configure Smart Protection Server settings from the Deep Discovery Inspector management console.

   For details, see *Configuring web reputation settings on page 6-42*, from Step 3.

Note

- Smart Protection Server may not have reputation data for all URLs because it cannot replicate the entire Smart Protection Network database. When updated infrequently, Smart Protection Server may also return outdated reputation data.
- Enabling this option improves the accuracy and relevance of the reputation data.
- Disabling this option reduces the time and bandwidth to obtain the data.

Managing the Smart Protection server list

When multiple Smart Protection Servers are added and a failover occurs, Deep Discovery Inspector uses only the Web Reputation Services of the failover server and does not use the other services.

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Web Reputation** > **Smart Protection Server List**.
2. To verify the connection status with a Smart Protection Server, click **Test Connection**.
3. To modify server settings:
   a. Click the server address.
   b. In the window that appears, modify the server's IP address, description, and settings.
   c. After specifying a new IP address, click **Test Connection** to confirm the connection.
   d. Click **OK**.
4. To remove a server from the list, select the server and click **Delete**.

5. To change the order in which the servers are used, click the icon in the **Order** column.
6. Click **Save**.

Web Reputation

Deep Discovery Inspector integrates the Trend Micro Smart Protection Network, a cloud-based infrastructure that determines the reputation of websites that users attempt to access. Deep Discovery Inspector logs URLs that Smart Protection technology identifies as fraudulent or known sources of threats.

Note

Web Reputation logs can be queried from **Detections** > **All Detections**.

For detailed information about Smart Protection technology and to set up a Smart Protection Server (standalone), see *Smart Protection on page 6-38*.

Configuring web reputation settings

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Web Reputation**.
2. Select **Enable Web Reputation**.
3. Select a Smart Protection source:
   - Trend Micro Smart Protection Network™

     Trend Micro Smart Protection Network is a globally-scaled, cloud-based infrastructure providing reputation services to Trend Micro products that integrate Smart Protection technology. Deep Discovery Inspector connects to the Smart Protection Network using HTTP. Select this option if you do not plan to set up a Smart Protection Server.

Important

Selecting this option allows you to enable Retro Scan, a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network. Web access logs may include undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations and may help you determine if your network is affected by attacks.

Trend Micro recommends enabling Retro Scan in step 4.

- Smart Protection Server

  Smart Protection Server (standalone) does the following:

  - Provides Web Reputation Services, Certified Safe Software Service (CSSS), Mobile App Reputation Service (MARS), and Community File Reputation as offered by Smart Protection Network
  - Relays these services to the global Trend Micro Smart Protection Network for network efficiency

  As a Trend Micro product administrator, you must set up and maintain this server. Select this option if you have already set up a server.

Important

Selecting this option disables Retro Scan and deletes all previous Retro Scan detection logs.

4. (Optional) Enable Retro Scan.

   For details, see *Enabling retro scan on page 4-51*.

5. To select Smart Protection Server, configure the **Smart Protection Server List**.

   a. Type the Smart Protection server name or IP address.

Obtain the IP address by going to **Smart Protection** > **Reputation Services** > **Web Reputation** on the Smart Protection Server console.

The IP address forms part of the URL listed on the screen.

b. (Optional) Click **Test Connection**.

c. Type a description for the server.

d. Update Smart Protection Server regularly.

On the Smart Protection server console, go to **Updates** > **Program** > **Update Schedule** and click **Enable scheduled updates**.

e. (Optional) If proxy settings for Deep Discovery Inspector have been configured for use with Smart Protection Server connections, select **Connect through a proxy server** .

Note

If proxy settings are disabled, Smart Protection Servers that connect through the proxy server will connect to Deep Discovery Inspector directly. Under the **Proxy Connection** column, the status displays "No" when proxy settings are disabled.

Note

On the proxy server, configure the following ports to allow a connection to Smart Protection Server:

- 5275
- 443

f. Click **Add**.

The Smart Protection Server is added to the **Smart Protection Server List**.

g. (Optional) Add more servers.

Note

Add up to 10 servers. If multiple servers are configured, Deep Discovery Inspector connects to servers following the order in which they appear in the list.

Tip

Trend Micro recommends adding multiple Smart Protection Servers for failover purposes. If Deep Discovery Inspector is unable to connect to a server, it attempts to connect to other servers on the Smart Protection Server List.

h. Use the arrows under the **Order** column to set server priority.

6. To filter excessive Web Reputation detections, check **Exclude Spam and Adware detections to reduce detection volume**.

   Most Web Reputation detections are related to spam and adware. Reduce detection volume by excluding spam and adware detections.

7. Click **Save**.

Application filters

Application Filters provide valuable information to quickly identify security risks and prevent the spread of malicious code.

Enable detection for the following applications:

TABLE 6-6. Application Types

APPLICATION	DESCRIPTION
Instant Messaging	Communicate and share information and files between contacts
P2P Traffic	Share files from one computer to another

APPLICATION	DESCRIPTION
Streaming Media	Play audio-visual content while downloading

Configuring application filter settings

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Application Filters**.
2. Enable detection for **Instant Messaging**.
   a. Select the **Instant Messaging** check box.
   b. Select instant message applications for detection.

      Tip
      Use the Ctrl key to select one or multiple applications.

   c. Click the >> icon to move the selected applications under **Selected Instant Messaging applications**.
3. Enable detection for **P2P Traffic**.
   a. Select the **P2P Traffic** check box.
   b. Select peer-to-peer applications for detection.

      Tip
      Use the Ctrl key to select one or multiple applications.

   c. Click the >> icon to move the selected applications under **Selected Peer-to-Peer applications**.
4. Enable detection for **Streaming Media**.

a. Select the **Streaming Media** check box.

b. Select streaming media applications for detection.

> **Tip**
> Use the Ctrl key to select one or multiple applications.

c. Click the >> icon to move the applications under **Selected streaming media applications**.

5. Click **Save**.

Deny list / allow list

To access the **Deny List** and the **Allow List**, go to **Administration** > **Monitoring / Scanning** > **Deny List / Allow List**.

The **Deny List / Allow List** screen includes the following tabs: **Deny List**, **Allow List**, and **Import/Export**.

TABLE 6-7. Deny List / Allow List Tabs

TAB	DESCRIPTION
Deny List	Deep Discovery Inspector allows you to manage the connection to entities in the **Deny List**. You can set the action for **Deny List** entities as follows: • **Monitor** • **Monitor and reset**
Allow List	Deep Discovery Inspector allows the connection to entities in the **Allow List**. **Tip** Use the **Allow List** to lower the number of false positive detections from the **Deny List**.
Import/Export	Import or export **Deny List** or **Allow List** entities.

Deny list / allow list format rules

The following format rules apply to Deep Discovery Inspector Deny Lists and Allow Lists.

Go to **Administration** > **Monitoring / Scanning** > **Deny List / Allow List**.

TABLE 6-8. Deny List / Allow List Format Rules

FORMAT RULE	DESCRIPTION
IP Address	**Syntax** • Single IP: IP addresses must be in the format: XXX.XXX.XXX.XXX, where X is a whole number between 0 and 255. IPv4 example: 192.168.1.1 IPv6 example: fd00:1:1111:200::1000 • IP Range: IP addresses must be in the format: XXX.XXX.XXX.XXX-XXX.XXX.XXX.XXX, where X is a whole number between 0 and 255. IPv4 example: 192.168.1.0-192.168.1.255 IPv6 example: fd00:1:1111:200::1000-fd00:1:1111:200::1fff • Subnet: IP addresses must be in the format: XXX.XXX.XXX.XXX/<Mask Bit>, where X is a whole number between 0 and 255, and <Mask Bit> is a whole number between 1 and 32. IPv4 example: 192.168.1.0/24 IPv6 example: fd00:1:1111:200::1000/116
	Maximum IP Address Entities Add up to 10,000 Deny / Allow List **IP Address** entities.

Format Rule	Description
Domain	**Supported Characters** Each domain name must have at least one character. Deep Discovery Inspector supports the following characters for domain names: ASCII • 0x2D (-), 0x2E (.) • 0x30 (0) ~ 0x39 (9) • 0x41 (A) ~ 0x5A (Z) • 0x61 (a) ~ 0x7A (z) UTF-8 characters (ASCII code >=0x80) **Note** Convert non-UTF8 characters to Punycode.
	Maximum Length Maximum length of each domain name: 63 characters Maximum length of domain: 255 characters
	Wildcards (*) Wildcards are only allowed in a prefix. When a wildcard is used in a prefix, it must be connected with ". ". Only one wildcard may be used in a domain. Domain matching is case-sensitive.
	Maximum Domain Entities Add up to 10,000 Deny List / Allow List **Domain** entities.

Format Rule	Description
URL	**Syntax** [http:// | https://]<Domain>[:<Port>][/<URI-prefix>] • [http:// | https://] If unassigned, the default is "http://". To match both "http://:" and "https://", create multiple rules. • <Domain> Follow the syntax of Domain deny list for DNS. • [:<Port>] (Optional) If unassigned, the default is ":80" (port 80) for HTTP or ":443" (port 443) for HTTPS. Assign a specific port with a whole number between 1 and 65,535, or use a wildcard (*) to assign all ports. • [/<URI-prefix>] (Optional) If unassigned, the default is a wildcard that matches all paths. Use "/" and "/*" to match a URL without a path. Example: `www.abc.com/*` matches `www.abc.com` [/<URI-prefix>] is always applied as a prefix matching. Only one wildcard is accepted in a prefix. URI matching is not case-sensitive.
	Maximum URL Entities Add up to 10,000 Deny / Allow List **URL** entities.

Format Rule	Description
SHA-1	**Syntax** Deep Discovery Inspector supports the following characters for SHA-1 rules: ASCII • 0x30 (0) ~ 0x39 (9) • 0x41 (A) ~ 0x46 (F) • 0x61 (a) ~ 0x66 (f)
	Maximum Length Maximum length of a SHA-1 rule: 40
	Maximum SHA-1 Entities Add up to 10,000 Deny / Allow List **SHA-1** entities.

Configure deny lists and allow lists

Configure the following functions on the **Deny List** and **Allow List** screens:

- **View**
- **Add**
- **Delete**
- **Status**
- **Edit**
- **Priority** (**Deny List** only)

In addition, you can query different entities with **Search**.

To save changes and apply all updates, click **Reload**.

Configure deny lists and allow lists

Procedure

1. Configure **View** to display one of the following Deny List / Allow List entities.
   - **Files**
   - **IP Addresses**
   - **URLs**
   - **Domains**

   (Optional) For **Allow List**, choose **All**.
2. Click **Add** to open the **Add Item to Deny List**/**Add Item to Allow List** screens.
   a. Under **Type**, choose **File**, **IP Address**, **URL**, or **Domain**.
   b. Type a value in the appropriate text box.

List Type	Name Type
Files	SHA-1
IP Addresses	IP Address
URLs	URL
Domains	Domain

Note

To configure the maximum file size, go to **Administration** > **System Maintenance** > **Storage Maintenance**.

   c. (**Deny List** only) Set an **Action** to manage the connection to the new entity.

List Type	Action
Files	**Monitor**
IP Addresses	• **Monitor** • **Monitor and reset**
URLs	• **Monitor** • **Monitor and reset**
Domains	• **Monitor** • **Monitor and reset**

d. (Optional) Add a comment.

3. To remove one or more **Deny List** or **Allow List** entities, click **Delete**.

   Deleted entities are removed from the database.

4. Enable or disable the status of a **Deny List** or **Allow List** entity.

5. To edit **Type**, **IP Address/SHA-1**, comments, and **Action** (**Deny List** only), click a **Deny List** or **Allow List** entity.

6. (Optional: **Deny List** only) To change the priority of a **Deny List Entity**, click the icon next to its priority number.

   The priority number indicates the order that a **Deny List Entity** is matched to detections. Priority numbers are sequential in numerical order. Smaller numbers match first.

7. To query different Deny/Allow List entities, specify an IP Address, SHA-1, Domain, or URL.

   Note

   To search for a SHA-1 entity, type the exact value. For IP Address, Domain, or URL entities, Deep Discovery Inspector matches partial values.

8. To apply all updates and retain changes, click **Reload**.

Note

For optimum performance, use the **Reload** button when updating a **Deny List / Allow List**.

Format rules for importing deny lists / allow lists

The following format rules apply to importing Deep Discovery Inspector Deny Lists and Allow Lists.

Go to **Administration** > **Monitoring / Scanning** > **Deny List / Allow List** > **Import/Export**.

TABLE 6-9. Format Rules for Importing Deny Lists / Allow Lists

FORMAT RULE	DESCRIPTION
Comments	Comments are limited to 64 characters.
Duplicate Files	You can import duplicate files.
CSV Format	Deep Discovery Inspector supports only standard .csv format. Use comma separation and UTF-8 encoding.

For all other Deny List / Allow List format rules, refer to *Deny list / allow list format rules on page 6-48*.

Exporting custom deny lists / allow lists

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Deny List / Allow List** > **Import/Export**.
2. Select the **Import/Export** tab.
3. To export a Deny List, click **Export Deny List**, and then click **Export**.

   Deep Discovery Inspector exports a .csv file that includes all custom Deny Lists.

4. To export an Allow List, click **Export Allow List**, and then click **Export**.

   Deep Discovery Inspector exports a .csv file that includes all custom Allow Lists.

Importing custom deny lists / allow lists

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Deny List / Allow List** > **Import/Export**.
2. Select the **Import/Export** tab.
3. (Optional) Prepare a .csv file.

   Do one of the following:

   - Prepare a custom Deny List.

     Prepare a .csv file that includes the following fields: **Status**, **Priority**, **Deny List Entity**, **Source Type**, **Type**, **Action**, **Comments**, and **Last Modified**

   - Prepare a custom Allow List.

     Prepare a .csv file that includes the following fields: **Status**, **Allow List Entity**, **Source Type**, **Type**, **Comments**, and **Last Modified**

   Status

   - 0: Disable
   - 1: Enable

   Source Type

   - 0: User-defined
   - 1: Virtual Analyzer
   - 2: C&C Callback

   Action (Deny List only)

- 0: Monitor
- 1: Monitor and reset

Note

If you do not input a value for **Status**, **Source Type**, and **Action**, default values are applied as follows:

- **Status**: `1`
- **Source Type**: `0`
- **Action**: `0`

4. Browse to select a file.

   The file format is segregated by "," and is encoded by UTF-8.

Note

The .csv file, type, and allow list entity fields must be populated with a valid entity. Select **File**, **IP address**, **URL**, or **Domain** as **Type**.

For **Status** and **Action**, only `0` and `1` are valid characters. For **Source Type**, only `0`, `1`, and `2` are valid characters. If you use any other characters, the import attempt will return an error.

5. Click **Import**.

   The current selected list is overwritten.

Detection rules

Customize threat detections by enabling and disabling detection rules.

Tip

- You can manage the detection rules of your appliances from Network Inventory in Trend Vision One. For more information, see the Trend Vision One online help.
- Learn more about detection rules, by accessing the threat encyclopedia.

  To access the Threat Encyclopedia, in the management console go to **Help** > **Threat Encyclopedia** > **Network Content Inspection Rules** or search for a specific rule number.

The following table outlines the available actions to configure detection rules in the **Detection Rules** screen (**Administration** > **Monitoring / Scanning** > **Detection Rules**).

Action	Description
Export Detection Rules settings	Click **Export** to download a file containing your current Detection Rules settings.
Import Detection Rules settings	Click **Import** to import and replace all Detection Rules settings from file containing Detection Rules settings.
Change specific rule settings	Click an icon in the **Current** column to change the setting of specific rules, and then click **Save Changes**.
Change all rules to Default Status	Select **Default Status** from the **Change all rules to** menu, and then click **Save Changes**. This sets detection rules to default settings. Trend Micro recommends using the Default Status setting.
Enable all detection rules	Select **Enabled** from the **Change all rules to** menu, and then click **Save Changes** to enable all detection rules.
Disable all detection rules	Select **Disabled** from the **Change all rules to** menu, and then click **Save Changes** to disable all detection rules.
View rule details	In the **ID** column, click the detection rule number to view more details about the rule in the Threat Encyclopedia.

Packet capture

Note

This setting is not available when Deep Discovery Inspector is connected to Trend Vision One.

Deep Discovery Inspector captures not only detected traffic but also traffic related to the client or server involved in the connection at the time of detection.

Trend Micro recommends using this feature sparingly. Capturing too many network packets might consume processing capability and disk space.

The following table outlines the actions available in the **Packet Capture** screen.

Action	Description
Enable packet capture	Select **Enable packet capture** to capture TCP/UDP packets that linked to specific detections. **WARNING!** Enabling this feature requires restarting the appliance.
Add a packet capture rule	Click **Add** to create a new packet capture rule. For more information, see *Adding a packet capture rule on page 6-59*
Delete a packet capture rule	Select one or more packet capture rules from the list and click **Delete**.
Import packet capture rules	Click **Import** to import packet capture rules from other Deep Discovery Inspector appliances.
Export packet capture rules	Click **Export** to download all the packet capture rules of your Deep Discovery Inspector appliance.

Tip

- You can download packet capture files for the specified detections on the **Detection Details** screen.
- In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection. For details, see *All detections - detection details - connection details on page 4-63* and *Connection details on page 4-14*.

Adding a packet capture rule

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Packet Capture**.
2. Click **Add**.

   A new screen appears.
3. Select **Enable**.
4. Specify the rule priority.
5. (Optional) Type a **Description**.
6. Type one or more IP addresses, or IP address ranges.

   Note

   Only packets for detections of the specified addresses or within the specified ranges are captured.

   You can add a maximum of 50 entries that can be IP addresses or IP address ranges.
7. In **Detection Criteria**, do nothing to apply the rule to any detection, or click **add specific criteria**.
8. If you clicked **add specific criteria**, specify the criteria.

- Detection Type
- Detection Rule ID
- Threat/Detection/Reference

Note

Contains and **Does not contain** match partial strings. **Equals** does not match partial strings.

- Severity

Note

Click "+" to add additional criteria. Alternatively, click "-" to remove criteria.

You can add a maximum of 10 criteria.

9. Select the action to perform when packets match the criteria.
   - **Capture**
   - **Do not capture**
10. Click **Add**.

Detection exceptions

Detection Exceptions contains a list of exception criteria. Detections that match any of the enabled criteria are not recorded in the logs.

Configuring detection exceptions

Important

Configuring detection exceptions is not available when Deep Discovery Inspector is connected to and managed from Network Inventory.

Procedure

1. Go to **Administration** > **Monitoring / Scanning** > **Detection Exceptions**.
2. (Optional) Add a detection exception.
   a. Click **Add**.

      The **Add Exception** window appears.

   b. Select the **Status**.

      - **Enabled**: enable the detection exception.
      - **Disabled**: disable the detection exception.

   a. (Optional) For **Description**, type your own description about the detection exception.

   b. For **Exception criteria**, specify the criteria for the detection exception. Click **+** to add additional criteria.

      Use `TAB` or `ENTER` as the delimiter to specify multiple values.

      Use the **contains** operator to match a partial string, use the **in** operator to match an exact string, or use the **end with** operator to match a domain name. Deep Discovery Inspector uses case-insensitive string matching.

      Examples:

      - Host Name - In - `abc,DEF`

        This criteria matches any host name that is exactly (case-insensitive) "abc" or "def".

        - "abc" is matched
        - "deF" is matched
        - "abcxyz" is not matched
        - "xyzdEf" is not matched

      - Host Name - Contains - `abc,DEF`

This criteria matches any host name that contains (case-insensitive) "abc" or "def" in any part of the host name.

- "abc" is matched
- "deF" is matched
- "abcxyz" is matched
- "xyzdEf" is matched

- Domain - End with - `trendmicro.com`

  This criteria matches any domain that ends with (case-insensitive) "trendmicro.com"

  - "www.trendmicro.com" is matched
  - "www.NOTrendmicro.com" is matched
  - "www.trendmicro.com.tw" is not matched

c. Click **Add**.

The **Add Exception** window closes.

d. Click **Save**.

3. (Optional) Delete one or more detection exceptions.

   a. Select each checkbox next to the detection exceptions that you want to delete.

   b. Click **Delete**.

   c. Click **Save**.

4. (Optional) Click **Export All** to save a file containing all the detection exceptions criteria.

5. (Optional) Import detection exceptions.

WARNING!

Importing detection exceptions replaces all current detection exceptions.

Trend Micro recommends creating a backup of your current detection exceptions using the **Export All** feature.

a. Click **Import**.

   The **Import to Detection Exceptions** window appears.

b. Select a file containing detection exceptions criteria.

c. Click **Import and Replace**.

6. (Optional) Edit a detection exception.

   a. Click the icon in the **Edit** column next to the item that you want to edit.

      The **Edit Exception** window appears.

   b. Edit the detection exception.

   c. Click **Save**.

      The **Edit Exception** window closes.

   d. Click **Save**.

7. (Optional) Enable or disable a detection exception.

   a. Click the icon in the **Status** column to switch the status.

   b. Click **Save**.

TLS traffic inspection

Important

To use TLS traffic inspection, your Deep Discovery Inspector appliance must support inline deployment. For details, see the *Installation and Deployment Guide*.

Use TLS traffic inspection with Deep Discovery Inspector deployed inline to decrypt and inspect TLS traffic. TLS traffic inspection supports IPv4, VLAN, and TLS. When Deep Discovery Inspector is deployed inline and TLS traffic inspection is not enabled, traffic flowing through the inline ports is not inspected.

Deep Discovery Inspector does not support inline and out-of-band deployment at the same time. To inspect traffic, you must either enable TLS traffic inspection and use the inline ports, or disable TLS traffic inspection and mirror traffic to the data ports.

Deep Discovery Inspector does not have the ability to block traffic. Deep Discovery Inspector can only inspect traffic.

Use the following screens to configure TLS traffic inspection.

- To configure general TLS traffic inspection settings, go to **Inspection Settings** screen.

  For details, see *Inspection settings on page 6-65*.

- To configure certificates for TLS traffic inspection, go to the **Certificate Management** screen.

  Note

  You must configure a Trusted CA Certificate and Signing Certificate for TLS traffic inspection.

  For details, see *Certificate management on page 6-66*.

- To configure the decryption policy for TLS traffic inspection, go to the **Decryption Policy** screen.

  For details, see *Decryption policy on page 6-68*.

To view the amount of TLS traffic decrypted by Deep Discovery Inspector, see the "appliance information at a glance" section or the **Monitored Network Traffic in Past 30 Days** widget. For details see, *Monitored network traffic in past 30 days on page 3-15* and *Management console on page 2-3*.

Note

When TLS traffic inspection is enabled, **scanned traffic** in Deep Discovery Inspector refers to traffic that flowed through the inline ports and was decrypted by Deep Discovery Inspector

Inspection settings

On the **Inspection Settings** screen, you can configure the following:

Setting	Description
Enable TLS traffic inspection	Toggle to enable or disable. When enabled, Deep Discovery Inspector becomes an inline appliance to monitor encrypted outbound traffic. Before enabling the setting, you must configure a decryption policy. For details, see *Decryption policy on page 6-68*.
Enable domain tunneling	Toggle to enable (default) or disable. TLS connections that Deep Discovery Inspector is unable to inspect, appear in the tunneled domain list. When enabled, Deep Discovery Inspector does not inspect new connections between a client-domain pair in the tunneled domain list for the next 24 hours. If an inspection of a TLS connection to a domain or URL is unsuccessful and the domain or URL is trusted, then you can configure it as an **Exception** in the **Domain Objects** section in the **Decryption Policy** screen.

Configuring tunneled domains

To view a list of domains whose TLS traffic Deep Discovery Inspector has attempted to decrypt and inspect, go to **Administration** > **Monitoring/**

Scanning > **TLS Traffic Inspection** > **Inspection Settings** and then click on **Configure tunneled domains**.

To not decrypt TLS traffic for a domain, click **Move to Domain Exceptions** or add the domain to the **Domain Objects** > **Exceptions** list on the **Decryption Policy** screen.

Tip

To include all sub-domains in the domain exception, specify the domain in the **Decryption Policy** screen and use the wildcard (*) character.

Certificate management

For TLS traffic inspection, you must configure a Trusted CA Certificate and a Signing Certificate. For more details, see the following topics.

- *Trusted CA certificates on page 6-66*
- *Signing certificate on page 6-67*

Trusted CA certificates

Deep Discovery Inspector behaves like a proxy on the behalf of the client to verify the server certificate when inspecting TLS traffic. For Deep Discovery Inspector to verify the server, you must import a Trusted CA Certificate. If you do not import a Trusted CA Certificate, Deep Discovery Inspector will not be trust the server and therefore will not connect to the server.

To manage trusted CA certificates, go to **Administration** > **Monitoring/Scanning** > **TLS Traffic Inspection** > **Certificate Management** > **Trusted CA Certificates**. You must have one valid trusted CA certificate for Deep Discovery Inspector to decrypt TLS traffic.

Deep Discovery Inspector only supports the following formats for trusted certificates:

- PEM
- DER

- PKCS#7

Note

The Deep Discovery Inspector back up and restore operations, and Deep Discovery Director configuration replication do support trusted certificate configuration.

On the **Trusted CA Certificates** screen, you can do the following:

Action	Description
Add	Add a new certificate.
Delete	Delete the selected certificates.
Import	Import new certificates.
Export All	Export all of the certificates.
Refresh	Refresh the list of certificates.
Search subject	Search the list based on a certificate subject.

Signing certificate

The client connects to the server through Deep Discovery Inspector when TLS traffic inspection is enabled. For the client to trust Deep Discovery Inspector, you must import a Signing Certificate.

To manage the signing certificate that Deep Discovery Inspector uses to decrypt TLS traffic, go to **Administration** > **Monitoring/Scanning** > **TLS Traffic Inspection** > **Certificate Management** > **Signing Certificate**.

Important

The Deep Discovery Inspector back up and restore operations, and Deep Discovery Director configuration replication do not support signing certificate configuration.

You can do one of the following to configure the Signing Certificate.

- Directly import the certificate downloaded from Deep Discovery Inspector
  1. Click **Download Certificate** to download the Deep Discovery Inspector self-generated certificate.
  2. Import the certificate on the client.
- Use a Certificate Signing Request (CSR)
  1. Click **Generate CSR** to generate and download a Signing Certificate.
  2. Sign the CSR using the user's private key and certificate to generate a Signing Certificate.
  3. Click **Import and Replace Certificate** to import the Signing Certificate in to Deep Discovery Inspector.
  4. On the client, import the user's certificate that signed the CSR.

To remove, instead of replace, a private key and Signing Certificate, you must reset the appliance to the default settings. For details, see *Restoring default settings on page 6-206*.

Decryption policy

Go to **Administration** > **Monitoring/Scanning** > **TLS Traffic Inspection** > **Decryption Policy** to specify which traffic to decrypt and which traffic to except from decryption.

You can perform the follow actions on the **Decryption Policy** screen:

Section	Decrypt or Exceptions	Action or Setting	Description
All	All	**Import Policy**	Import a policy.
All	All	**Export Policy**	Export a policy to create a backup or use in another appliance.

Section	Decrypt or Exceptions	Action or Setting	Description
All	All	**Save**	Save the current policy settings.
Client IP Addresses	Decrypt	**Add**	Add a client IP address to decrypt.
Client IP Addresses	Decrypt	**Import**	Import client IP addresses to decrypt.
Client IP Addresses	Decrypt	**Export All**	Export all client IP addresses from the decrypt list.
Client IP Addresses	Decrypt	**Delete**	Delete selected client IP addresses from the decrypt list.
Client IP Addresses	Decrypt	**Search IP or description**	Search for the specified client IP address or description in the decrypt list.
Client IP Addresses	Exceptions	**Add**	Add a client IP address to exceptions.
Client IP Addresses	Exceptions	**Import**	Import client IP addresses to exceptions.
Client IP Addresses	Exceptions	**Export All**	Export all client IP addresses from exceptions.
Client IP Addresses	Exceptions	**Delete**	Delete selected client IP addresses from exceptions.

SECTION	DECRYPT OR EXCEPTIONS	ACTION OR SETTING	DESCRIPTION
Client IP Addresses	Exceptions	**Search IP or description**	Search for the specified client IP address or description in exceptions.
Server Ports	Decrypt	• **Any** • **Custom**	Select **Any** to decrypt connections to any server port, or select **Custom** and specify specific ports.
Server Domain Categories **Note** Server Domain Categories is disabled when using a Smart Protection Server. For details, see *Configuring web reputation settings on page 6-42*.	• **Decrypt** • **Not decrypt**	• **Any** • **None** • **Custom**	Select which server domain categories to decrypt or not decrypt.
Domain Objects	Decrypt	**Any**	Select to decrypt any connection to a domain.

Section	Decrypt or Exceptions	Action or Setting	Description
Domain Objects	Decrypt	**None**	Select to decrypt no connections based on domain.
Domain Objects	Decrypt	**Custom**	Select to specify which connections to decrypt based on domain. You can do the following: • **Add** a domain name or IP address • **Delete** selected domains from the list • **Import** a list of domain IP addresses and domain names • **Export All** domains in the list • **Search domain** in the list
Domain Objects	Exceptions	**Add**	Add a domain name or IP address
Domain Objects	Exceptions	**Delete**	Delete selected domains from the list
Domain Objects	Exceptions	**Import**	Import a list of domain IP addresses and domain names
Domain Objects	Exceptions	**Export All**	Export All domains in the list

Section	Decrypt or Exceptions	Action or Setting	Description
Domain Objects	Exceptions	**Search domain**	Search for a domain in the list

Virtual Analyzer

Virtual Analyzer provides an isolated virtual environment to manage and analyze samples with no network risk. Virtual Analyzer uses system images to observe sample behavior and characteristics, and then assigns a risk level to the sample.

Deep Discovery Inspector can use both internal and external virtual analyzers, including those built into other Trend Micro products.

When file submission to Virtual Analyzer is enabled, the maximum storage file size increases to 15 MB to minimize dropped file occurrences. Deep Discovery Inspector drops a file if the size exceeds the value set in the **File Size Settings** screen.

To modify the maximum storage file size, go to **Administration** > **System Maintenance** > **Storage Maintenance** > **File Size Settings**.

Types of virtual analyzer

Important

The availability of **Internal Virtual Analyzer** and **Sandbox as a Service** depends on your model and license.

The following table lists the types of Virtual Analyzer Deep Discovery Inspector can submit files to:

Type	Description
Internal	The virtual analyzer built into Deep Discovery Inspector.

Type	Description
External	The virtual analyzer from other Trend Micro products. For details about supported external Virtual Analyzer products, see *Integrated Trend Micro products and services on page 6-108*.
Sandbox as a service	A cloud-based sandbox service Trend Micro provides.
Trend Vision One — Sandbox Analysis	The sandbox service offered in Trend Vision One. For more information about Sandbox Analysis, see the Trend Vision One online help at https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sandbox-analysis

Internal Virtual Analyzer configuration

Important

The availability of this type of Virtual Analyzer depends on your Deep Discovery Inspector model and license.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Setup**.
2. Select **Submit files to Virtual Analyzer**.
3. In the **Virtual Analyzer** menu, select **Internal**.
4. Specify the settings for the selected Virtual Analyzer:
   a. Select a network type.

      Virtual Analyzer requires an internet connection to query Trend Micro cloud-based services (for example, Web Reputation Service) for available threat data. The network type determines the internet connectivity of Virtual Analyzer.

      The following table describes the available network types:

NETWORK TYPE	DESCRIPTION
Custom network (recommended)	Configure a specific port for Virtual Analyzer traffic. Specify a port that can connect to outside networks. Make sure that there are no port conflicts. **WARNING!** The custom network should be independent of the management network and other internal networks so malicious samples in the custom network do not affect hosts in the other networks.
Management network	Virtual Analyzer connects to the internet using the Deep Discovery Inspector management port.
No network	Virtual Analyzer has no internet connection and relies only on the analysis engine.

b. Configure a dedicated proxy for the internal Virtual Analyzer.

To configure the proxy settings, select **Management network** or **Custom network** as the network type.

1. In **Proxy Setting** select **Use dedicated proxy settings**.
2. In **Server address**, type the IP address, host name, or FQDN of the proxy server.

   Virtual Analyzer supports HTTP and HTTPS proxy servers.
3. Type the port number.
4. If the proxy requires authentication, specify the authentication credentials of the proxy server.

c. Click **Test Connection**.

5. Click **Save**.

6. To verify the internal Virtual Analyzer has connection to the internet, click **Test internet Connectivity**.

Tip

Trend Micro recommends testing the internet connectivity every time you change the settings.

7. If you want to analyze samples that might affect macOS, go to **Internal Virtual Analyzer** > **Sandbox for macOS** and turn on **Send possible threats for macOS to Trend Micro Sandbox as a Service for analysis**.

External Virtual Analyzer Configuration

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Setup**.
2. Select **Submit files to Virtual Analyzer**.
3. In the **Virtual Analyzer** menu, select **External**.
4. Specify the settings for the selected Virtual Analyzer:
   a. Specify the IP address and port number of the Virtual Analyzer appliance.
   b. Specify the API key from the external Virtual Analyzer.

      You can get the API key from the external Virtual Analyzer.
   c. Click **Test Connection**.
5. Click **Save**.

Sandbox as a Service Configuration

Important

The availability of this type of Virtual Analyzer depends on your Deep Discovery Inspector model and license.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Setup**.
2. Select **Submit files to Virtual Analyzer**.
3. In the **Virtual Analyzer** menu, select **Sandbox as a Service**.
4. By default, the proxy setting is enabled when you select **Sandbox as a Service**. If a proxy is not configured, Deep Discovery Inspector still connects to the service.
   a. Click **Test Connection**.
5. Click **Save**.

Trend Vision One — Sandbox Analysis configuration

Important

- The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation.
- Send to sandbox is a paid feature and requires allocating credits to enable.

Procedure

1. Connect your Deep Discovery Inspector appliance to Trend Vision One.

   For more information, see *Trend Vision One on page 6-109*.
2. On the **Trend Vision One** console, go to **Network Security** > **Network Inventory** > **Deep Discovery Inspector**
3. Configure **Send to Sandbox** in the supported appliances.
   a. Select one or more supported Deep Discovery Inspector appliances.
   b. Click **Configure Sandbox Settings** > **Turn on Send to Sandbox**.

c. Review the credit requirements and click **Enable**.

Trend Vision One configures your Deep Discovery Inspector appliances to use Sandbox Analysis as the virtual analyzer.

Important

When **Send to sandbox** is enabled:

- You cannot select a virtual analyzer in **Administration** > **Virtual Analyzer** > **Setup**.
- The **Proxy setting** in **Administration** > **Virtual Analyzer** > **Setup** is enabled automatically.

File submissions

To reduce the number of files in the Virtual Analyzer queue, enable Certified Safe Software Service (CSSS) and configure file submission rules.

Deep Discovery Inspector submits files based on the following configurations:

- **General Submission Settings**: By default, Deep Discovery Inspector checks files against CSSS before submitting to Virtual Analyzer.
- **File Submission Rules**: Deep Discovery Inspector checks all files submitted to Virtual Analyzer according to the configured rule criteria.

Certified safe software service

Certified Safe Software Service (CSSS) is the Trend Micro cloud database of safe files. Deep Discovery Inspector queries Trend Micro datacenters to check submitted files against the database.

When CSSS is enabled, Deep Discovery Inspector prevents safe files from entering the Virtual Analyzer queue. Benefits include the following:

- Saved computing time and resources
- Fewer false positive detections

Tip

Certified Safe Software Service is enabled by default. Trend Micro recommends using the default settings.

File submission rules

Deep Discovery Inspector allows you to create file submission rules to reduce the number of files in the Virtual Analyzer queue. To ensure that only suspicious files are analyzed, file submission rules check files based on detection types, detection rules, and file properties.

File submission rules contain the following elements:

- **Status**: “Enabled” or “Disabled”
- **Priority**: Position of a rule in the overall list
- **Criteria**: Set of conditions that a file must satisfy before the specified action is taken
- **Action**: "Submit" or "Do not submit files"

Deep Discovery Inspector checks a file against each rule in the list until finding a match. If you do not add any rules, Deep Discovery Inspector uses the following default rules.

TABLE 6-10. Default Submission Rule Elements

RULE TYPE	CRITERIA	ACTION
Basic	Known malware	Do no submit files
Basic	No detection types AND CHM / JAR / JAVA Applet / LNK / Mach-O / WIN_EXE	Submit files
Basic	No detection types AND HTTP AND *.vbs / *.vbe / *.ps1 / *.hta / *.wsf	Submit files

Rule Type	Criteria	Action
Basic	No detection types AND SMTP AND *.vbs / *.vbe / *.ps1 / *.hta / *.wsf / *.js / *.jse / *.bat / *.cmd / *.html / *.htm	Submit files
Basic	No detection types AND SMTP AND SWF	Submit files
Advanced	Rule 28/29/40/52	Do not submit files
Basic	Heuristic detections / Highly suspicious files	Submit files

File submission rule types and criteria

Deep Discovery Inspector provides two types of file submission rules. Each rule type requires a specific set of criteria.

- **Basic**: Checks files based on detection type and other properties
- **Advanced**: Checks files based on detection rules and other properties

Select the following optional criteria when creating basic or advanced file submission rules.

1. Protocol
    - Common Internet File System (CIFS)
    - File Transfer Protocol (FTP)
    - Hypertext Transfer Protocol (HTTP)
    - Instant Messaging (IM)
    - Internet Message Access Protocol (IMAP)
    - Post Office Protocol 3 (POP3)
    - Simple Mail Transfer Protocol (SMTP)
2. File Type

Option	File Type	Example File Extensions
7zip	7-zip archive	.7z
ALZ	ALZip compressed file	.alz
BZIP2	BZIP2 archive	.bz2
CHM	Compiled HTML (CHM) help file	.chm
EGG	ALZip archive file	.egg
ELF	Executable and Linkable Format binary file	.elf
JAR	Java™ Archive	.jar
Java Applet	Java™ class file	.class
LNK	Microsoft™ Windows™ Shell Binary Link shortcut Microsoft™ Windows™ 95/NT shortcut	.lnk
Mach-O	Mach-O x86/x64	No extension for most executables
Mac OS X Installer Package	Mac OS X Installer Package	.pkg
OFFICE	Microsoft Office file	.doc .docx .ppt .pptx .xls .xlsx
OpenDocument	Open Document file	.odt .odp .ods

Option	File Type	Example File Extensions
PDF	Adobe™ Portable Document Format (PDF)	.pdf
RAR	RAR archive	.rar
SWF	Adobe™ Shockwave™ Flash file	.swf
TAR	TAR archive	.tar
WIN_EXE	Windows executable file	.exe
ZIP	PKWARE PKZIP archive (ZIP)	.zip

Note

To submit Mac OS X Installer Packages, you must select **Mac OS X Installer Package** for the **File Type** option and specify pkg for the **File Extension** option.

3. File Extension

   Type one or more file extensions. Separate multiple entries with a comma (,).

4. File Size

   Specify a value that is less than or equal to the maximum file size configured at **Administration** > **System Maintenance** > **Storage Maintenance** > **File Size Settings**.

5. Direction

   - **Internal hosts**: Hosts in monitored networks
   - **External hosts**: Hosts outside the network

6. Src / Dest IP

   - All
   - Specific IP address

- IP address from any monitored network group

7. URL

   Type up to 20 URLs. Separate multiple entries with a comma (,).

   Syntax: [http://]<Domain>[:<Port>][/<URI-prefix>]

   - [http://]

     Accepted and ignored

   - <Domain>

     Wildcards (*) are only allowed in a prefix. When a wildcard is used in a prefix, it must be connected with ". ". Only one wildcard may be used in a domain.

   - [:<Port>]

     (Optional) If unassigned, the default is ":80" (Port 80).

     Assign a specific port with a whole number between 1 and 65,535, or use a wildcard (*) to assign all ports.

   - [/<URI-prefix>]

     (Optional) If unassigned, the default is a wildcard that matches all paths.

     Use "/" and "/*" to match a URL without a path.

     Example: `www.abc.com/*` matches `www.abc.com`

     [/<URI-prefix>] is always applied as a prefix matching. Only one wildcard is accepted in a prefix.

     URI matching is not case-sensitive.

Tip

If you add URL criteria, Trend Micro recommends also adding a new criteria for **Protocol**. For example, add **HTTP** or email related protocols.

File submission rules screen

You can perform any of the following actions on the **File Submission Rules** screen:

- **Add**: Add a maximum of 1000 rules.
- **Import**: Import rules that were exported from any Deep Discovery Inspector appliance.

  Note

  Importing replaces all existing rules. Trend Micro recommends creating a backup of all existing rules before importing.

- **Export**: Export rules for backup or for importing to other Deep Discovery Inspector appliances.

  Note

  Deep Discovery Inspector exports rules to a .dat file.

- **Reset**: Delete all user-defined rules and retain default rules.
- **Edit**: Enable or disable rules and edit rule components.

Adding a file submission rule

Deep Discovery Inspector supports a maximum of 1000 rules.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **File Submissions**.
2. Under **File Submission Rules**, click **Add**.

   The **New Submission Rule** window appears.
3. Select **Enable submission rule**.
4. Under **Criteria**, select one of the following:

- **Basic**: Checks files based on detection type and other properties
- **Advanced**: Checks files based on detection rules and other properties

5. (Optional) For **Basic**, select at least one of the following detection types:
   - **No detection types**: Files that did not trigger any Deep Discovery Inspector detection rules

     Note

     Select this option to search for files that meet certain criteria but do not have detections.

   - **Any of the following:**

     Note

     Select at least one detection type.

     - **Known malware**: Malicious files that are detected through signature-based methods
     - **Heuristic detections**: Suspicious files that are detected through heuristic analysis
     - **Highly suspicious files**: Files exhibiting highly suspicious behavior that are detected through detection rules
6. (Optional) For **Advanced**, click **Select** and check at least one detection rule.

   For details about Deep Discovery Inspector detection rules, go to **Administration** > **Monitoring / Scanning** > **Detection Rules**.
7. (Optional) Click **New Criteria**.
8. Select any of the following criteria and configure the applicable settings.
   - **Protocol**: Select at least one protocol.

- **File type**: Select at least one file type.
- **File extension**: Type one or more file extensions. Separate multiple entries with a comma (,).
- **File size**: Specify a value that is less than or equal to the maximum file size configured at **Administration** > **System Maintenance** > **Storage Maintenance** > **File Size Settings**.
- **Direction**:
  - Internal hosts
  - External hosts
- **Src / Dest IP**: For both source and destination, click **Select** and select one of the following:
  - All
  - Specify IP address
  - Select from monitored network groups
- **URL**: Type up to 20 URLs. Separate multiple entries with a comma (,).

Tip

If you add URL criteria, Trend Micro recommends also adding a new criteria for **Protocol**. For example, add **HTTP** or email related protocols.

9. Select the action that Deep Discovery Inspector takes when the file meets the configured criteria.
10. Specify the rule priority. Type a number between one and the total number of rules.
11. Click **Add**.

Internal Virtual Analyzer

Some Deep Discovery Inspector models provide an internal Virtual Analyzer that you can enable any time.

Before using Deep Discovery Inspector, import images and configure the internal Virtual Analyzer settings.

Note

No settings under **Internal Virtual Analyzer** apply to an external Virtual Analyzer nor Sandbox as a Service. For details about external analysis modules, refer to the applicable product Administrator's Guide.

Internal Virtual Analyzer contains the following screens:

- Sandbox Management
- YARA Rules

Sandbox management

The **Sandbox Management** screen contains the following tabs:

- Status
- Images
- Passwords
- Sandbox for macOS

Note

No settings under **Sandbox Management** apply to an external Virtual Analyzer nor Sandbox as a Service. For details about external analysis modules, refer to the applicable product Administrator's Guide.

Virtual Analyzer status

The **Status** tab provides the following information:

1. Current overall status of Virtual Analyzer
   - Initializing...
   - Starting...
   - Configuring...
   - Importing images...
   - Stopping...
   - Stopped
   - Running
   - No active images
   - Disabled
2. Status of each image, including the number of deployed instances, state (idle or busy), and utilization information

Virtual Analyzer images

Virtual Analyzer does not contain any images by default. You must prepare and import an image before Virtual Analyzer can analyze samples.

To allow Virtual Analyzer to analyze files, import custom OVA files that are between 1 GB and 30 GB in size.

Deep Discovery Inspector supports a maximum of 2 images. The hardware specifications of your Deep Discovery Inspector appliance determine the total number of instances that you can deploy.

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*.

The hardware specifications of your product determine the number of images that you can import and the number of instances that you can deploy per image.

Importing an image

Deep Discovery Inspector stops all analysis and keeps all samples in the Virtual Analyzer queue whenever an image is imported or deleted, or when instances are modified. All instances are also automatically redistributed whenever you import images.

Note

Windows operating systems and other Microsoft products are available separately from Microsoft and Microsoft channel partners.

Important

Trend Micro does not provide any Microsoft Windows operating systems or third-party products required for installation on virtual appliances or sandboxes you create within Deep Discovery Inspector. You must provide the operating system and any other application installation media with appropriate licensing rights necessary for you to create any sandboxes.

Procedure

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

   The **Import Image** screen appears.
3. Select one of the following image sources and configure the applicable settings.

Source	Procedure
Local or network folder	a. Type an image name with a maximum of 260 characters. **Note** **Trend Micro Cloud Sandbox** is a reserved name and cannot be used. b. Click **Connect**. c. Once connected, import the image using the Virtual Analyzer Image Import Tool. For details, see *Import an image using the Virtual Analyzer Image Import Tool on page 6-90*. **Note** Deep Discovery Inspector deploys instances immediately after the image uploads. Wait for deployment to complete.
HTTP or FTP server	a. Type an image name with a maximum of 260 characters. **Note** **Trend Micro Cloud Sandbox** is a reserved name and cannot be used. b. Type the HTTP or FTP URL. c. (Optional) Type logon credentials if authentication is required or select **Log on anonymously**. **Note** Select **Log on anonymously** only if the server supports this function. d. Click **Import**.

Import an image using the Virtual Analyzer Image Import Tool

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

Procedure

1. Verify your computer has established a connection to Deep Discovery Inspector by going to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Status**.
2. Configure the import settings in **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Images**:
   - **Source**: **Local or network folder**
   - **Port**: If necessary, specify a port for the connection
3. Click **Connect**.
4. If the connection is successful, click **Download image import tool**.
5. Open the file `VirtualAnalyzerImageImportTool.exe`.
6. Type the IP address for Deep Discovery Inspector.
7. If you specified a port number in the management console, specify the same port number in the tool.
8. Select the image you want to import
9. Click **Import**

   Deep Discovery Inspector deploys instances immediately after an image uploads. Wait for the instance deployment to complete.

Note

The image import process might stop or fail because of the following reasons:

- No connection established. The product may be busy.
- The connection to the appliance was interrupted.
- The connection timed out.
- Memory allocation was unsuccessful.
- Windows socket initialization was unsuccessful.
- The image file is corrupt.
- The image upload did not complete.
- The image upload was cancelled.

Modify instances

Deep Discovery Inspector stops all analysis and keeps all samples in the Virtual Analyzer queue whenever an image is imported or deleted, or when instances are modified. All instances are also automatically redistributed whenever you import images.

Modifying instances

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Images**.
2. Click **Modify**.

   The **Modify Instances** screen appears.
3. Specify the number of instances for each image.

   Note

   Each image must have a minimum of one instance.

4. Click **Save**.

Deleting instances

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Images**.
2. Click **Modify**.

   The **Modify Instances** screen appears.
3. To delete an instance, click the minus icon to the left of an image's instance count.

   Note

   Each image must have a minimum of one instance.
4. Click **Save**.

Archive passwords

Suspicious files must always be handled with caution. Trend Micro recommends adding such files to a password-protected archive file before transporting across the network.

Virtual Analyzer uses user-specified passwords to extract files from archive files.

To use this feature, add and enable a basic file submission rule with the following criteria:

- **Detection type**: Files with no detections
- **File type**: Selectable file types to be decrypted with the listed passwords

For details, see *Adding a file submission rule on page 6-83*.

If Virtual Analyzer is unable to extract encrypted files using any of the specified passwords, Deep Discovery Inspector displays the status "Unsupported file type" and removes the archive file from the queue.

Note

Passwords can only be used for the first encryption layer. Decryption of SMTP attachments is not supported.

Deep Discovery Inspector stores archive file passwords as unencrypted text.

Adding an archive password

Deep Discovery Inspector supports a maximum of five passwords.

To use this feature, add and enable a basic file submission rule with the following criteria:

- **Detection type**: Files with no detections
- **File type**: Selectable file types to be decrypted with the listed passwords

For better performance, list commonly used passwords first.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Passwords**.
2. Under **Archive File Passwords**, type a password.
3. (Optional) Click **Add password...** and type another password.
4. Click **Save**.

Sandbox for macOS

When the sandbox for macOS setting is enabled, Deep Discovery Inspector sends possible threats for macOS to Sandbox as a Service for analysis.

To enable the sandbox for macOS, go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **Sandbox Management** > **Sandbox for macOS**

and then enable **Send possible threats for macOS to Sandbox as a Service for analysis**.

Verify the service connectivity on the **Network Services Diagnostics** screen. For details, see *Cannot connect to network services on page 7-11*.

Important

Replacing the Deep Discovery Inspector Activation Code automatically disables the sandbox for macOS. After replacing the Deep Discovery Inspector Activation Code, re-enable the sandbox for macOS.

YARA rules

Important

- After you register Deep Discovery Inspector to Deep Discovery Director, Deep Discovery Inspector automatically synchronizes YARA rule settings from Deep Discovery Director and overwrites existing YARA rule settings that you have configured.
- All settings under **YARA Rules** apply only to objects submitted to the **internal Virtual Analyzer**.

YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment. Deep Discovery Inspector uses YARA rules to identify malware.

Deep Discovery Inspector supports a maximum of 5,000 enabled YARA rules regardless of the number of YARA rule files. On the top-right corner of the YARA rule table, the **Rules in use** field indicates the number of YARA rules currently enabled in the system.

When integrated with Deep Discovery Director, Deep Discovery Director centrally manages all YARA rules and you must manage the YARA rules in the Deep Discovery Director management console. For details, see the *Deep Discovery Director Administrator's Guide*.

The following table shows information about YARA rule files.

Field	Description
File Name	Name of the YARA rule file.
Rules	Number of YARA rules contained in the YARA rule file.
Files To Analyze	File types to analyze using the YARA rules in the YARA rule file.
Last Updated	Date and time the YARA rule file was last updated.

Creating a YARA rule file

Deep Discovery Inspector supports YARA rules that follow version 4.1.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

For more information about writing YARA rules, visit the following site:

https://yara.readthedocs.io/en/v4.1.0/writingrules.html

A YARA rule file must fulfill certain requirements before it can be added to Virtual Analyzer for malware detection:

- File name must be unique
- File content cannot be empty

The following example shows a simple YARA rule:

```
rule NumberOne
{
meta:
desc = "Sonala"
weight = 10
strings:
$a = {6A 40 68 00 30 00 00 6A 14 8D 91}
$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
$c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
condition:
$a or $b or $c
}
```

The following table lists the different parts of the YARA rule and how they are used:

TABLE 6-11. YARA Rule Parts and Usage

PART	USAGE
rule	The YARA rule name. Must be unique and cannot contain spaces.
meta:	Indicates that the "meta" section begins. Parts in the meta section do not affect detection.
desc	Optional part that can be used to describe the rule.
weight	Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met: • 1 to 9 = Low risk • 10 = High risk **Note** The weight value does not correspond to the risk level assigned by Deep Discovery Inspector.
strings:	Indicates that the "strings" section begins. Strings are the main means of detecting malware.
$a / $b / $c	Strings used to detect malware. Must begin with a $ character followed by one of more alphanumeric characters and underscores.
condition:	Indicates that the "condition" section begins. Conditions determine how your strings are used to detect malware.
$a or $b or $c	Conditions are Boolean expressions that define the logic of the rule. They tell the condition under which a submitted object satisfies the rule or not. Conditions can range from the typical Boolean operators `and`, `or` and `not`, to relational operators `>=`, `<=`, `<`, `>`, `==` and `!=`. Arithmetic operators (`+`, `-`, `*`, `\`, `%`) and bitwise operators (`&`, `|`, `<<`, `>>`, `~`, `^`) can be used on numerical expressions.

Adding a YARA rule file

When integrated with Deep Discovery Director 5.0 or later, Deep Discovery Director centrally manages all YARA rules and you must manage the YARA rules in the Deep Discovery Director management console. For details, see the *Deep Discovery Director Administrator's Guide*.

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **YARA Rules**.
2. Click **Add** to add a YARA rule file.

   The Add YARA Rule File window appears.
3. In the new window that opens, configure the following:
   a. **Rule file**: Browse and select a YARA rule file to add.
   b. **Files to analyze**: Select file types that Virtual Analyzer processes specific to this YARA rule file.

   Note

   Analyzing all file types may cause unintended detections. Trend Micro recommends analyzing specific file types that are targeted by the YARA rule file.
4. Click **Add** when you have selected the YARA rule file to add and the file types to analyze.

   Virtual Analyzer validates the YARA rule file before adding it.

Editing a YARA rule file

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **YARA Rules**.

2. Click a file name to edit a YARA rule file.

   The **Edit YARA Rule File** window appears.

3. Make changes to the settings.
4. Click **Save**.

Deleting a YARA rule file

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **YARA Rules**.
2. Select one or several YARA rule files to remove.
3. Click **Delete**.

Exporting a YARA rule file

Procedure

1. Go to **Administration** > **Virtual Analyzer** > **Internal Virtual Analyzer** > **YARA Rules**.
2. Select a YARA rule file to export.

   Note

   You can export only one YARA rule at a time.

3. Click **Export File**.

Network groups and assets

Network Groups and Assets include network groups, registered domains, and registered services.

Network configuration defines and establishes the profile of the network that Deep Discovery Inspector monitors for the Network Content Correlation Engine.

Important

- When Deep Discovery Director manages network groups and assets:
  - These settings are disabled in Deep Discovery Inspector. To configure them, go to the Deep Discovery Director management console.
  - The **Sync to Registered Products** option in Deep Discovery Director controls synchronization to Deep Discovery Inspector. By default, this option is disabled
- When Deep Discovery Inspector 6.8 Service Pack 1 or later is connected to Trend Vision One, you can decide whether to configure network groups and assets directly from the Deep Discovery Inspector management console or from the **Network Security** > **Network Resources** screen in Trend Vision One.

Adding network groups

To allow Deep Discovery Inspector to determine whether attacks originate from within or outside the network, use IP addresses to establish groups of monitored networks.

Note

When Deep Discovery Director is managing the network groups and assets, the settings for network groups and assets are disabled in Deep Discovery Inspector. Go to the Deep Discovery Director management console to configure the network groups and assets.

Procedure

1. Go to **Administration** > **Network Groups and Assets** > **Network Groups**.
2. Click **Add**.

   The **Network Groups** window appears.
3. Type a group name.

   Note

   Provide specific groups with descriptive names for easy identification of the network to which the IP address belongs. For example: "Finance network", "IT network", or "Administration".
4. Type an IP address range in the text box (up to 1,000 IP address ranges).

   Note

   The IP address range cannot contain a Class D or Class E address (224.0.0.0 - 255.255.255.255)

   Deep Discovery Inspector provides a default network group containing the following IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks:

   - IPv4: `10.0.0.0 - 10.255.255.255`
   - IPv4: `172.16.0.0 - 172.31.255.255`
   - IPv4: `192.168.0.0 - 192.168.255.255`
   - IPv6: `fe80::-febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff`
   - IPv6: `fc00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`
   - IPv6: `fec0::-feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`

Tip

Create a new network group by editing the **Default** network group.

a. Click **Default** to edit and add a new network group.

b. Use a dash to specify an IP address range.

The **Network Groups** window supports IPv4 and IPv6:

- IPv4 example: `192.168.1.0-192.168.1.255`
- IPv6 example: `2620:1005::123-2620:1005::460`

c. Use a slash to specify the subnet mask/prefix for IP addresses.

- IPv4 subnet mask example: `192.168.1.0/24`
- IPv6 subnet prefix example: `fd00:1:1111:200::1000/116`

Note

Add up to three layers of sub-groups.

5. Select the **Network zone**.

Note

Trusted indicates a secure network and **Untrusted** indicates a degree of doubt about the security of the network.

6. Click **Add**.
7. Click **Save**.

Adding registered domains

Add domains used by companies for internal purposes or those considered trustworthy. Identifying trusted domains ensures detection of unauthorized domains.

Add only trusted domains (up to 10000 domains) to ensure the accuracy of your network profile.

Deep Discovery Inspector supports suffix-matching for registered domains. For example, adding `domain.com` adds `one.domain.com`, `two.domain.com`.

Note

When Deep Discovery Director is managing the network groups and assets, the settings for network groups and assets are disabled in Deep Discovery Inspector. Go to the Deep Discovery Director management console to configure the network groups and assets.

Procedure

1. Go to **Administration** > **Network Groups and Assets** > **Registered Domains**.
2. (Optional) Specify registered domains to add.
   a. Click **Add**.

      The **Add Registered Domains** window appears.

   b. For **Domains**, type one or more domains delimited by spaces.

   c. (Optional) For **Description**, type your own description for the domains.

      The description can be 256 characters or less.
3. (Optional) Analyze detections and select registered domains to add.
   a. Click **Analyze**.

      The detections are analyzed. After analysis, a list of detected services and domains on your network appears.

   b. Select the checkbox for each item you want to add.

   c. (Optional) In the **Description** column, type a description for each item that you selected.

d. Click **Save**.

e. Refresh the page in your browser.

The domains appear in the list.

4. (Optional) To edit a domain, click on the domain in the list.

Adding registered services

Add dedicated servers for specific services that your organization uses internally or considers trustworthy. Identifying trusted services in the network ensures detection of unauthorized applications and services.

Add only trusted services to ensure the accuracy of your network profile.

Note

Add up to 10000 total registered services. More than one server (IP address) may be dedicated to each service.

Each service-IP address combination adds an entry that counts towards the total 10000 registered services. For example, if you specify `DNS` for **Services**, and `10.2.1.1` and `10.2.1.2` for **IP addresses**, then 2 registered services are added.

Note

When Deep Discovery Director is managing the network groups and assets, the settings for network groups and assets are disabled in Deep Discovery Inspector. Go to the Deep Discovery Director management console to configure the network groups and assets.

Procedure

1. Go to **Administration** > **Network Groups and Assets** > **Registered Services**.

2. (Optional) Specify registered services to add.

a. Click **Add**.

The **Add Registered Services** window appears.

b. For **Services**, select one or more services.

TABLE 6-12. Service Types

SERVICE	NETWORK SERVER DESCRIPTION
Active Directory	Provides directory services and stores user accounts and passwords Configure the same server as the Domain Controller.
Authentication Servers - Kerberos	Provides Kerberos authentication
Content Management Server	Manages content
Database Server	Used as a database server
DNS	Used as a DNS server
Domain Controller	Responds to security authentication requests and allows host access to domain resources Configure the same server as the Active Directory.
File Server	Provides a location for shared file access
FTP	Used as an FTP server
HTTP Proxy	Used as an HTTP Proxy server
Radius Server	Used as the Radius authentication server
Security Audit Server	Detects vulnerabilities and insecure configurations
SMTP	Used as an SMTP server

Service	Network Server Description
SMTP Open Relay	Used as an SMTP Open Relay server
Software Update Server	Used for the following: • Responsible for Windows Server Update Services (WSUS) • Performs remote deployment
Web Server	Used as a web server

c. For **IP addresses**, type one or more IP addresses delimited by spaces.

The **Add Registered Services** screen supports IPv4 and IPv6. You can specify single IP addresses, IP address ranges, or IP addresses or ranges in CIDR format. Refer to the following examples:

- Single IP address: `10.0.0.5`
- IP address range: `10.0.0.0-10.255.255.255`
- CIDR format: `10.0.0.0/8`

When you specify multiple services and multiple IP addresses, a registered service for each service-IP address combination is added. For example, if you specify `DNS` and `SMTP` for **Services**, and `10.2.1.1` and `10.2.1.2` for **IP addresses**, then the following 4 registered services are added:

- DNS: 10.2.1.1
- DNS: 10.2.1.2
- SMTP: 10.2.1.1
- SMTP: 10.2.1.2

d. (Optional) For **Description**, type your own description for the services.

The description can be 256 characters or less.

3. (Optional) Analyze detections and select registered services to add.
   a. Click **Analyze**.

      The detections are analyzed. After analysis, a list of detected services and domains on your network appears.

   b. Select the checkbox for each item you want to add.

   c. (Optional) In the **Description** column, type a description for each item that you selected.

   d. Click **Save**.

   e. Refresh the page in your browser.

      The services appear in the list.

4. (Optional) To edit a service, click on the IP address in the list.

Synchronize network groups and assets from Trend Vision One

Trend Vision One allows you to define and synchronize network assets to all your connected Deep Discovery Inspector appliances.

Important

- Syncing network assets from Trend Vision One overwrites the existing lists in your Deep Discovery Inspector appliances.
- The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-network-resources.

Procedure

1. In the Trend Vision One console, go to **Network Security** > **Network Resources**.
2. Click **Central Management Settings**.

3. Select **Use Network Resource settings from Trend Vision One** and then click **Save**.
4. Use the available options to define your network topology.

   Trend Vision One synchronizes the following lists to your registered Deep Discovery Inspector appliances:

   - Trusted Domain List
   - Network Group List
   - Trusted Service Source List
5. Click **Save**

Importing/exporting configuration settings

To replicate network configuration settings from one Deep Discovery Inspector appliance (Appliance 1) to another appliance (Appliance 2), export the settings to a file and then import the file to other Deep Discovery Inspector appliances.

The default file name is `cav.xml`, which you can change to a preferred file name.

Note

- To replicate Deep Discovery Inspector settings in addition to network configuration settings, see *Backup / restore on page 6-203*.
- When Deep Discovery Director is managing the network groups and assets, all settings except export for network groups and assets are disabled in Deep Discovery Inspector. Go to the Deep Discovery Director management console to configure the network groups and assets.

Procedure

1. On Appliance 1, go to **Administration** > **Monitoring / Scanning** > **Network Groups and Assets** > **Import/Export**.

2. Under **Export Configuration**, click **Export**.

   A message prompts you to open or save the `cav.xml` file.

3. Click **Save**, browse to the target location of the file, and click **Save** again.

4. On Appliance 2, go to **Administration** > **Monitoring / Scanning** > **Network Groups and Assets** > **Import/Export**.

5. Under **Export Configuration**, click **Export**.

   A message prompts you to open or save the `cav.xml` file.

6. Click **Save**, browse to the target location of the file, and click **Save** again.

   This backs up the current network configuration settings.

7. Under **Import Configuration**, click **Choose File**.

8. Locate the `cav.xml` file and click **Open**.

9. Click **Import**.

Important

Any descriptions in `cav.xml` that are over 256 characters are truncated during import.

Integrated products/services

Deep Discovery Inspector integrates with other Trend Micro products and services.

Integrated Trend Micro products and services

The following table describes the Trend Micro products and services that integrate with Deep Discovery Inspector 6.8 Service Pack 2.

Note

Deep Discovery Inspector 40G does not support the features associated with Deep Discovery Director.

Product/ Service	Version
Apex Central	2019 HF6658
Deep Discovery Analyzer	• 7.5 • 7.6
Deep Discovery Director - Network Analytics	5.3
Deep Discovery Director - Network Analytics as a Service	Not applicable
Deep Discovery Director - On-premises version	5.3
Service Gateway	Not applicable
Smart Protection Server	3.3 Patch 11
Threat Investigation Center	Not applicable
Trend Micro TXOne OT Defense Console	1.5
Trend Vision One	Not applicable

Trend Vision One

Use one of the available methods to connect Deep Discovery Inspector to Trend Vision One.

Trend Vision One extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With Trend Vision One, you can respond more effectively to threats, minimizing the severity and scope of a breach.

The following table outlines the available methods to connect Deep Discovery Inspector to Trend Vision One.

Method	Description
Direct connection	Connect your Deep Discovery Inspector appliance using the Network Inventory app. For details, see *Direct connection to Trend Vision One on page 6-110*. **Note** Information related to Network Analytics as a Service appears on the Network Inventory app.
Using a service gateway as a proxy	Connect your Deep Discovery Inspector appliance using a Service Gateway as a proxy. For details, see *Connection to Trend Vision One using a Service Gateway as a proxy on page 6-112*.
Deep Discovery Director	Connecting Deep Discovery Director to Trend Vision One automatically connects all managed Deep Discovery Inspector appliances. For details, see *Connecting an On-premises Deep Discovery Director* at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ConnectingOnPremDDD. **Important** You cannot connect to Deep Discovery Director if Deep Discovery Inspector is already connected to Trend Vision One.

Direct connection to Trend Vision One

Connect a deployed Deep Discovery Inspector appliance to Trend Vision One using the Network Inventory app.

Network Inventory supports connecting with Deep Discovery Inspector version 5.7 Service Pack 3 or later. If your appliance is using a previous version (5.7 Service Pack 2 or prior), upgrade to the latest version to connect to Network Inventory.

Important

The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ConnectingDeployedDDIDirectly

Procedure

1. If you want to use **Network Analytics as a Service**, disconnect from **Deep Discovery Director - Network Analytics**.
2. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances**.
3. Click **Connect Appliance**.
4. For **Product**, select **Deployed Deep Discovery Inspector**.
5. Select **6.7 or later**.
6. Select **Direct connection** from the connection method list.
7. Specify the Deep Discovery Inspector appliance IP address or FQDN.

   You can only access appliances that are part of your corporate network or that you can reach directly.
8. Click **Go**.

   The Deep Discovery Inspector appliance console opens.
9. On the Deep Discovery Inspector console, sign in with an administrator account.
10. (Optional) Change the password.
11. In the **Registering to Trend Vision One** dialog, click **Continue** to confirm the process.
12. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances** to verify the connection status.

Note

When Deep Discovery Inspector connects to Trend Vision One, Deep Discovery Inspector creates the “Trend Vision One Administrator” and “Trend Vision One Viewer” accounts automatically.

Connection to Trend Vision One using a Service Gateway as a proxy

Connect a deployed Deep Discovery Inspector appliance to Trend Vision One using a Service Gateway as a proxy.

Important

The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ConnectingDeployedDDI

Procedure

1. If you want to use **Network Analytics as a Service**, disconnect from **Deep Discovery Director - Network Analytics**.
2. Make sure your Service Gateway has the Forward Proxy Service configured.

   For more information, see **Forward Proxy Service** at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ForwardProxyService.
3. Configure your firewall to allow communication with port 8080.

   Service Gateway uses port 8080 as the default port for the Forward Proxy service.
4. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances**.

5. Click **Connect Appliance**.
6. For **Product**, select **Deployed Deep Discovery Inspector**.
7. Select **6.7 or later**.
8. Select **Connect using a Service Gateway as proxy** from the connection method list.
9. Select a Service Gateway from the list.
10. Specify the Deep Discovery Inspector appliance IP address or FQDN.

    You can only access appliances that are part of your corporate network or that you can reach directly.
11. Click **Go**.

    The Deep Discovery Inspector appliance console opens.
12. On the Deep Discovery Inspector console, sign in with an administrator account.
13. (Optional) Change the password.
14. In the **Registering to Trend Vision One** dialog, click **Continue** to confirm the process.
15. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances** to verify the connection status.

Note

When Deep Discovery Inspector connects to Trend Vision One, Deep Discovery Inspector creates the “Trend Vision One Administrator” and “Trend Vision One Viewer” accounts automatically.

Disconnect Deep Discovery Inspector from Trend Vision One using Network Inventory

Tip

If you need to disconnect Deep Discovery Inspector from Deep Discovery Director, see *Unregistering from Deep Discovery Director on page 6-126*.

Disconnecting Deep Discovery Inspector from Trend Vision One unbinds Network Analytics and Service Gateway appliances that integrated with Deep Discovery Inspector.

Procedure

1. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances**.
2. In the Network Inventory list, find your Deep Discovery Inspector appliance and click the Disconnect button ( ) at the right of the row.
3. Click **Disconnect**.

Tip

For details about re-connecting Deep Discovery Inspector to Trend Vision One, see *Direct connection to Trend Vision One on page 6-110*.

Service Gateway connection

Configure Deep Discovery Inspector appliances which connect directly to Trend Vision One to use a Service Gateway as a service source.

A Service Gateway enables connections from Trend Vision One to Deep Discovery Inspector appliances within the corporate network, providing more services.

Procedure

1. In Trend Vision One, configure at least one Service Gateway.

   For details, see *Service Gateway Inventory* at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ServiceGateway

2. Ensure your service gateway has the following services installed:

   - ActiveUpdate
   - Smart Protection Services
   - Suspicious Object List synchronization

   For details, see *Managing Services in Service Gateway* at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ManagingServicesSG

3. Configure the connection to your Service Gateway.

   Important

   The following instructions were valid as of November 2025.
   For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ConnectingNetworkSensorsServiceGateway

   a. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances**.

   b. Select one or more connected appliances.

   c. Click **Configure Connection Settings**.

      The **Appliance Connection Settings** panel appears.

   d. If your appliance is using the **Direct connection** method, select **Use a Service Gateway as the service source** and select the Service Gateway to use as the source.

e. If the version of your Deep Discovery Inspector appliance is 6.7 or later, click **Test Connection**.

You can apply the settings to Deep Discovery Inspector 6.7 or later appliances if the status is **Successful**.

Earlier versions of Deep Discovery Inspector show a status of **Not tested**. You can apply settings even if all other appliances return a status of **Failed**.

f. Click **Apply** to apply the settings to all Deep Discovery Inspector appliances with a status of **Successful** or **Not tested**.

Service Gateway services

Tip

For details about managing services in a Service Gateway, see *Managing Services in Service Gateway* at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ManagingServicesSG

To configure or view the enabled services, see the following sections:

- *Viewing enabled Service Gateway services on page 6-116*
- *Smart Protection services on page 6-117*
- *Component service updates on page 6-118*

Viewing enabled Service Gateway services

Procedure

1. In the Deep Discovery Inspector management console, go to **Administration** > **Integrated Products/Services** > **Trend Vision One**.
2. In the **Service Gateway** section, verify the enabled services.

Smart Protection services

Important

The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ManagingServicesSG.

Procedure

1. In the Trend Vision One console, go to **Workflow and Automation** > **Service Gateway Management**.
2. Click the name of the Service Gateway you want to manage.

   The Service Gateway screen appears.
3. Configure Smart Protection Services.
   a. Click **Manage Services**.
   b. In the **Manage Services** panel, locate **Smart Protection Services**.
   c. Click the install icon ( ).

   Note

   - When enabling the service, Deep Discovery Inspector automatically configures the Service Gateway Smart Protection Server as the primary Smart Protection Server.
   - When disabling the service, Deep Discovery Inspector automatically configures Smart Protection Server to the previous setting.

   Deep Discovery Inspector configures the Smart Protection Server automatically.

Tip

For details about managing services in a Service Gateway, see *Managing Services in Service Gateway* at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ManagingServicesSG

Component service updates

Important

The following instructions were valid as of November 2025. For further help, check the Trend Vision One documentation at https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-help/ManagingServicesSG.

Procedure

1. In the Trend Vision One console, go to **Workflow and Automation** > **Service Gateway Management**.
2. Click the name of the Service Gateway you want to manage.

   The Service Gateway screen appears.
3. Configure the ActiveUpdate service.
   a. Click **Manage Services**.
   b. In the **Manage Services** panel, locate **ActiveUpdate Service**.
   c. Click the install icon ().

Deep Discovery Inspector configures Service Gateway ActiveUpdate Server as the ActiveUpdate source automatically.

Disconnecting a Service Gateway

Procedure

1. In the Trend Vision One console, go to **Network Security Operations** > **Network Inventory** > **Deep Discovery Inspector Appliances**.
2. Select one or more connected appliances.
3. Click **Configure Connection Settings**.
4. If your appliance is using the **Direct connection** method, select **Use the default service source**.
5. Click **Apply**

Important

Deep Discovery Inspector stops sharing suspicious object data via Service Gateway.

Apex Central

Trend Micro Apex Central is a software management solution that simplifies the administration of your corporate antivirus and content security policies. Apex Central provides the following features:

- Centrally manages the following:
  - Suspicious objects, user-defined lists, and exception lists
  - Multiple Deep Discovery Inspector system statuses
  - Antivirus and content security programs, regardless of the program's physical location or platform
- Consolidates multiple Deep Discovery Inspector logs

For information about managing products using Apex Central, see the *Trend Micro Apex Central Administrator's Guide*.

Use the **Apex Central** screen on the Deep Discovery Inspector management console to perform the following:

- Verify that Deep Discovery Inspector can register to an Apex Central server.
- Register to an Apex Central server.
- Check the connection status between Deep Discovery Inspector and Apex Central.
- Check the latest communication heartbeat with Apex Central.
- Unregister from an Apex Central server.
- Synchronize suspicious objects with Apex Central.

Note

Make sure that both Deep Discovery Inspector and the Apex Central server belong to the same network segment. If Deep Discovery Inspector is not in the same network segment as Apex Central, configure the port forwarding settings for Deep Discovery Inspector.

For details, see *Registering to Apex Central on page 6-121*.

Apex Central components

TABLE 6-13. Apex Central Components

COMPONENT	DESCRIPTION
Apex Central server	The appliance with Apex Central installed This server hosts the web-based Apex Central management console.
Entity	A representation of a managed product (such as Deep Discovery Inspector) on the Apex Central console's directory tree The directory tree includes all managed entities.

Registering to Apex Central

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Apex Central**.
2. Under **Connection Settings**, specify the name that identifies Deep Discovery Inspector in the Apex Central Product Directory.

   Note

   Specify a unique and meaningful name to help you quickly identify Deep Discovery Inspector.

3. Under **Apex Central Server Settings**, do the following:
   a. Type the Apex Central server FQDN or IP address.
   b. Type the port number that Deep Discovery Inspector uses to communicate with Apex Central.
   c. (Optional) Select **Connect using HTTPS** if Apex Central security is set to the following levels:
      - **Medium**: Trend Micro allows HTTPS and HTTP communication between Apex Central and Deep Discovery Inspector.
      - **High**: Trend Micro allows only HTTPS communication between Apex Central and the Deep Discovery Inspector.
   d. (Optional) If your network requires authentication, specify the **User name** and **Password** for your Internet Information Services (IIS) server.
4. (Optional) If you use a NAT device, select **Enable two-way communication port forwarding**, and type the NAT device **IP address** and **Port** number.

Note

- Deep Discovery Inspector uses the port forwarding IP address and port forwarding port number for two-way communication with Apex Central.
- Configuring the NAT device is optional and depends on the network environment.

5. If you have configured proxy settings for Deep Discovery Inspector and want to use these settings for Apex Central connections, select **Connect through a proxy server**.
6. (Optional) Under **Suspicious Object Synchronization**, do the following:
   a. Select **Synchronize suspicious objects with Apex Central**.

      Important

      You can only choose to synchronize suspicious objects with one source. If you enable Deep Discovery Inspector to sync with Apex Central, you will not receive suspicious objects from any other external sources.

      Before selecting this option, verify that your external sandbox is configured to send suspicious objects to Apex Central.

   b. Type an API Key.

      Note

      Log on to Apex Central to obtain an API key.

   Deep Discovery Inspector synchronizes suspicious object lists with Apex Central every 20 seconds, and displays the time of the last synchronization.
7. Click **Test Connection** to verify that Deep Discovery Inspector can connect to the Apex Central server.

8. Click **Register** if a connection was successfully established.

Unregistering from Apex Central

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Apex Central**.
2. Under **Connection Status**, click **Unregister**.

Note

Use this option to unregister Deep Discovery Inspector from Apex Central or to register to another Apex Central.

Managing the connection with Apex Central

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Apex Central**.
2. Under **Connection Status**, perform the following actions:
   a. Verify that the product can connect to Apex Central.
   b. If the product is not connected, restore the connection immediately.
   c. Check the heartbeat to verify the last communication between Deep Discovery Inspector and the Apex Central server.
3. To update the Apex Central server with changes after registration, click **Update Settings**.
4. To transfer control of Deep Discovery Inspector management to another Apex Central server, click **Unregister** and then register Deep Discovery Inspector to the new Apex Central server.

   For details, see *Registering to Apex Central on page 6-121*.

Deep Discovery Director

Trend Micro Deep Discovery Director is a management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication and log aggregation for Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

In addition, Deep Discovery Inspector feeds and obtains threat intelligence with Deep Discovery Director to provide enhanced threat intelligence sharing and detection.

For details about Deep Discovery Director integration, see the *Deep Discovery Director Administrator's Guide* and the following topics:

- *Connecting to Deep Discovery Director on page 6-124*
- *Unregistering from Deep Discovery Director on page 6-126*
- *Settings replicated by Deep Discovery Director and Trend Vision One on page B-1*

Connecting to Deep Discovery Director

Important

You cannot connect to Deep Discovery Director if Deep Discovery Inspector is already connected to Trend Vision One.

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.

Deep Discovery Director cloud version is integrated with Trend Vision One. View the connection status at **Administration** > **Integrated Products/ Services** > **Trend Vision One**.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director** > **Management Server**.
2. Under **Connection Settings**, type the **Server address** for Deep Discovery Director.
3. Under **Connection Settings**, type **Port** number for Deep Discovery Director.
4. Under **Connection Settings**, 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.

5. (Optional) If you have configured proxy settings for Deep Discovery Inspector and want to use these settings for Deep Discovery Director connections, select **Use the system proxy settings**.

   Tip

   This setting can be changed after registering to Deep Discovery Director.

   To update this setting without unregistering from Deep Discovery Director, click **Update Settings**.

6. Click **Register**.

   The **Status** changes to **Registered | Connected**.

Note

If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust**.

After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.

Note

To register to Deep Discovery Director - Network Analytics as a Service (DDD - NAaaS), see the Deep Discovery Director documentation.

Deep Discovery Inspector cannot register to both DDD - NAaaS and Deep Discovery Director - Network Analytics (DDD - NA) at the same time. If Deep Discovery Inspector is registered to DDD - NA and you want to register DDD - NAaaS, then you must first unregister DDD - NA.

When Deep Discovery Inspector is registered to DDD - NAaaS, the information of DDD - NAaaS appears on the **Management Server** tab.

Unregistering from Deep Discovery Director

Follow this procedure to unregister from Deep Discovery Director or before registering to another Deep Discovery Director.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.
2. Click **Unregister**.

Note

When you unregister Deep Discovery Director, Deep Discovery Director - Network Analytics and Deep Discovery Director - Network Analytics as a Service also become unregistered.

Threat investigation center

Trend Micro Threat Investigation Center is a scalable service that collects, aggregates, formalizes, and correlates big data. Threat Investigation Center transforms big data into actionable intelligence and provides visualizations and reports. In addition to supporting Windows Event logs, Threat Investigation Center integrates with several Trend Micro products and services, including Advanced Threat Assessment Service, Deep Discovery Email Inspector, Deep Discovery Inspector, Deep Security, Apex Central and Endpoint Sensor.

Integrating threat investigation center

The following steps integrate Threat Investigation Center via a built-in agent.

Additional steps may need to be performed on Threat Investigation Center. For details, see the Threat Investigation Center documentation.

Procedure

1. Open the Deep Discovery Inspector management console, and go to the **Administration** > **Integrated Products/Services** > **Threat Investigation Center**.

   The **Threat Investigation Center** screen appears.

2. Click **Add**.

   The **Add Threat Investigation Center Server** window appears.

3. Select **Enabled**.

4. In **Server address**, type the HTTPS log server address for Threat Investigation Center.

5. (Optional) Enable **File retrieval**.

Note

When file retrieval is enabled, Threat Investigation Center collects the investigation package and packet capture files from Deep Discovery Inspector. This feature is available when Deep Discovery Inspector is registered to Threat Investigation Center.

6. (Optional) Enable **Use CA certificate** and then click **Select** to select the Threat Investigation Center CA certificate.

Note

Using a CA certificate is optional. A certificate is necessary when there is a man-in-the-middle appliance between the Threat Investigation Center server and Deep Discovery Inspector.

7. (Optional) Enable **Use the system proxy settings**.

Note

Configure the system proxy settings at **Administration** > **System Settings** > **Proxy**.

8. (Optional) Click **Test Connection** to verify the connection to the Threat Investigation Center server.
9. Click **Save**.

TXOne OT Defense Console

Trend Micro TXOne OT Defense Console provides centralized continuous monitoring of operational technology (OT) cyber threats with secure,distributed industrial network support for uninterrupted production line operation.

Configuring TXOne OT Defense Console

Procedure

1. On the Deep Discovery Inspector management console, go to **Administration** > **Integrated Products/Services** > **TXOne OT Defense Console**.
2. Enable **Distribute objects to TXOne OT Defense Console**.
3. Provide the following information:
   - Server address

     Note

     The server address must be the IPv4 address or FQDN of TXOne OT Defense Console.

   - API key: Existing authentication credential
   - API secret: Existing authentication credential
4. (Optional) Click **Test Connection**.
5. (Optional) Under **Object Distribution**, select a new **Frequency**.
6. To send object information from Deep Discovery Inspector to TXOne OT Defense Console, configure the following criteria:
   - Object:
     - Suspicious Object
       - IPv4 address
       - SHA1
   - Risk level:
     - High only
     - High and medium

- High, medium, and low

7. Click **Save**.

Threat intelligence sharing

Deep Discovery Inspector can share threat intelligence data (such as suspicious URLs) with other products or services (for example, a Blue Coat ProxySG device) through HTTP or HTTPS web service.

Threat intelligence sharing configuration

Procedure

1. On the Deep Discovery 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 Inspector**.
3. Under **Criteria**, select which objects to include in the threat intelligence data file.

Note

The maximum length of shared URL objects is 997 characters.

The objects appear in the generated file under the following categories.

TABLE 6-14. Object Categories in Generated File

OBJECT	CATEGORY IN GENERATED FILE
Suspicious URL identified by Virtual Analyzer	DDI_va_suspicious_objects
URL in Deny List	DDI_custom_defense_denylists

Object	Category in Generated File
URL in Apex Central or Deep Discovery Director User-Defined Suspicious Objects list	DDI_control_manager_denylists
Malicious URL detected by Web Reputation Service	DDI_wrs_malicious_urls
C&C Callback URL	DDI_aggressive_rule_urls
Source URL for any of the following files: • Suspicious file identified by Virtual Analyzer • File in Deny List • File in Apex Central or Deep Discovery Director User-Defined Suspicious Objects list	DDI_aggressive_rule_urls
Source URL for malicious file	DDI_aggressive_rule_urls

4. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.
5. (Optional) By default, Deep Discovery Inspector shares threat intelligence data through HTTPS web service. You can also enable HTTP web service for data sharing. Under **Server Settings**, select **Share information using HTTP (in addition to HTTPS)** and specify the HTTP port number.
6. Click **Save**.
7. Click **Generate Now**.

Note

After the file generation is successful, you can click the URL to download the threat intelligence data file to view the content.

8. Configure an integrated product/service (for example, Blue Coat ProxySG device) to obtain threat intelligence data from Deep Discovery

Inspector. For more information, see the documentation for the integrated product/service.

Inline products and services

To help provide effective detection and blocking at the perimeter, Deep Discovery Inspector can distribute Virtual Analyzer suspicious objects to inline products and services.

Deep Discovery Inspector integrates with the following inline solutions:

TABLE 6-15. Supported Inline Solutions

NAME	VERSIONS
Trend Micro TippingPoint Security Management System (SMS)	• 5.5 • If you want to share file hashes as suspicious objects: 6.4.0 or later
Check Point Open Platform for Security (OPSEC)	Check Point R81
IBM Security Network Protection (XGS)	XGS 5.5
Palo Alto Panorama or Firewalls	• PAN-OS 10.2 • Panorama 10.2

Note

Deep Discovery Inspector supports only one inline product/service at a time.

Trend Micro TippingPoint Security Management System (SMS)

Both Deep Discovery Inspector and Trend Micro Apex Central can send suspicious objects and C&C callback addresses to Trend Micro TippingPoint Security Management System (SMS). Deep Discovery Inspector sends each suspicious object with the following optional information:

- Trend Micro Severity: Severity of each suspicious object or C&C callback attempt

- Trend Micro Publisher: Trend Micro Deep Discovery Inspector
- Trend Micro Source: Deep Discovery Inspector host name
- Trend Micro Detection Category: Suspicious object or C&C callback attempt

Trend Micro TippingPoint SMS uses reputation filters to apply block, permit, or notify actions across an entire reputation group. For more information about reputation filters, refer to your Trend Micro TippingPoint documentation.

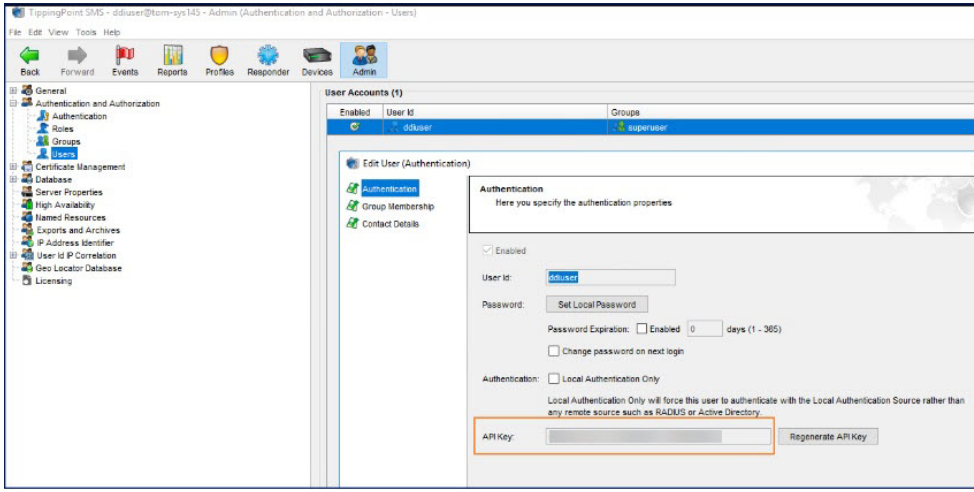
Configure Trend Micro TippingPoint Security Management System (SMS)

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Inline Products/Services**.
2. Select **Trend Micro TippingPoint Security Management System (SMS)**.
3. Under **Server Information**, select a connection method.
   - **API key (recommended)**

Tip

You can find your API key on the TippingPoint SMS console.



- **Username / password**

4. Specify all the required information.

Important

- The server address must be the IPv4 address or FQDN of the inline product.
- User names and passwords can have up to 15 characters.

5. Click **Test Connection**.
6. Under **Object Distribution**, click **Enabled**.
7. If needed, specify a new object distribution frequency.
8. Under **Criteria**, specify the type and risk level of the objects that Deep Discovery Inspector sends to Trend Micro TippingPoint Security Management System.

Object Type	Detection type	Supported TippingPoint SMS version	Risk Level
IPv4 address	• C&C Callback Address • Suspicious Object	5.5 or later	• High only • High and medium • High, medium, and low
Domain			
URL			
SHA1	Suspicious Object	6.4.0 or later	

9. Click **Save**.

   The following tag categories appear in the TippingPoint SMS Reputation Database.

Tag Category	Value
Trend Micro Source	The host name of Deep Discovery Inspector
Trend Micro Severity	Possible values: • High • Medium • Low
Trend Micro Publisher	The product name of Deep Discovery Inspector
Trend Micro Detection Category	The detection type of the threat.

10. If you need to see the distributed suspicious objects and C&C callback addresses in TippingPoint SMS.

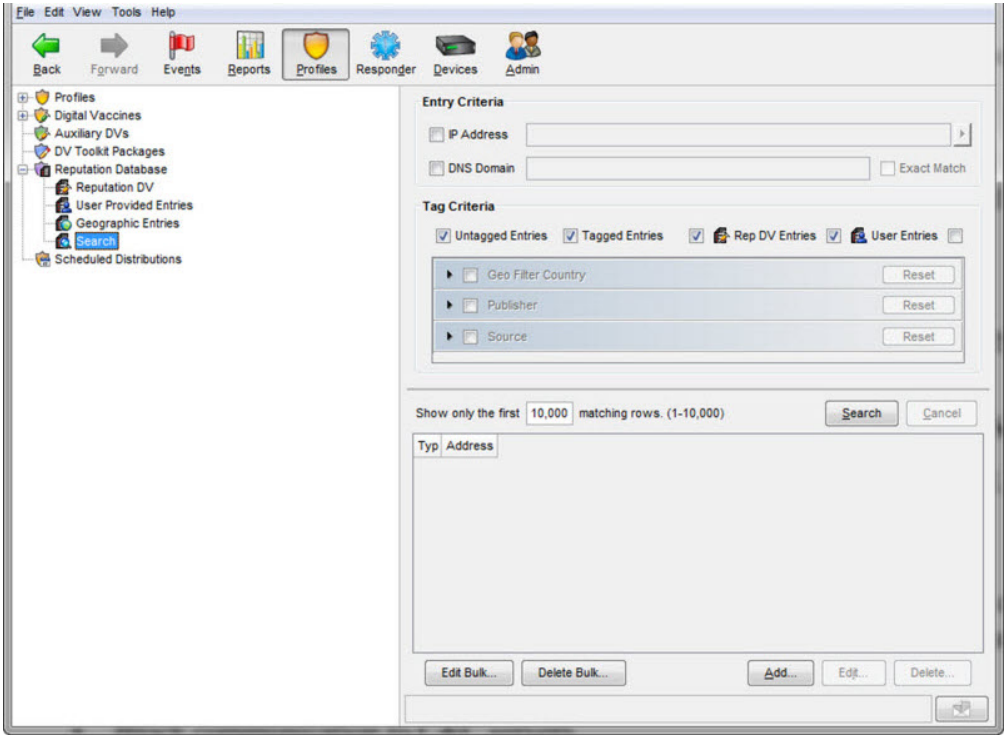
    a. Verify that the following tag categories exist in the **Tag Categories** list of the TippingPoint SMS Client.

       • Trend Micro Severity

       • Trend Micro Source

- Trend Micro Publisher
- Trend Micro Detection Category

b. On **Profile**, go to **Reputation Database** > **Search**.



c. On **Entry Criteria**, type search parameters and click **Search**.

The TippingPoint SMS console displays suspicious objects and C&C callback addresses distributed by Deep Discovery Inspector

Check Point Open Platform for Security (OPSEC)

Check Point Open Platform for Security (OPSEC) manages network security through an open, extensible management framework.

Deep Discovery Inspector integrates with Check Point OPSEC via the Suspicious Activities Monitoring (SAM) API.

The SAM API implements communications between the SAM client (Deep Discovery Inspector) and the Check Point firewall, which acts as a SAM Server. Deep Discovery Inspector uses the SAM API to request that the Check Point firewall take specified actions for certain connections.

For example, Deep Discovery Inspector may ask Check Point OPSEC to block a connection with a client that is attempting to issue illegal commands or repeatedly failing to log on.

Configuring Check Point Open Platform for Security (OPSEC)

Procedure

1. Configure your Check Point appliance.
   a. Check or configure the SAM communication mode ports on your Check Point appliance.

      For details, see *Preconfiguring a security gateway on page 6-145*.

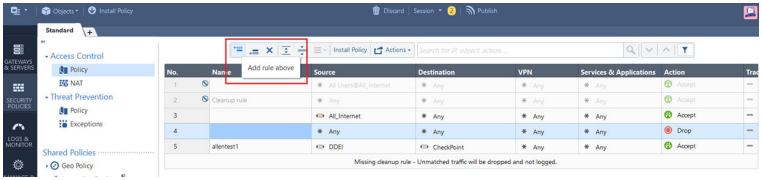
   b. Configure the OPSEC Application on your Check Point appliance.

      For details, see *Configuring a secured connection on page 6-147*.

   c. Enable purging of SAM file on your Check Point appliance.
      1. Open the Check Point SmartDashboard.
      2. Expand **Other** and go to **SAM**.
      3. Enable **Purge SAM file when it reaches:**.
      4. Specify the file size.
      5. Click **OK**.
      6. Save the

   d. Configure Security Policies on your Check Point appliance.
      1. Open the Check Point SmartConsole.

2. On the **SECURITY POLICIES** tab, go to **Access Control** > **Policy**.

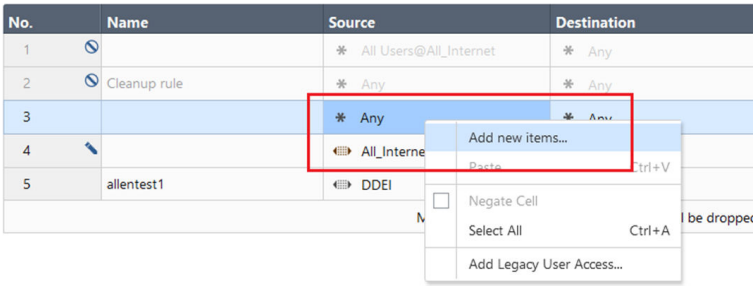


3. To add a rule, click the **Add rule above** icon.

4. To configure the new policy, right-click the action.

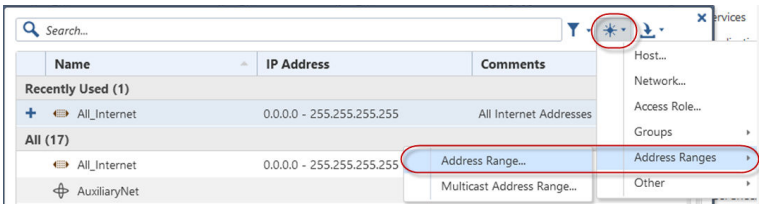
5. Change the action to **Accept**.

6. Right-click the source.



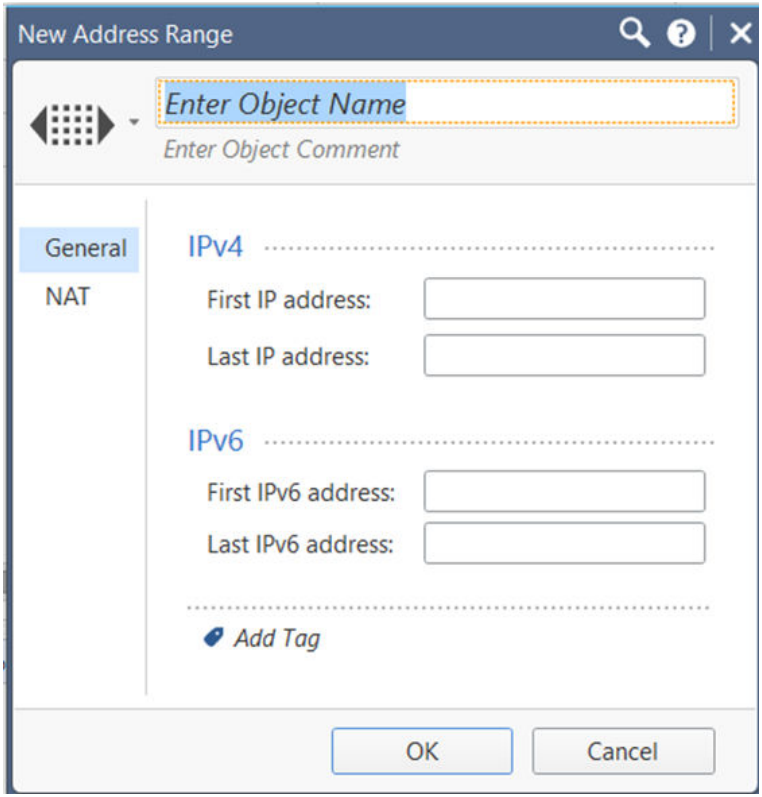
7. Select **Add new items...**.

8. Click the new icon ( ).



9. Select **Address Ranges** > **Address Range...**.

   The **New Address Range** window appears.

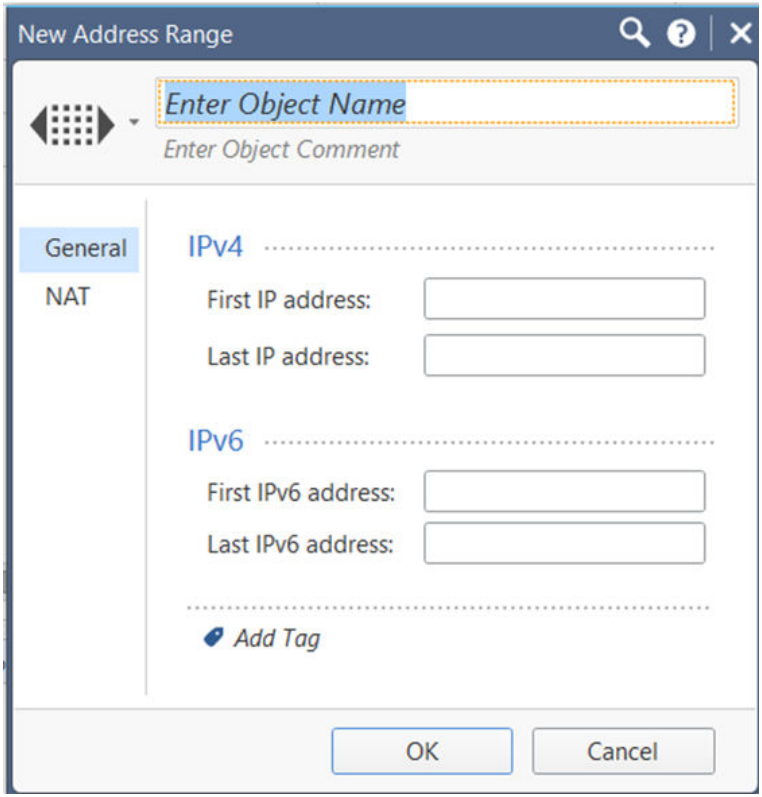


10. n the **Enter Object Name** field, type `DDI`.
11. In **First IP address**, type the Deep Discovery Inspector IP address.
12. In **Last IP address**, type the Deep Discovery Inspector IP address.
13. Click **OK**.
14. Right-click the destination.
15. Select **Add new items...**.

16. Click the new icon ( ).

17. Select **Address Ranges** > **Address Range...**.

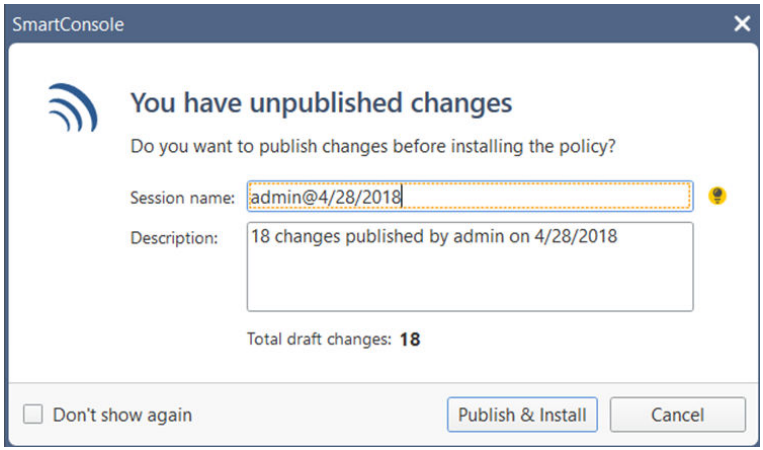
    The **New Address Range** window appears.



18. In the **Enter Object Name** field, type `CheckPoint`.
19. In **First IP address**, type the CheckPoint IP address.
20. In **Last IP address**, type the CheckPoint IP address.
21. Click **OK**.

22. Click **Install Policy**.

    The following window opens.



23. Click **Publish & Install**.

24. Click **Install**.

    The Check Point appliance is enabled to receive suspicious objects and C&C callback addresses from Deep Discovery Inspector.

2. Configure Deep Discovery Inspector.

a. On the Deep Discovery Inspector management console, go to **Administration** > **Integrated Products/Services** > **Inline Products/Services**.

b. Select **Check Point Open Platform for Security (OPSEC)**.

c. Select a connection type.

Note

Ensure that your network configuration allows Deep Discovery Inspector to connect to the Check Point appliance.

Deep Discovery Inspector may connect to the Check Point appliance through the secured connection port or clear connection port that is configured on the Check Point appliance. Deep Discovery Inspector also pulls the certificate from the Check Point appliance through port 18210.

If you selected **Secured connection**, the **OPSEC application name** and **SIC one-time password** settings appear.

d. Type the server address.

Note

The server address must be the IPv4 address or FQDN of the inline product.

e. Type the port.

Note

This port must be the same port that is configured on the security gateway. For details, see *Preconfiguring a security gateway on page 6-145*.

f. If you selected **Secured connection**, type the **OPSEC application name** and **SIC one-time password**.

For more details, see *Configuring a secured connection on page 6-147*.

Note

If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

g. (Optional) Click **Test Connection**.

h. Under **Object Distribution**, click **Enabled**.

The **Legal Statement** opens.

i. Read and accept the **Legal Statement**.

Note

To enable integration with this inline product/service, you must accept the **Legal Statement**.

j. (Optional) Select a new **Frequency**.

k. Configure the following criteria to send suspicious object and C&C callback address information from Deep Discovery Inspector to your Check Point appliance:

- **Object type**:
  - C&C Callback Address
    - IPv4 address
  - Suspicious Object
    - IPv4 address
- **Risk level**:
  - High only
  - High and medium
  - High, medium, and low

l. Under **Advanced Settings**, select one of the following actions:

- **Reject**: Packets will be rejected and a notification sent to the communicating peer that the packet has been rejected.
- **Drop**: Packets will be dropped without sending the communicating peer a notification.

- **Notify**: A notification about the defined activity will be sent but the activity will not be blocked.

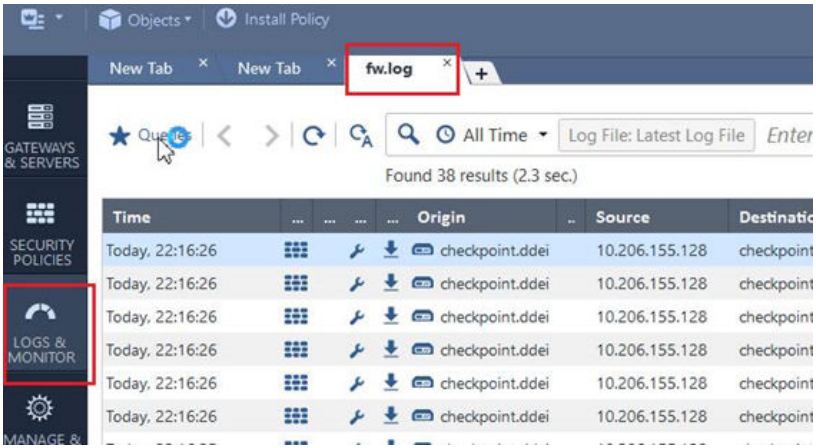
m. Click **Save**.

n. (Optional) Click **Distribute Now** to distribute suspicious objects and C&C callback addresses to Check Point immediately.

3. To view suspicious objects and C&C callback addresses distributed by Deep Discovery Inspector on Check Point SmartView Monitor, do the following:

a. On Check Point SmartConsole, go to **Logs & Monitor**.

b. Add a new tab.



c. Click **Tunnels & User Monitoring** to open SmartView Monitor.

d. Click the **Launch Menu** icon and go to **Tools** > **Suspicious Activity Rules**.

The **Enforced Suspicious Activity Rules** window opens.

e. At **Show On**, select the target Check Point appliance name.

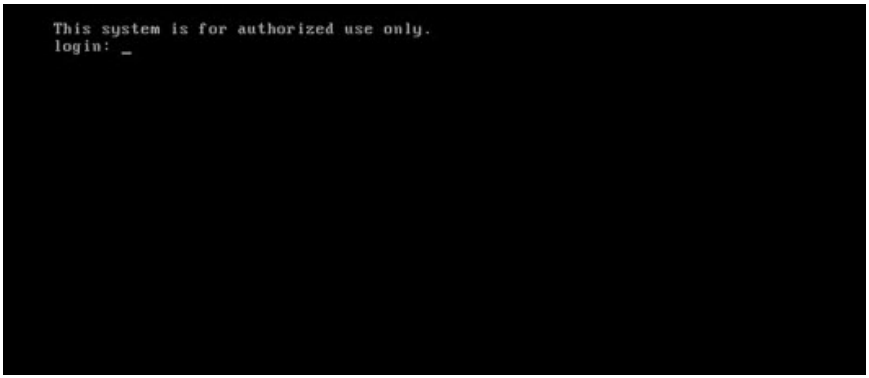
f. Click **Refresh**.

Suspicious objects and C&C callback addresses distributed by Deep Discovery Inspector are displayed.

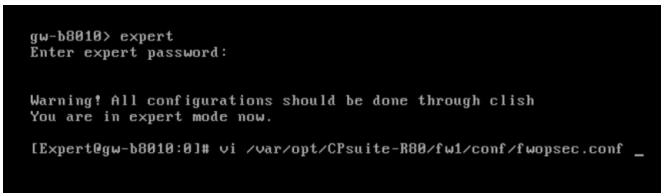
Preconfiguring a security gateway

Procedure

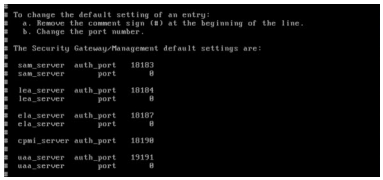
1. Log on to your Check Point appliance.



2. (Optional) Set a password for expert mode.
3. Type the password to enter expert mode.



4. Use the vi editor to open `/var/opt/CPsuite-R80/fw1/conf/fwopsec.conf`.



Note

The image of the default configuration is for reference only. The actual file contents may vary.

5. In `fwopsec.conf`, configure the SAM communication mode ports using one of the following options:

   - Secured connection (default port)
     - No changes in `fwopsec.conf` are necessary. The default port 18183 is used for the **sam_server auth_port** setting.

       Note

       On Deep Discovery Inspector, verify that the **Check Point Open Platform for Security (OPSEC) Port** setting at **Administration** > **Integrated Products/Services** > **Inline Products/Services** is also 18183.

   - Secured connection (user-defined port)
     - In `fwopsec.conf`, remove the comment sign (#) from `sam_server auth_port: 18183` and then change the port number.

       Note

       Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Inspector at **Administration** > **Integrated Products/Services** > **Inline Products/Services**.

- Clear connection (user-defined port)
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server port: 0` and then change the port number.

> **Note**
>
> Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Inspector at **Administration** > **Integrated Products/Services** > **Inline Products/Services**.

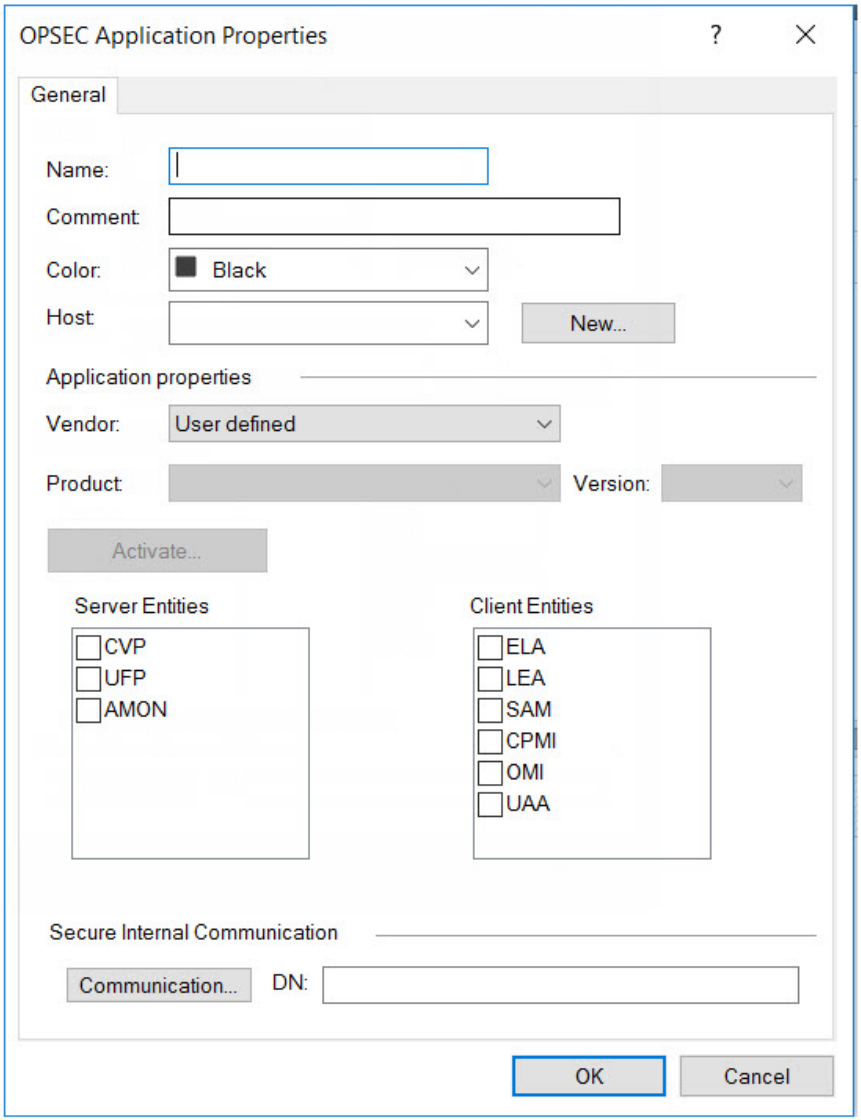
6. If changes were made to the `fwopsec.conf` file, save the `fwopsec.conf` file and restart your Check Point appliance.

Configuring a secured connection

Procedure

1. Open the Check Point SmartConsole and click the main menu icon ( ).
2. Go to **New object** > **More object types** > **Server** > **OPSEC Application** > **New Application...**.

The **OPSEC Application Properties** window appears.



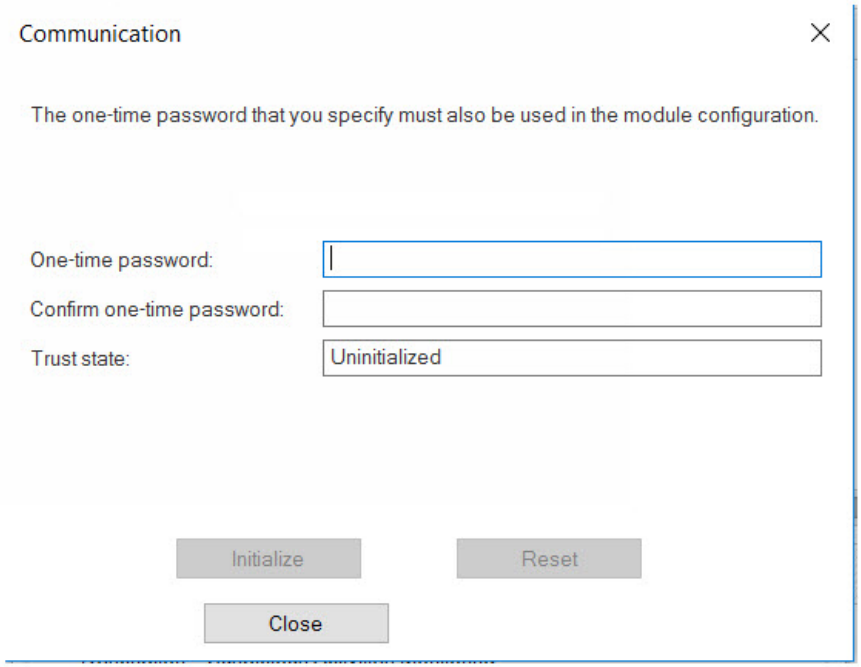
3. Type a **Name**.

Note

- Use this name as the **OPSEC application name** in Deep Discovery Inspector.
- The application name must be less than 101 characters, start with an English alphabetical letter, and contain only English alphabetical letters, periods, underscores, or dashes.

4. Select a **Host**.
5. Under **Client Entities**, select **SAM**.
6. Click **Communication...**.

The **Communication** window appears.



7. Type a password in **One-time password** and type the same password in **Confirm one-time password**.

Note

Use this password as the **SIC one-time password** in Deep Discovery Inspector.

Note

If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

8. Click **Initialize**.

   The **Trust state** becomes **Initialized but trust not established**.

9. Install the user definition.

   a. In the **Check Point SmartConsole** main window, click and select **Install database...**.

      The **Install database** window appears.

   b. Choose the installation components and then click **OK**.

      The user definition starts installing.

IBM Security Network Protection

IBM Security Network Protection (XGS), provides a web services API that enables third-party applications such as Deep Discovery Inspector to directly submit suspicious objects. IBM XGS can perform the following functions:

- Quarantine hosts infected with malware
- Block communication to C&C servers
- Block access to URLs found to be distributing malware

To integrate Deep Discovery Inspector with IBM XGS, configure a generic agent to do the following:

- Accept alerts that adhere to a specific schema
- Create quarantine rules based on a generic ATP translation policy

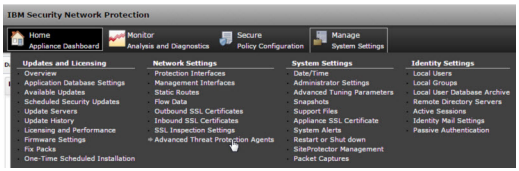
The ATP translation policy allows several categories of messages to take different actions on IBM XGS, including blocking and alerting.

Configuring IBM security network protection

Procedure

1. On the IBM XGS console, do the following to configure the generic agent:

a. Go to **Manage System Settings** > **Network Settings** > **Advanced Threat Protection Agents**.



The **Advanced Threat Protection Agents** window opens.

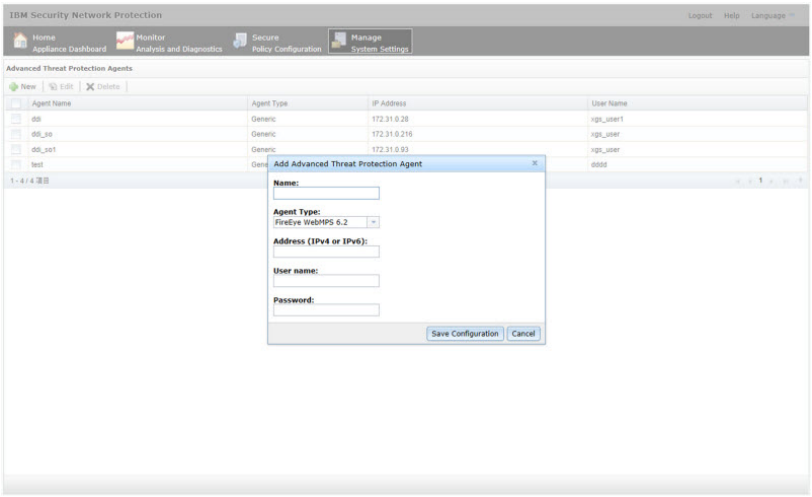
b. Click **New**.

c. Provide the following information:

- Name: Type a name
- Agent Type: Select **Generic**
- Address: Deep Discovery Inspector management port IP address in IPv4 or IPv6 format
- User name: Existing authentication credential
- Password: Existing authentication credential

TABLE 6-16. Valid Character Sets

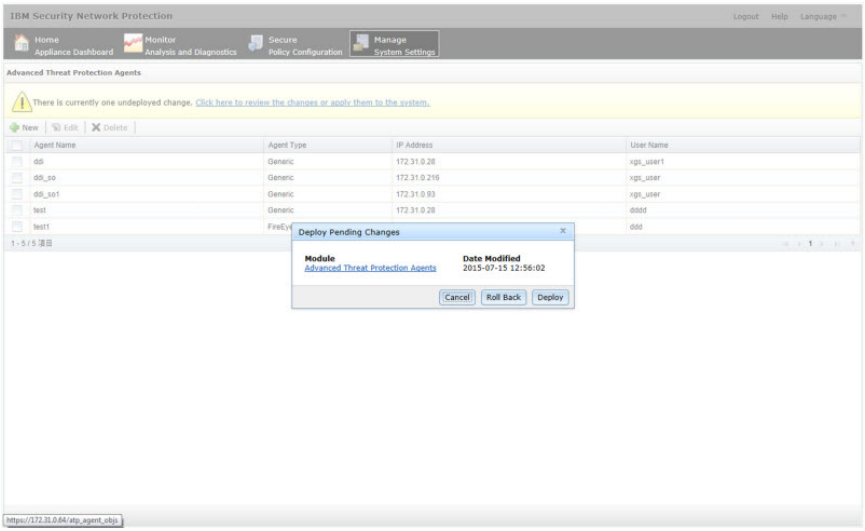
	USER NAME	PASSWORD
Minimum length	1 character	1 character
Maximum length	15 characters	15 characters



2. Click **Save Confirmation**.

   The **Deploy Pending Changes** window opens.

3. To apply changes to IBM XGS, click **Deploy**.



The new agent appears in the **Advanced Threat Protection Agents** list.

4. On the Deep Discovery Inspector management console, go to **Administration** > **Integrated Products/Services** > **Inline Products/Services** and select **Configuring IBM Security Network Protection (XGS)**.

5. Provide the following information:

   - Server address

   Note

   The server address must be the IPv4 address or FQDN of the inline product.

   - User name: Existing authentication credential
   - Password: Existing authentication credential

   TABLE 6-17. Valid Character Sets

	USER NAME	PASSWORD
Minimum length	1 character	1 character
Maximum length	15 characters	15 characters

6. (Optional) Click **Test Connection**.

7. Under **Object Distribution**, click **Enabled**.

   The **Legal Statement** opens.

8. Read and accept the **Legal Statement**.

   Note

   To enable integration with this inline product/service, you must accept the **Legal Statement**.

9. (Optional) Select a new **Frequency**.

10. To send object information from Deep Discovery Inspector to this inline product/service, configure the following criteria:
    - Object type:
        - C&C Callback Address
            - IPv4 address
            - URL
        - Suspicious Object
            - IPv4 address
            - URL
    - Risk level:
        - High only
        - High and medium
        - High, medium, and low
11. Click **Save**.
12. (Optional) On the IBM XGS console, go to **Secure Policy Configuration** > **Security Policies** > **Active Quarantine Rules** to view suspicious objects and C&C callback addresses sent by Deep Discovery Inspector to IBM XGS.

Note

Suspicious objects with a low risk level do not appear in the IBM XGS **Active Quarantine Rules**. To view all suspicious objects sent by Deep Discovery Inspector, go to **Security Policy Configuration** > **Advanced Threat Policy** and specify the following settings:

- **Agent Type**: **Generic**
- **Alert Type**: **Reputation**
- **Alert Severity**: **Low**

Suspicious objects and C&C callback addresses distributed by Deep Discovery Inspector are displayed.

Palo alto panorama or firewalls

Palo Alto Networks® firewalls identify and control applications, regardless of port, protocol, encryption (SSL or SSH) or evasive characteristics.

Deep Discovery Inspector can send IPv4, domain, and URL suspicious objects to the URL category of Palo Alto Firewall or Palo Alto Panorama™ as match criteria allow for exception-based behavior.

Use URL categories in policies as follows:

- Identify and allow exceptions to general security policies for users who belong to multiple groups within Active Directory

  Example: Deny access to malware and hacking sites for all users, while allowing access to users that belong to the security group.

- Allow access to streaming media category, but apply quality of service policies to control bandwidth consumption
- Prevent file download and upload for URL categories that represent higher risks

  Example: Allow access to unknown sites, but prevent upload and download of executable files from unknown sites to limit malware propagation.

- Apply SSL decryption policies that allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.

Configuring Palo Alto Panorama or firewalls

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Inline Products/Services** and select **Palo Alto Panorama or Firewalls**.
2. Provide the following information:
   - Server address

     Note

     The server address must be the IPv4 address or FQDN of the inline product.

   - Server type
     - Panorama
     - Firewalls

     Note

     Deep Discovery Inspector supports Palo Alto Panorama and firewalls with virtual systems.

     On Panorama devices and firewalls with virtual systems, a policy rule must be configured to utilize the suspicious objects and C&C callback addresses.

   - User name: Existing authentication credential
   - Password: Existing authentication credential

TABLE 6-18. Valid Character Sets

	USER NAME	PASSWORD
Minimum length	1 character	1 character
Maximum length	15 characters	15 characters

3. (Optional) Click **Test Connection**.
4. Under **Object Distribution**, click **Enabled**.

   The **Legal Statement** opens.
5. Read and accept the **Legal Statement**.

> **Note**
>
> To enable integration with this inline product/service, you must accept the **Legal Statement**.

6. (Optional) Select a new **Frequency**.
7. To send object information from Deep Discovery Inspector to this inline product/service, configure the following criteria:
   - Object type:
     - C&C Callback Address
       - IPv4 address
       - Domain
       - URL
     - Suspicious Object
       - IPv4 address
       - Domain
       - URL
   - Risk level:

- High only
- High and medium
- High, medium, and low

8. Under **Advanced Settings**, customize URL category names:

   URL category names must include a minimum of one character and a maximum of 31 characters, and may include the following characters:

   - Uppercase (A-Z)
   - Lowercase (a-z)
   - Numeric (0-9)
   - Special characters: - _
   - Space

9. Click **Save**.

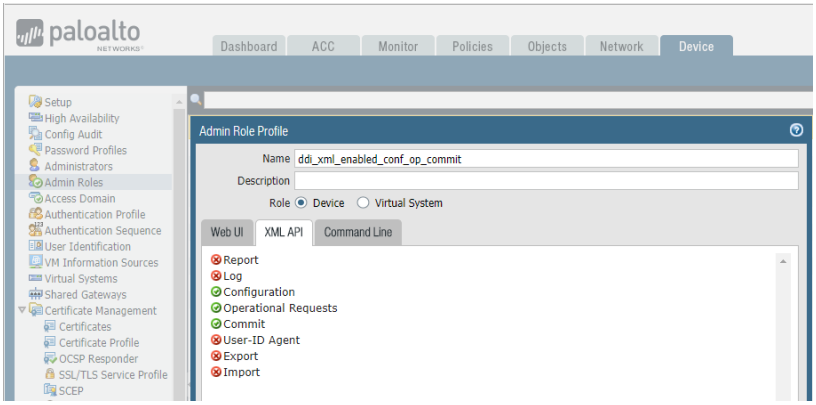
10. For PAN-OS 7.1 or later, enable XML API access.

    a. On the Palo Alto product console, go to **Device** > **Admin Roles** and select or create an admin role.

    b. Select the **XML API** tab.

    c. Enable the following XML API features from the list.

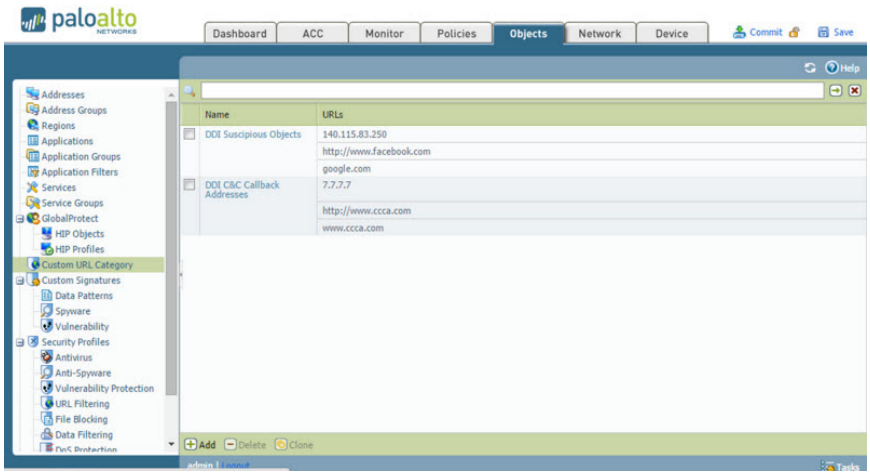
       - Configuration
       - Operation Requests
       - Commit



d. Click **OK**.

e. Assign the admin role to an administrator account.

11. (Optional) To view suspicious objects and C&C callback addresses sent by Deep Discovery Inspector on the Palo Alto product console, go to **Objects** > **Custom URL Category**.



Suspicious objects and C&C callback addresses distributed by Deep Discovery Inspector are displayed.

SAML Authentication

Security Assertion Markup Language (SAML) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports single sign-on (SSO), a technology that allows for a single user login to work across multiple applications and services. When you configure SAML settings in Deep Discovery Inspector, users signing in to your organization's portal can seamlessly sign in to Deep Discovery Inspector without an existing Deep Discovery Inspector account.

In SAML single sign-on, a trust relationship is established between the identity provider (IdP) and the service provider (SP) by using SAML metadata files. The identity provider contains the user identity information stored on a directory server. The service provider (which in this case is Deep Discovery Inspector) uses the user identity information from the identity provider for user authentication and authorization.

Deep Discovery Inspector supports the following identity providers for single sign-on:

- Microsoft Active Directory Federation Services (AD FS) 4.0 or 5.0
- Microsoft Entra ID
- Okta

To connect Deep Discovery Inspector to your organization environment for single-sign-on, complete the following:

1. Access the Deep Discovery Inspector management console to obtain the service provider metadata file.

   You can also update the certificate in Deep Discovery Inspector.

2. In your identity provider:

   a. Configure the required settings for single sign-on.

   b. Obtain the metadata file.

For more information, see the documentation that comes with your identity provider.

3. In Deep Discovery Inspector:
   a. Import the metadata file for your identity provider.
   b. Create SAML user groups.

Service Provider Metadata and Certificate

Obtain the service provider metadata from Deep Discovery Inspector to provide to your identity provider.

On the **SAML Authentication** screen, the Service Provider section displays the following service provider information:

- **Entity ID**: Identifies the service provider application
- **Single Sign On URL**: The endpoint URL responsible for receiving and parsing a SAML assertion (also referred to as "Assertion Consumer Service")
- **Single Sign Off URL**: The endpoint URL responsible for initiating the SAML logout process
- **Certificate**: The encryption certificate (verification certificate) in X.509 format

You can click the following in the Service Provide section:

- **Download Metadata**: Downloads the Deep Discovery Inspector metadata file. You can import the metadata file on an Active Directory Federal Services (ADFS).

Note

If you change the Deep Discovery Inspector FQDN after importing the metadata file on your identity provider, you will need to download the metadata file again and reimport the file on your identity provider.

- **Download Certificate**: Downloads the Deep Discovery Inspector certificate file.

- **Update**: Uploads a new certificate on Deep Discovery Inspector. The certificate must meet the following specifications:
  - The certificate must be in X.509 PEM format.
  - The certificate must not be protected by a password or pass phrase.
  - Certificates from a private CA or a CA chain must include **Authority Information Access** and **CRL Distribution Points**.

Configuring Identity Provider Settings

Note

- Before you add an identity provider, obtain the metadata file from your identity provider.
- You can add up to two identity providers in Deep Discovery Inspector, one each for AD FS and Okta.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **SAML Authentication**.
2. In the Identity Provider section, do one of the following:
   - In the drop-down box above the table, select **Custom Identity Provider** to add or view your Identity Providers, or select **Internal Identity Provider** to view to view the internal Identity Provider used for Vision One.

     Note

     The drop-down box only appears when Deep Discovery Inspector is integrated with Vision One.

   - Click **Add** to add a new entry.
   - Click an identity provider service name to change the settings.

3. Select a status option to enable or disable the identity provider settings.
4. Type a descriptive name for the identity provider.

Note

Deep Discovery Inspector displays the service name in the drop-down list on the Log On screen.

5. Type a description.
6. Click **Select** and choose the metadata file obtained from your identity provider.

   After importing the metadata file, the system displays the identity provider information.
7. Click **Save**.

Configuring Okta

Okta is a standards-compliant OAuth 2.0 authorization server that provides cloud identity solutions for your organization. Okta is a single sign-on provider that allows you to manage user access to Deep Discovery Inspector.

This section describes how to configure Okta as a SAML (2.0) identity provider for Deep Discovery Inspector to use.

Before you begin configuring Okta, make sure that:

- You have a valid subscription with Okta that handles the sign-in process and that eventually provides the authentication credentials to the Deep Discovery Inspector management console.
- You are logged on to the management console as a Deep Discovery Inspector administrator.

Procedure

1. Log in to your Okta organization as a user with administrative privileges.

2. Click **Admin** in the upper right, and then navigate to **Applications** > **Applications**.
3. Click **Add Application**, and then click **Create New App**.

   The **Create a New Application Integration** screen appears.
4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.
5. On the **General Settings** screen, type a name for Deep Discovery Inspector in **App name**, for example, "Deep Discovery Inspector", and click **Next**.
6. On the **Configure SAML** screen, specify the following:
   a. Type the **Single sign on URL** for Deep Discovery Inspector.

      Note

      To obtain the Deep Discovery Inspector single sign on URL, go to **Administration** > **Integrated Products/Services** > **SAML Integration** in the Deep Discovery Inspector management console, and copy the **Single Sign On URL** in the **Service Provider** section.

   b. Select **Use this for Recipient URL and Destination URL**.
   c. Specify the Audience URI in **Audience URI (SP Entity ID)** based on your serving site:
   d. Type `EmailAddress` in **Name ID format**.
   e. In the **Group Attribute Statements (Optional)** section, specify the following:
      - **Name**: `DDI_GROUP`
      - **Filter**: **Matches** `^(.*)*$`
   f. Click **Next**.
7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, select **This is an internal app that we have created**, and then click **Finish**.

The **Sign On** tab of your newly created Deep Discovery Inspector application appears.

8. Click **Identity Provider Metadata** to download the metadata file from Okta.

Note

Import this metadata file to Deep Discovery Inspector.

9. Assign the application to groups and add people to groups.
   a. Select **Directory** > **Groups**.
   b. Click the groups that you want to assign the application to, and then click **Manage Apps**.

      The **Assign Applications** screen appears.
   c. Locate Deep Discovery Inspector you added and click **Assign**.
   d. Click **Manage People**.

      The **Add People to Groups** screen appears.
   e. Locate the user you want to allow access to Deep Discovery Inspector and add the user to the Deep Discovery Inspector group.
   f. Confirm that the application is assigned to the user and group.

      After assigning an application to a group, the system automatically assigns the application to all users in the group.
   g. Repeat the above steps to assign the application to more groups as necessary.

You are now ready to configure Okta for single sign-on and create the required SAML groups in the Deep Discovery Inspector management console.

Configuring Active Directory Federation Services

This section describes how to configure a federation server using Active Directory Federation Services (AD FS) to work with Deep Discovery Inspector.

Note

Deep Discovery Inspector supports connecting to the federation server using AD FS 4.0 and 5.0.

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

Before you begin configuring AD FS, make sure that:

- You have a Windows Server installed with AD FS 4.0 or AD FS 5.0 to serve as a federation server.
- You are logged on to the management console as a Deep Discovery Inspector administrator.
- You have obtained the metadata file from Deep Discovery Inspector.
- You have configured web browser settings on each endpoint to trust Deep Discovery Inspector and the federation server.

  For details, see *Configuring Endpoints for Single Sign-on through AD FS on page 6-169*.

Procedure

1. Go to **Start** > **All Programs** > **Administrative Tools** to open the AD FS management console.
2. Click **AD FS** in the left navigation, and under the **Action** area on the right, click **Add Relying Party Trust...**.
3. Complete settings on each tab of the **Add Relying Party Trust Wizard** screen.

a. On the **Welcome** tab, select **Claims aware** and click **Start**.

b. On the **Select Data Source** tab, select **Import data about the relying party from a file**, click **Browse** to select the metadata file you obtain from Deep Discovery Inspector; then, click **Next**.

c. On the **Specify Display Name** tab, specify a display name for Deep Discovery Inspector, for example, "Deep Discovery Inspector", and click **Next**.

d. On the **Choose Access Control Policy** tab, select **Permit everyone** and click **Next**.

e. On the **Ready to Add Trust** tab, click **Next**.

f. On the **Finish** tab, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** and click **Close**.

   The **Edit Claim Rules** screen appears.

4. On the **Issuance Transform Rules** tab, click **Add Rule...**.

5. Complete the settings on each tab of the **Add Transform Claim Rule Wizard** screen.

   a. On the **Choose Rule Type** tab, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list, and click **Next**.

   b. On the **Configure Claim Rule** tab, specify a claim rule name in the **Claim rule name** text box, and select **Active Directory** from the **Attribute store** drop-down list.

   c. Select the **User-Principal-Name** LDAP attribute and specify **Name ID** as the outgoing claim type for the attribute.

   d. Click **OK**.

6. Click **Add Rule...**.

   The **Add Transform Claim Rule Wizard** screen appears.

7. Complete the settings on each tab of the **Add Transform Claim Rule Wizard** screen.

a. On the **Choose Rule Type** tab, select **Send Group Membership as a Claim** from the **Claim rule template** drop-down list, and click **Next**.

   The **Configure Claim Rule** tab appears.

b. For **Claim rule name**, type the name of the AD group.

c. For **User's group**, click **Browse** and then select the AD group.

d. For **Outgoing claim type**, type `DDI_GROUP`.

e. For **Outgoing claim value**, type the name of the AD group.

f. Click **Apply** and then click **OK**.

8. Collect the single sign-on URL and export the Identity Provider metadata for AD FS.

   a. On the AD FS management console, go to **AD FS** > **Service** > **Endpoints**.

   b. In the right pane, under **Endpoints** > **Metadata**, in the **Federation Metadata** row, copy the URL path.

   c. Add the host name of the AD FS computer to the URL path that you copied.

      For example, `https://hostname/FederationMetadata/2007-06/FederationMetadata.xml`

   d. To retrieve the Identity Provider metadata, use a web browser to navigate to the complete URL that you obtained in the previous step.

   e. Save the Identity Provider metadata file as an XML file.

Note

Import this metadata file to Deep Discovery Inspector.

Configuring Endpoints for Single Sign-on through AD FS

Before endpoints can access Deep Discovery Inspector using single sign-on through Active Directory Federation Services (AD FS), configure the web

browser settings on each endpoint to trust both Deep Discovery Inspector and the federation server.

You can configure the web browser settings on endpoints manually or through group policies.

The following provides the procedure for endpoints running Windows 10. Steps may vary depending on the Windows version.

Procedure

1. On an endpoint, open the **Control Panel** from the Start menu.
2. Click **Network and Internet** > **Internet Options**.

   The Internet Properties screen appears.
3. Click the **Security** tab.
4. Select **Local intranet** and click **Sites**.
5. Click **Advanced**.
6. In the **Add this website to the zone** field, type FQDN or IP address of the account federation server and click **Add**.
7. Repeat Step 6 to add the FQDN or IP address of Deep Discovery Inspector to the Websites list.
8. Click **Close**.
9. Click **OK**.
10. Click **OK**.

Microsoft Active Directory

Use the **Microsoft Active Directory** screen to integrate a Microsoft Active Directory server with Deep Discovery Inspector. Deep Discovery Inspector can then add Active Directory accounts to the list of accounts that can access the management console.

Deep Discovery Inspector supports Microsoft Windows Server 2012 R2 and above.

Configuring Microsoft Active Directory integration

Note

Before starting, obtain the information required to configure the Active Directory integration from the server administrator.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Microsoft Active Directory**.
2. Select **Use Microsoft Active Directory**.
3. Configure the following settings:

Setting	Description
Server type	The type of Active Directory server you want to connect to. Available options: • **Microsoft Active Directory** • **Microsoft Active Directory Global Catalog**
Server address	The IP address or public FQDN of the Active Directory server.
Encryption	The protocol used to protect data during communication between the Deep Discovery Inspector and the Active Directory server. Available options: • **SSL** • **STARTTLS**

Setting	Description

Port	The network port number used for communication with the Active Directory server.
	
	Note
	Trend Micro recommends using the following default ports:
	• For Microsoft Active Directory, or OpenLDAP:
	  • **SSL**: 636
	  • **StartTLS**: 389
	• For Microsoft AD Global Catalog:
	  • **SSL**: 3269
	  • **STARTTLS**: 3268

Base distinguished name	The starting point in the Active Directory hierarchy from which Deep Discovery Inspector syncs data.
User name	The user name of your Active Directory server.
Password	The password associated with the user account.

4. If your organization uses a CA certificate, select Use CA certificate and click Select to locate the CA certificate file.
5. (Optional) Click **Test Connection** to verify that a connection to the LDAP server can be established using the specified information.
6. Click **Save**.

Syslog

Deep Discovery Inspector transports log content to syslog servers through the following channels:

- Transmission Control Protocol (TCP)

- Transmission Control Protocol (TCP) with Secure Sockets Layer (SSL) encryption
- User Datagram Protocol (UDP)

Configure Deep Discovery Inspector to send log content in the following formats:

- Common Event Format (CEF)
- Log Event Extended Format (LEEF)
- Trend Micro Event Format (TMEF)

Adding a syslog server

Add a maximum of three syslog servers.

Procedure

1. Go to **Administration** > **Integrated Products / Services** > **Syslog**.
2. Click **Add**.

   The **Add Syslog Server** screen appears.
3. Select **Enable syslog server**.
4. Type the server name or IP address and the port number of the syslog server.

   Trend Micro recommends using the following default syslog ports:

   - UDP: 514
   - TCP: 601
   - SSL: 6514
5. Select a facility level.

   The facility level specifies the source of a message.
6. Select a syslog severity level.

The syslog severity level specifies the type of messages to be sent to the syslog server.

TABLE 6-19. Syslog Severity Levels

LEVEL	SEVERITY	DESCRIPTION
0	Emergency	• Complete system failure Take immediate action.
1	Critical	• Primary system failure Take immediate action.
2	Alert	• Urgent failures Take immediate action.
3	Error	• Non-urgent failures Resolve issues quickly.
4	Warning	• Error pending Take action to avoid errors.
5	Notice	• Unusual events Immediate action is not required.
6	Informational	• Normal operational messages useful for reporting, measuring throughput, and other purposes No action is required.
7	Debug	• Useful information when debugging the application. **Note** Setting the debug level can generate a large amount of syslog traffic in a busy network. Use with caution.

7. Select the format to send event logs to the syslog server.

   - **CEF**

     Common Event Format (CEF) is an open log management standard developed by Micro Focus 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® QRadar® Security Intelligence Platform. LEEF comprises an LEEF header, event attributes, and an optional syslog header.

   - **Trend Micro Event Format (TMEF)**

     Trend Micro Event Format (TMEF) is the format used by Trend Micro products for reporting event information. Deep Discovery Advisor uses TMEF to integrate events from various Trend Micro products.

8. Select the logs to send to the syslog server.

9. Select **Connect through a proxy server** to use the settings configured on **Administration** > **System Settings** > **Proxy** to connect to a syslog server.

   Select this option if you require the use of proxy servers for intranet connections.

10. Click **Save**.

System settings

Go to **Administration** > **System Settings** to configure basic Deep Discovery Inspector settings.

This section includes the following basic settings:

- *Network on page 6-176*
- *Network interface on page 6-176*
- *Proxy on page 6-178*

- *SMTP on page 6-179*
- *SNMP on page 6-180*
- *HTTPS certificate on page 6-183*
- *Time on page 6-185*
- *Session timeout on page 6-186*

Network

The **Network** screen enables management of the appliance's network settings, including TLS 1.2 or above enforcement.

Go to **Administration** > **System Settings** > **Network**.

See *Configuring the appliance IP settings on page 2-9* for details on configuring the network settings.

Network interface

Manage the management port, data ports, and inline ports on the **Network Interface** screen.

See the following topics for more details:

- *Data and management ports on page 6-176*
- *Inline ports on page 6-177*

Note

Inline ports are only available when Deep Discovery Inspector has a inline (LAN bypass) network interface card installed. For more details, see the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

Data and management ports

For details about managing the data and management network interface ports, see *Managing network interface ports on page 2-14*.

On the **Network Interface** screen, you can do the following:

- View the status of these ports
- View the network interface of these ports
- Configure Encapsulated Remote Mirroring
- Configure identification for decrypted SSL traffic

Inline ports

Inline ports are only available when Deep Discovery Inspector has a inline (LAN bypass) network interface card installed. For more details, see the *Installation and Deployment Guide*, and the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

When Deep Discovery Inspector is deployed as an inline appliance and configured to decrypt TLS traffic, an event such as a system crash, power outage, or other unexpected condition may have an impact on the network accessibility. Deep Discovery Inspector uses traffic bypass to cross-connect the two physical network ports. Traffic bypass helps to prevent Deep Discovery Inspector from being a single point of failure in the network.

Deep Discovery Inspector can automatically enable traffic bypass and you can manually enable traffic bypass.

- Automatic traffic bypass

  Deep Discovery Inspector performs self-health checks. If an issue is detected, Deep Discovery Inspector automatically enters traffic bypass mode to prevent the potential impact on the network. When this occurs, a global notification appears in the management console, and if configured, Deep Discovery Inspector can send an email notification or an SNMP trap.

Important

Issues such as power outage, system hang, or kernel panic can prevent Deep Discovery Inspector from sending email notifications and SNMP traps. Trend Micro recommends that you use tools like an NMS or system monitoring to identify these issues.

- Manual traffic bypass

  You can manually enable traffic bypass mode. To enable traffic bypass mode, go to **Administration** > **System Settings** > **Network Interface** and toggle **Enable traffic bypass**.

  You can also enable traffic bypass mode in the preconfiguration console. For more details, see the *Installation and Deployment Guide*.

Proxy

Configure a proxy server for the following operations:

- Downloading updates from the Trend Micro ActiveUpdate server or another update source
- Updating the product license
- Connecting to other Trend Micro products (Deep Discovery Director, Apex Central, and Smart Protection Server).

Configure a proxy server

Deep Discovery Inspector can use a proxy server for pattern, engine, and license updates. Other products and services may be able to use the same proxy server.

You need to enable proxy server settings on the configuration page of each product or service.

Procedure

1. Go to **Administration** > **System Settings** > **Proxy**.
2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Specify the **Server address** and the **Port** number.

   Deep Discovery Inspector supports HTTP and HTTPS proxy servers.
4. If the proxy server requires authentication, select **Proxy server requires authentication** and specify a **User Name** and **Password**.

5. Click **Test Connection** to verify connection settings.
6. Click **Save**.

SMTP

The Simple Mail Transfer Protocol (SMTP) is used to send email notifications and reports.

Configuring SMTP settings

Procedure

1. Enable **Use an SMTP server for sending notifications and reports**.
2. Type a valid SMTP server address and port number.
3. Select the **Connection security**.
4. Type the **Sender email address**.
5. If the SMTP server requires authentication, specify the authentication settings.

   Important

   Make sure to add the Deep Discovery Inspector IP address to the SMTP relay list.

   Note

   Deep Discovery Inspector supports LOGIN, PLAIN, and CRAM-MD5 SMTP authentication.

   a. Enable **server requires authentication**.

   b. Type the user name and password.
6. Click **Save**.

7. (Optional) Send a test email using the SMTP server.

   a. Click **Test Mail**.

   b. Type the **Recipient email address**.

   c. Click **OK**.

   If the SMTP server settings are correctly configured, Deep Discovery Inspector sends a test email message to the recipient addresses.

SNMP

Simple Network Management Protocol (SNMP) is used to manage devices on IP networks. Deep Discovery Inspector supports SNMP version 1, 2, and 3.

Enable the SNMP to check system running status, network card link up or link down, and component update status.

The SNMP has two modes:

- SNMP trap

  SNMP trap allows a managed product to report its status to the SNMP Network Management Station.

- SNMP agent

  An SNMP agent is a program that gathers and organizes information about a product into predefined hierarchies, and responds to queries using the SNMP protocol.

  Use SNMP agent to obtain Deep Discovery Inspector system information, including the following:

  - Product version
  - CPU, memory, and disk information
  - network interface throughput and concurrent connections

Configuring SNMP trap mode

The following table lists the product-Specific SNMP OIDs for Trap Mode:

OID Value	OID Description
.1.3.6.1.4.1.6101.999.2.2	Important component update failures
.1.3.6.1.4.1.6101.3003.3.1	NTP sync-up failure
.1.3.6.1.4.1.6101.3003.3.2	Entered traffic bypass mode unexpectedly

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Select **Send SNMP trap messages**.
3. Specify the address of the manager server.
4. Configure SNMP trap mode.
   - For **SNMP v1/v2c**, specify the community name
   - For **SNMP v3**, specify a security model:
     - **No authentication or privacy**: Specify the user name
     - **Authenticated**: Specify the user name and password
     - **Authenticated with privacy**: Specify the user name, password, and the privacy passphrase.
5. Click **Save**.

Configuring SNMP agent mode

You can use an SNMP network management station to monitor Deep Discovery Inspector.

The following table lists the product-Specific SNMP OIDs for Agent Mode:

OID Value	OID Description
.1.3.6.1.4.1.6101.3003.1	Product version
.1.3.6.1.4.1.6101.3003.2	Network interface throughput
1.3.6.1.4.1.6101.3003.4	Concurrent connections
.1.3.6.1.4.1.6101.3003.5	Inline network card status

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Select **Listen for requests from SNMP managers**.
3. If needed, specify a **System location** and **Administrator contact**.
4. Configure SNMP agent mode.
   - For **SNMP v1/v2c**:
     a. Specify the allowed community names.
     b. Specify the trusted manager server address.
   - For **SNMP v3**, specify a security model:
     - **No authentication or privacy**: Specify a user name
     - **Authenticated**: Specify user name and password
     - **Authenticated with privacy**: Specify user name, password, and a privacy passphrase.
5. Click **Save**.
6. If needed, click **Export MIB file**.

   The MIB file can be imported to the SNMP Management Station.

HTTPS certificate

Verify that the HTTPS certificate details are accurate.

TABLE 6-20. HTTPS Certificate Details

ITEM	DESCRIPTION
Version	Certificate version number
Serial Number	Certificate unique identification number
Signature Algorithm	Algorithm used to create the signature
Issuer	Entity that verified the information and issued the certificate
Valid From	Date the certificate is first valid
Valid To	Certificate expiration date
Subject	Person or entity identified
Public Key	The 2048-bit or higher public key used for encryption

Generating an HTTPS certificate

Deep Discovery Inspector supports the following HTTPS formats:

- X509 PEM

Procedure

1. From a Linux operating system, use the following command to generate a certificate:

   ```
   openssl req -newkey rsa:2048 -x509 -sha512 -days 365 -nodes
   -out server.pem -keyout server.pem
   ```

2. Specify the following values:
   - Country Name (2 letter code)
   - State or Province Name (full name)

- Locality Name (for example, city)
- Organization Name (for example, company)
- Organization Unit Name (for example, section)
- Common Name (for example, your name or your server's host name)
- Email Address

3. Press **Enter**.

   A file named `server.pem` is generated.

4. Save the `server.pem` file and import it into Deep Discovery Inspector as your HTTPS Certificate.

   For details, see *Importing an HTTPS certificate on page 6-184*.

5. (Optional) To verify that the HTTPS certificate imported successfully, do the following:

   a. Go to **Administration** > **System Logs**.

   b. Select the time period, including the day of the HTTPS Certificate import.

   c. For **Log Type**, select **System events**.

      If the import is successful, the following log appears in the list:

      Import certificate: Import new certificate successfully

Importing an HTTPS certificate

To eliminate any potential browser security issues, replace the Deep Discovery Inspector default security certificate with an imported security certificate from a reputable Certificate Authority (CA).

Deep Discovery Inspector supports the following HTTPS formats:

- X509 PEM

Procedure

1. Go to **Administration** > **System Settings** > **HTTPS Certificate**.
2. On the **HTTPS Certificate** screen, click **Replace Certificate**.

   The **Import Certificate** screen appears.
3. On the **Import Certificate** screen, click **Choose File** to navigate to and select a new certificate.
4. Click **Import**.

   A new certificate is imported.
5. Log on to Deep Discovery Inspector from another browser to verify the new certificate.

Note

Deep Discovery Inspector does not need to be restarted.

Time

Synchronize the system time with the Network Time Protocol (NTP) server or configure it manually.

Configuring time options

Procedure

1. Go to **Administration** > **System Settings** > **Time**.
2. Under **System Time Settings**, select one of the following:
   - **Synchronize appliance time with a Network Time Protocol (NTP) server**:
     a. Specify the NTP server address.
     b. Click **Synchronize Now**.

Note

For virtual Deep Discovery Inspector appliances, Trend Micro recommends using an NTP server to synchronize the appliance time.

- Set the system time manually:
  a. Click the calendar icon or type the month, day, and year using the mm/dd/yyyy format.
  b. Select the hour, minute, and second.

3. Using the **Time Zone** drop-down menu, select the time zone.
4. Click **Save**.

Session timeout

Configure how long Deep Discovery Inspector waits before logging out an inactive management console user session.

Configuring session timeout

Procedure

1. Go to **Administration** > **System Settings** > **Session Timeout**.
2. At **Timeout Settings**, select a time period before inactivity logoff.
   - **2 minutes**
   - **5 minutes**
   - **10 minutes**
   - **15 minutes (Recommended)**
   - **30 minutes**
   - **60 minutes**

- **1 day**
- **3 days**

3. Click **Save**.

Note

The default management console timeout is 15 minutes.

Accounts

This section includes the following topics:

- *About accounts on page 6-187*
- *User roles and menu item permissions on page 6-188*
- *Adding a local account on page 6-191*
- *Adding an Active Directory account on page 6-193*
- *Editing an account on page 6-196*
- *Resetting an account password on page 6-197*
- *Deleting an account on page 6-198*
- *Unlocking an account on page 6-199*

About accounts

Deep Discovery Inspector allows you to grant access to selected sections of the management console.

Important

You cannot disable or modify the “Trend Vision One Administrator” and “Trend Vision One Viewer” accounts.

Deep Discovery Inspector supports 128 local accounts, 512 Active Directory accounts, and 512 SAML accounts, including the following roles:

- System administrator (default)
- Administrator (user-created)
- Viewer (user-created)

All users (system administrator, other administrators, viewers) share one dashboard. Each management console viewer account is provided a partially independent dashboard. Changes to any account's dashboard affect the dashboards of other accounts.

Deep Discovery Inspector logs the following activities for all users:

- Log on
- Account password changes
- Log off
- Session timeout

Deep Discovery Inspector displays the state of each user as follows:

- Online: Green
- Offline: Gray

Deep Discovery Inspector displays users who sign on to Deep Discovery Inspector from Trend Micro Apex Central.

Created By	Example
Deep Discovery Inspector	`SYSTEM`
Deep Discovery Inspector user name	`admin`
Trend Micro Apex Central user name	`admin(admin)`

User roles and menu item permissions

Each user is assigned a specific role. The role determines the management console menu items accessible to that user.

TABLE 6-21. User Roles

ROLE	DESCRIPTION
System administrator	Accesses all sections of the management console
Administrator	Accesses all sections of the management console
Viewer	Views detection and system information

Permissions determine the level of access to each menu item on the management console. Deep Discovery Inspector provides the following permissions:

- **Configure**: Full access to a menu item

  Users can configure all settings, perform all tasks, and view data.

- **View**: View-only settings, tasks, and data
- **No access**: Blocked menu items

SECTION	SUBSECTION	SYSTEM ADMINISTRATOR	ADMINISTRATOR	VIEWER
Dashboard	N/A	Configure	Configure	Configure Exceptions: Add IP addresses to Network Groups, Registered Domains, and Registered Services
Detections	Affected Hosts	Configure	Configure	Configure Exceptions: Configure Add IP addresses to Network Groups, Registered Domains, and Registered Services

Section	Subsection	System Administrator	Administrator	Viewer
	Hosts with Notable Event Detections	Configure	Configure	Configure Exceptions: Add IP addresses to Network Groups, Registered Domains, and Registered Services
	C&C Callback Addresses	Configure	Configure	No access
	Suspicious Objects	Configure	Configure	No access
	Retro Scan	Configure	Configure	View
	All Detections	Configure	Configure	Configure Exceptions: Add IP addresses to Network Groups, Registered Domains, and Registered Services
Reports	Scheduled Reports	View	View	View
	Schedules	Configure	Configure	View
	On-demand Reports	Configure	Configure	View
	Customization	Configure	Configure	View
Administration	All	Configure	Configure	No access

Section	Subsection	System Administrator	Administrator	Viewer
	Accounts	Configure	Configure Exceptions: • Reset system administrator password • Edit system administrator	
	System Logs	View	View	
	System Maintenance	Configure	Configure	
Help	All	View	View	View
User Account	Change Password	Configure	Configure	Configure
	Log Off	View	View	View

Adding a local account

Procedure

1. Go to **Administration** > **Accounts**.
2. Click the **Local** tab.
3. Click **Add**.

   The **Add Local Account** screen appears.
4. Configure the account status.

- **Enabled** (default)
- **Disabled**

Note

A user cannot disable their own account.

5. Verify that the **Type** is **Local user**.
6. Type a user name that contains 4 to 32 alphanumeric characters.

Note

The user name can include the following special characters:

- Underscore (_)
- Period (.)
- Hyphen (-)

7. Select a user role.
   - **Viewer** (default)
   - **Administrator**
8. (Optional) For viewer accounts, select **Allow user to mark detections as resolved**.

   For details, see *Viewing all detections on page 4-57*.

Note

The default value for **Allow user to mark detections as resolved** is unselected.

9. Click **Save**.

   Deep Discovery Inspector adds the account information to the local accounts list and generates a default account password.

Tip

Click the reveal password icon ( ) to show or hide the password.

Next steps

Provide the generated default password to the new user. The user must change this password after logging on for the first time. For details, see *Management console account passwords on page 2-6*

Adding an Active Directory account

Procedure

1. Go to **Administration** > **Accounts**.
2. Click the **Active Directory** tab.
3. Click **Add**.

   The **Add Active Directory User / Group** screen appears.
4. Configure the account status.
   - **Enabled** (default)
   - **Disabled**

Note

A user cannot disable their own account.

5. Select **Active Directory user or group** as the **Type** of this account.
6. Type a user or group name and click **Search** to search the Active Directory for matching user accounts or groups.

   Matching user accounts and groups are displayed in the results table.

Note

User accounts are not displayed in the results table if:

- 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

7. Select the Active Directory user account or group to add.
8. Select a user role.
   - **Viewer** (default)
   - **Administrator**
9. (Optional) For viewer accounts, select **Allow user to mark detections as resolved**.

   For details, see *Viewing all detections on page 4-57*.

   Note

   The default value for **Allow user to mark detections as resolved** is unselected.
10. Click **Save**.

    The new account is added to the Active Directory accounts list.

Adding a SAML account

Note

To transfer a user's detection filters and generated reports from an Active Directory account to a SAML account, create the SAML account and have the user log in to the SAML account first before deleting the user's Active Directory account.

Procedure

1. Go to **Administration** > **Accounts**.
2. Click the **SAML** tab.
3. Click **Add**.

   The **Add SAML Account** screen appears.
4. Configure the account status.

   Note

   A user cannot disable their own account.
5. Type the claim value.

   Note

   The claim value is the outgoing claim value in ADFS Claim Issuance Policy Rules or the group name in Okta.
6. (Optional) Type a description for the account.
7. Select a user role.
   - **Viewer** (default)
   - **Administrator**
8. (Optional) For viewer accounts, select **Allow user to mark detections as resolved**.

   For details, see *Viewing all detections on page 4-57*.

   Note

   The default value for **Allow user to mark detections as resolved** is unselected.
9. Click **Save**.

The new account is added to the SAML accounts list.

Editing an account

Only administrators can edit accounts. Any administrator can add an account and edit or delete any other administrator account except for the system administration account. Administrators can change their account password but cannot edit or delete their own accounts.

Procedure

1. Go to **Administration** > **Accounts**.
2. Click the tab for the account type.
   - **Local**
   - **Active Directory**
   - **SAML**
3. Configure the account status.
   - **Enabled** (default)
   - **Disabled**
4. (Optional) To reset the password of a local account, do the following:

   Important

   Make sure you are targeting the correct account before clicking **Reset**.

   a. Under the **Reset Password** column for the target account, click **Reset**.

      Deep Discovery Inspector immediately resets the account password and generates a new default password.

   b. Provide the generated default password to the user. The user must change this password after logging on for the first time. For details, see *Management console account passwords on page 2-6*.

5. Click on a user name.

   The **Edit Account** screen appears.

6. Select a user role.

   - **Viewer** (default)
   - **Administrator**

7. (Optional) For viewer accounts, select **Allow user to mark detections as resolved.**

   For details, see *Viewing all detections on page 4-57*.

   Note

   The default value for **Allow user to mark detections as resolved** is unselected.

8. Click **Save**.

   Deep Discovery Inspector updates the account information in the table in the **Accounts** screen.

Resetting an account password

The system administrator can reset the password of every local account. Other administrators can reset the password of any local account except the system administrator account.

Important

The passwords of Microsoft Active Directory accounts, SAML accounts, and Trend Micro Apex Central single sign-on (SSO) accounts cannot be changed from the management console.

Procedure

1. Go to **Administration** > **Accounts**.

2. Click the **Local** tab.

Important

Ensure you select the correct account before clicking **Reset**.

3. Under the **Reset Password** column for the target account, click **Reset**.

   Deep Discovery Inspector immediately resets the account password and generates a new default password.

Tip

Click the reveal password icon ( ) to show or hide the password.

Next steps

Provide the generated default password to the user. The user must change this password after logging on for the first time. For details, see *Management console account passwords on page 2-6*.

Deleting an account

An administrator can delete any account except the system administrator account, logged-on accounts, and Active Directory and SAML group accounts with logged-on accounts.

Important

When an account is deleted, any saved search and report schedule created by the account will also be deleted. However, any generated reports will not be deleted.

Procedure

1. Go to **Administration** > **Accounts**.
2. Click the tab for the account type.

3. Check the box beside a user name.
4. Click **Delete**.

Important

Make sure you are targeting the correct account before clicking **Delete**.

Unlocking an account

After 5 failed log in attempts, local accounts are automatically locked. Locked accounts are automatically unlocked after 10 minutes. To manually unlock an account, follow the procedure below.

Procedure

1. Log in to the Deep Discovery Inspector management console using an administrator account that is not locked.
2. Go to **Administration** > **Accounts**.
3. Click the **Local** tab.
4. View the locked status of accounts in the **Locked** column.
5. In the left-most column, select each account to unlock.
6. Click **Unlock**.

   The **Unlock Account** window appears and displays which accounts were unlocked.
7. In the **Unlock Account** window, click **Close**.

System logs

System Logs (**Administration** > **System Logs**) displays logs that contain summaries of system events, including component updates and appliance restarts.

Deep Discovery Inspector can store logs in a database or in a Syslog server. You can query logs from the log database and export logs to a CSV file.

The following table describes the information system logs contain:

Column	Description
Timestamp	The date and time of the event
Log Type	The type of event. Available options: • **All** • **System events** • **Update events**
Level	The severity of the event Available options: • `Informational` • `Warning` • `Error`
Outcome	Whether the event was successful or not.
Action By	The user account or system that triggered the event. The following entities can trigger an event: • Deep Discovery Inspector user accounts (Example: `johnadmin`) • **SYSTEM**: Deep Discovery Inspector • **TREND VISION ONE** • **DEEP DISCOVERY DIRECTOR** • **APEX CENTRAL**
IP Address	The IP address that triggered the event
Description	The Event details

Column	Description
Details	Extra information about events related to *Virtual Analyzer setup*, *packet capture*, and *network group and assets*.

System maintenance

Go to **System Maintenance** to perform the following operations:

- *Storage maintenance on page 6-201*
- *Backup / restore on page 6-203*
- *Power off / restart on page 6-207*

Storage maintenance

Use the **Storage Maintenance** screen for the following operations:

- Manage log and report storage
- View the status of the Deep Discovery Inspector database
- Repair corrupted database files

Deep Discovery Inspector maintains logs and reports in the appliance hard disk. To set criteria and view logs, go to *Detections on page 4-1* and *System logs on page 6-199*.

Manually delete logs and reports on a regular basis to manage hard disk space. The deletion schedule depends on your environment and the quantity of logs and reports you want to retain.

When log and report storage exceed the maximum disk space, Deep Discovery Inspector automatically deletes logs, beginning with the oldest, by date until the disk size is sufficient to hold the latest logs.

Note

Deep Discovery Inspector can send logs to a syslog server or Apex Central. For details, see *Syslog on page 6-172* and *Registering to Apex Central on page 6-121*.

Performing storage maintenance

Procedure

1. Go to **Administration** > **System Maintenance** > **Storage Maintenance**.
2. Under **Log/Report Deletion**, select logs to delete.
3. Select a deletion action.
   - **Delete all logs selected above**
   - **Delete logs selected above older than** the specified number of days

   Note

   Deep Discovery Inspector automatically deletes logs after 121 days and PCAP files after 16 days.
4. Click **Delete**.

Performing product database maintenance

Procedure

1. Go to **Administration** > **System Maintenance** > **Storage Maintenance**.
2. Under **Log Database Status**, click **Check database status**.
3. (Optional) If one or more database files are corrupted, click **Repair**.

   Deep Discovery Inspector repairs the corrupted files and indicates the database status when the repair action is complete.

Configuring file size settings

Deep Discovery Inspector drops detected files that are larger than the maximum size.

Enabling submission of files to Virtual Analyzer automatically increases the maximum storage file size to 15 MB.

Procedure

1. Go to **Administration** > **System Maintenance** > **Storage Maintenance**.
2. Under **File Size Settings**, specify the maximum file size.
3. Click **Save**.

Backup / restore

Configuration settings include both Deep Discovery Inspector and network configuration settings. Back up configuration settings by exporting them to an encrypted file. If needed, import this file to restore settings.

Deep Discovery Inspector can be reset by restoring the default settings that shipped with the product.

The following settings cannot be backed up:

- Appliance IP settings
- Apex Central settings
- Dashboard (widgets) settings
- Deep Discovery Director settings
- Licenses and Activation Codes
- Mitigation Device settings
- Network Interface settings
- Retro Scan settings
- SAML Authentication settings
- Sandbox as a Service settings
- Smart Protection settings in the **Web Reputation** screen
- Threat Investigation Center settings
- TLS Traffic Inspection setting to enable the feature in the **Inspection Settings** screen

- Trend Vision One settings
- Signing Certificate settings in the **Certificate Management** screen
- Virtual Analyzer settings except **File Submissions** and **Passwords**

Note

Virtual Analyzer is disabled after restoring configuration settings.

- HTTPS Certificate

Tip

Verify all the above settings after importing a configuration file.

Note

- Encrypted files cannot be modified.
- Importing an encrypted file overwrites any settings that are included in the encrypted file, but not all current settings.

  For example, when restoring back up settings from a previous version of Deep Discovery Inspector, any features not included in that version will not be overwritten because there are no settings for that version of Deep Discovery Inspector and are not included in the encrypted file.
- An encrypted file can also be used to replicate settings on another Deep Discovery Inspector.

Back up file settings

Procedure

1. Go to **Administration** > **System Maintenance** > **Backup / Restore**.
2. Under **Backup Configuration**, click **Backup**.

   A file download screen appears.

3. Click **Save**, browse to the target location of the file, and click **Save** again.

   The encrypted backup file is saved.

Importing file settings

Deep Discovery Inspector 6.8 Service Pack 2 can restore backup files only from versions 6.8 and 6.8 Service Pack 2. In addition, Deep Discovery Inspector can restore backup files only from Deep Discovery Inspector appliances that use the same language version.

Procedure

1. Before importing a file, back up the current configurations. For details, see *Back up file settings on page 6-204*.
2. Go to **Administration** > **System Maintenance** > **Backup / Restore**.
3. Under **Restore Configuration**, browse to the location of the encrypted backup file.

   The **File Upload** screen appears.
4. Select the encrypted file to import and click **Restore Configuration**.

   A confirmation message appears.
5. Click **OK**.

   Deep Discovery Inspector restarts after importing and checking the integrity of the configuration file.

Important

- After importing a configuration file, Deep Discovery Inspector disables Virtual Analyzer.
- The management console password might reset if the configuration file containing password information is corrupted.

  If you cannot sign to the management console using your password, use the default password (`admin`) instead.

6. To manually enable Virtual Analyzer, go to **Administration** > **Virtual Analyzer** > **Setup**.

Restoring default settings

Important

Restoring default settings resets all settings including the appliance network settings and product license.

Procedure

1. Before restoring settings, back up the current configurations. For details, see *Back up file settings on page 6-204*.
2. Go to **Administration** > **System Maintenance** > **Backup / Restore**.
3. Under **Default Settings**, click **Reset to Default Settings**.

   A confirmation message appears.
4. Click **OK**.

   Deep Discovery Inspector restarts after restoring the default configuration settings.
5. Wait one minute after re-starting to log onto the management console.

Tip

Use the preconfiguration console to modify the appliance network settings or access the management console using the default IP address, 192.168.252.1/24.

Note

When Deep Discovery Inspector starts, it checks the integrity of its configuration files. The management console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the management console using your preferred password, log on using the default password `admin`.

Power off / restart

The **Power Off / Restart** screen provides options to power off or restart the Deep Discovery Inspector appliance and its associated services.

Note

When Deep Discovery Inspector starts, it checks the integrity of its configuration files. The management console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the management console using your password, log on using the default password `admin`.

Restarting Deep Discovery Inspector

Procedure

1. Go to **Administration** > **System Maintenance** > **Power Off / Restart**.
2. Click **Restart**.
   - To restart services, click **Service**.
   - To restart Deep Discovery Inspector, click **System**.
3. (Optional) In the **Comment** field, specify a reason for restarting the system or service.
4. Click **OK**.

Powering off Deep Discovery Inspector

Procedure

1. Go to **Administration** > **System Maintenance** > **Power Off / Restart**.
2. Click **Power off**.
3. (Optional) In the **Comment** field, specify a reason for powering off Deep Discovery Inspector.
4. Click **OK**.

Licenses

The **License** screen displays license information and accepts valid Activation Codes for Deep Discovery Inspector and Sandbox as a Service.

The trial license for Deep Discovery Inspector limits some of the available on-screen information for the following widgets:

- **All Scanned Traffic**
- **Malicious Network Activities**
- **Malicious Scanned Traffic**
- **Monitored Network Traffic in Past 30 Days**
- **Real-time Scanned Traffic**
- **Virtual Analyzer**

Activation codes

Use a valid Activation Code to enable Deep Discovery Inspector and Sandbox as a Service. Deep Discovery Inspector and Sandbox as a Service 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 Deep Discovery Inspector at:

https://clp.trendmicro.com/

A Registration Key has 22 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxx-xxxx-xxxx

After registration, you will receive an email message with your Activation Code.

Product version

The Activation Code provided by Trend Micro is associated with the product version.

- **Trial version**: Includes all product features

  Upgrade a trial version to the fully licensed version at any time.

- **Fully licensed version**: Includes all product features and technical support

  A grace period takes effect after the license expires. The grace period length varies based on your license. Contact your sales representative to learn your grace period length. Renew the license before it expires by purchasing a maintenance renewal.

Deep Discovery Inspector license expiry

License status displays on the **License** screen. If you are renewing a license and need renewal instructions, click **View license renewal instructions**.

The status includes reminders when a license is about to expire or has expired.

TABLE 6-22. License Expiry Reminders

VERSION	REMINDER
Trial	Displays when the license expires

Version	Reminder
Fully Licensed	• 60 days before expiration ends • 30 days before grace period ends • When the license expires and grace period elapses

The consequences of not upgrading to a fully licensed version are as follows:

Table 6-23. Results of an Expired License

Licence Type and Status	Result
Trial (Expired)	Deep Discovery Inspector disables the following: • Component updates • Scanning • TLS traffic inspection • Virtual Analyzer sample analysis
Fully Licensed (Expired)	Technical support and component updates are not available. Deep Discovery Inspector monitors the network using out-of-date components. These components may not completely protect the network from the latest threats.

Activating or renewing licenses

Procedure

1. Go to **Administration** > **Licenses**.
2. Activate Deep Discovery Inspector.
   a. Under **Deep Discovery Inspector**, click **New Activation Code**.

      The **New Activation Code** screen displays.

   b. Type the new Activation Code and click **Save**.

      The **Trend Micro License Agreement** displays.

c. Read the license agreement and click **Agree**.

   After Deep Discovery Inspector is activated, the **Setup Guide** is displayed.

d. Follow the steps in the **Setup Guide**.

3. (Optional) Activate Sandbox as a Service.

Note

This option only appears on supported Deep Discovery Inspector models.

a. Under **Sandbox as a Service**, click **New Activation Code**.

   The **New Activation Code** screen displays.

b. Type the new Activation Code and click **Save**.

4. (Optional) On the **Licenses** screen, click **Refresh** next to the expiration date of a license to refresh the license details.

5. (Optional) Detailed license information is also available on the Customer Licensing Portal website. To view, click **View details**.

6. (Optional) To view the Trend Micro Terms of Sale and Software License Agreement for the family of products, go to `https://<appliance IP address>/html/eula.htm`.

Note

Deep Discovery Inspector may contain or be delivered with one or more third-party components, some of which may be open source software or other similar license agreements and be subject to different license agreement terms, conditions, limitations, and disclaimers than those set forth in the Trend Micro License Agreement. For details, go to **Help** > **About**.

7. (Optional) Re-enable the internal Virtual Analyzer sandbox for macOS.

Note

The internal Virtual Analyzer sandbox for macOS is automatically disabled when the Deep Discovery Inspector Activation Code is replaced.

For details, see *Sandbox for macOS on page 6-93*.

Chapter 7

Troubleshoot

Learn about common troubleshooting options available in Deep Discovery Inspector and find answers to frequently asked questions in the following topics:

- *Frequently asked questions (FAQs) on page 7-2*
- *Troubleshooting on page 7-5*

Frequently asked questions (FAQs)

Find answers to frequently asked questions in the following topics.

- *FAQs - appliance rescue on page 7-2*
- *FAQs - configuration on page 7-3*
- *FAQs - detections on page 7-3*
- *FAQs - installation on page 7-3*
- *FAQs - upgrade on page 7-4*
- *FAQs - virtual analyzer image on page 7-4*

FAQs - appliance rescue

How do I rescue the Deep Discovery Inspector appliance?

To rescue the Deep Discovery Inspector appliance, do one of the following:

- Reinstall Deep Discovery Inspector and use the saved or default settings.

  Important

  All log data is deleted during reinstallation.

- In the management console, go to **Administration** > **Updates** > **Product Updates** > **Sever Packs / Version Upgrade** and install the service pack or version upgrade file (*.R.tar).

  Important

  The service pack or version upgrade file must be the same version as the installed version.

How do I rescue the Deep Discovery Inspector appliance from unexpected traffic bypass?

To rescue the Deep Discovery Inspector appliance from unexpected traffic bypass, restart the Deep Discovery Inspector applaince. For details, see *Power Off / Restart* in the *Deep Discovery Inspector Administrator's Guide*.

FAQs - configuration

Can I register Deep Discovery Inspector to more than one Apex Central server?

No, you cannot register Deep Discovery Inspector to more than one Apex Central server. For details on registering to an Apex Central server, see *Registering to Apex Central* in the *Deep Discovery Inspector Administrator's Guide*.

FAQs - detections

Why are there no more Virtual Analyzer detections on the widget or the Log Query screen after Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls?

After Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls, the API key changes. Change the API key on the Deep Discovery Inspector management console from **Administration** > **Virtual Analyzer** > **Setup**.

FAQs - installation

Does Deep Discovery Inspector installation disrupt network traffic?

When deployed out-of-band Deep Discovery Inspector does not disrupt network traffic. When deployed out-of-band, Deep Discovery Inspector installation should not disrupt the network traffic because the appliance connects to the mirror port of the switch and not directly to the network.

When deployed inline, Deep Discovery Inspector can disrupt network traffic.

After a fresh installation, Deep Discovery Inspector is unable to obtain a dynamic IP address. What do I do?

Restart the appliance and verify that it is able to obtain an IP address. Next, connect an Ethernet cable from the management port to a known good Ethernet connection and restart the appliance.

FAQs - upgrade

Can I roll back to a previous version after upgrading to Deep Discovery Inspector 6.8 Service Pack 2?

No. The rollback function is not supported.

Why does Deep Discovery Inspector still use old components after updating the software and restarting?

When updating components, Deep Discovery Inspector updates the software first. Restart Deep Discovery Inspector and update the Network Content Inspection Engine. After updating the Network Content Inspection Engine, click **Update**, or wait for the next scheduled update.

How do I verify that the migration was successful?

After the upgrade, go to **Administration** > **System Logs** and in the **Description** column, find the 2 events that are similar to "Attempted to upgrade database instance" and "Updating Deep Discovery Inspector from <old version> to <new version>." Verify that the **Outcome** is **Success** for those 2 events.

What does Deep Discovery Inspector do when the database upgrade process is unsuccessful?

Deep Discovery Inspector rebuilds a new, empty database. All previous database data is not recoverable.

FAQs - virtual analyzer image

I am unable to download images from an FTP server. What should I do?

Verify the following:

- The specified server path, user name, and password are correct
- Both active and passive modes are enabled on the FTP server
- The FTP server supports UTF-8 (in case image names or file paths contain multi-byte characters)

The Found New Hardware wizard opens when the image is tested in VirtualBox. Does this affect Virtual Analyzer?

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another. If the **Found New Hardware** wizard appears when the image is tested in VirtualBox, it may interfere with the CD/DVD auto-run.

Troubleshooting

This section describes common troubleshooting options available in Deep Discovery Inspector.

- *Slow management console response on page 7-5*
- *Detections on page 7-6*
- *"database is corrupt" alert displays on page 7-8*
- *Virtual analyzer on page 7-8*
- *Virtual analyzer images on page 7-9*
- *Cannot connect to network services on page 7-11*
- *Diagnostics on page 7-11*

Slow management console response

The management console response is slow or times out.

This occurs when system resources are insufficient.

Procedure

1. To verify CPU, memory, and disk usage, go to `https://<appliance IP address>/html/troubleshooting.htm`.
2. Under **Real-time Status**, select **System Process (ATOP)**.

   The **System Process** screen appears.
3. Click **Suspend** and verify system resources real-time.

TABLE 7-1. System Resources

ITEM	LINE	COLUMN	DESCRIPTION
CPU	CPU	Idle	The lower the number, the busier the CPU is. If this number is low, view the process information and record the CPU with the highest usage.
MEM	MEM	Free, cache	The "Free" field indicates available memory. A low number means that there is not enough available memory to complete certain actions.
Disk	DSK	Busy	A high number indicates that the disk is busy.

Detections

- *No detections on all detections screen on page 7-6*
- *"unregistered service" server displays in all detections query on page 7-7*
- *Unknown IP addresses display on a screen on page 7-7*
- *Known safe objects flagged as malicious on page 7-7*

No detections on all detections screen

No detections appear on the management console **All Detections** screen.

Procedure

1. Verify that the switch mirror port is configured to mirror both directions of network traffic to the mirror port.

   For details, see *Deployment Planning* in the *Deep Discovery Inspector Installation and Deployment Guide.*

2. Verify that networked packets can be captured.

   a. Go to the troubleshooting pages at `https://<appliance IP address>/html/troubleshooting.htm` and then click on **Network Traffic Dump** .

b. In the drop-down menu, select the data port in use.

c. Click **Capture Packets**.

d. Wait 10 seconds and click **Stop**.

e. Click **View**.

The **Packet Capture Information** screen appears.

1. In the **Capfile information** section, verify that the data rate matches the real-time traffic rate.
2. Click **Conversation by TCP** or **Conversation by UDP**, and verify that TCP and UDP packets are visible.

"unregistered service" server displays in all detections query

A server appears as an **Unregistered service** on the **All Detections** screen.

Verify that the server has been added to the Registered Services list. For more details, see *Adding Registered Services* in the *Deep Discovery Inspector Administrator's Guide*.

Unknown IP addresses display on a screen

IP addresses that do not belong to your network appear on a screen.

Make sure that all IP addresses in your network have been added to the network group correctly. For details, see *Adding Network Groups* in the *Deep Discovery Inspector Adminstrator's Guide*.

Known safe objects flagged as malicious

Known safe files, IP addresses, domains, and URLs are flagged malicious by Virtual Analyzer.

- Add any safe objects to the Allow List. For details, see *Creating a Custom Allow List* in the *Deep Discovery Inspector Administrator's Guide*.

- Move any safe objects from the Suspicious Objects list to the Allow List. For details, see *Viewing Suspicious Objects* in the *Deep Discovery Inspector Administrator's Guide*.

"database is corrupt" alert displays

The management console displays the "Database is corrupt" alert.

This message occurs when the database has been corrupted. As a precaution, data is not written to the database, which now must be manually repaired. For details, see *Performing Product Database Maintenance* in the *Deep Discovery Inspector Administrator's Guide*.

WARNING!

Performing manual repairs on a database results in permanent loss of data.

Virtual analyzer

- *Cannot upload OVA on page 7-8*
- *No virtual analyzer response to file submissions on page 7-8*

Cannot upload OVA

The OVA is too large and cannot upload into Deep Discovery Inspector.

The OVA image must be between 1 GB and 30 GB in size.

No virtual analyzer response to file submissions

File samples were sent to Deep Discovery Inspector but no response was received from Virtual Analyzer.

To receive results, enable file submission to Virtual Analyzer.

Procedure

1. Verify that Virtual Analyzer is enabled.

For details, see *Enabling Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

2. Go to **Administration** > **Virtual Analyzer** > **File Submissions** > **Add** and verify file submission rules are configured as follows:
   - Under **Criteria**, click the applicable file types.
   - Under **Actions**, click **Submit**.

     For details, see *File Submission Rules* in the *Deep Discovery Inspector Administrator's Guide*.
3. Go to **Dashboard** > **Virtual Analyzer Status** and view the **Virtual Analyzer** status field on the **Virtual Analyzer** widget.
   a. If Virtual Analyzer status is "Disabled", enable Virtual Analyzer. Go to **Administration** > **Virtual Analyzer** > **Setup** to enable file submission to a Virtual Analyzer.

      For details, see *Enabling Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

   b. If the Virtual Analyzer status is "Enabled", restart Deep Discovery Inspector.
4. Verify notification settings.

   For details, see *Configuring Email Notification Settings* in the *Deep Discovery Inspector Administrator's Guide*.
5. If the problem persists, contact your technical support provider.

Virtual analyzer images

- *The installation media does not start on page 7-9*
- *"found new hardware" wizard on page 7-10*
- *An image displays a blue screen on page 7-10*

The installation media does not start

The installation CD/DVD does not automatically start.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.
2. Click **Settings** and select **Storage**.
3. Select **Controller: IDE** and verify that the specified type is **PIIX4**.
4. Select the optical disc icon and verify that the specified CD/DVD drive is **IDE Secondary Master**.

"found new hardware" wizard

During Virtual Analyzer image creation, the **Found New Hardware** wizard appears.

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another.

When an image is imported, the **Found New Hardware** wizard may interfere with the CD/DVD auto-run. Make sure the Virtual Analyzer image is created and prepared using the correct procedure. For details, see the *Virtual Analyzer Image Preparation User's Guide* at https://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

An image displays a blue screen

An image displays the blue "Cannot find Operating System" screen when tested in VirtualBox.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.

2. Click the **Settings** and select **System**.
3. On the **Motherboard** tab, verify that the following are selected:
   - **Chipset: ICH9**
   - **Enable IO APIC**
4. On the **Processor** tab, verify that the PAE/NX is enabled.
5. On the **Acceleration** tab, verify that the TV-x/AMD-V is enabled.

Cannot connect to network services

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.

Procedure

1. Go to `https://<appliance IP address>/html/troubleshooting.htm` and click **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.

Diagnostics

For any issue not mentioned, run diagnostics to give test results and debug logs to your Trend Micro Deep Discovery Inspector support provider.

Procedure

1. Open the preconfiguration console.
2. Select **4) System Tasks**, and press ENTER.
3. Follow the instructions in *Performing a Diagnostic Test* in the *Deep Discovery Inspector Installation and Deployment Guide*.

4. Generate a debug log.

   a. Go to `https://<appliance IP address>/html/troubleshooting.htm`.

   b. Go to **Logs** > **Debug Logs**

   c. Under **Debug Log Settings**, set the debug level to **Debug** for the modules you want to debug.

      To avoid performance loss, only set the debug level to **Debug** for required modules. Contact your support provider for advice on how to set the level to debug and obtain the debug report.

   d. Click **Save**.

   e. If possible, reproduce the issue.

   f. Select one or more debug logs to export.

      - **Export debug log**.
      - **Export advanced debug log**.
      - Select one or more dated debug logs under **Export advanced debug log** to export the advanced debug log for that date.

   g. Click **Export**.

      Tip

      To conserve system resources, perform one export at a time.

   h. Under **Debug Log Settings**, click **Reset to default log settings**.

   i. Under **Debug Log Maintenance**, click **Purge Debug Logs**.

Inline deployment and TLS inspection

- *Network connectivity issue on page 7-13*
- *TLS connection issue on page 7-14*

Network connectivity issue

Procedure

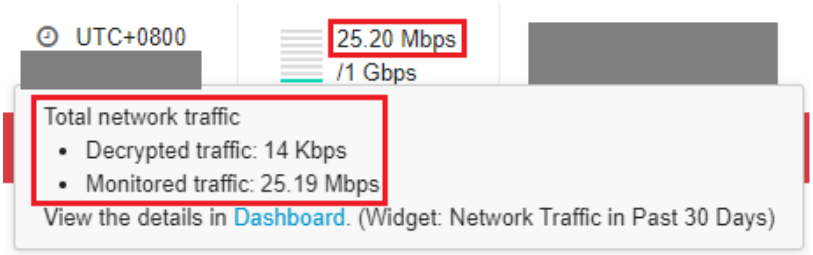
1. Verify that the link status of the inline port is connected.
   a. In the management console, go to **Administration** > **System Settings** > **Network Interface**.
   b. In the **Inline Interfaces** section, view the connection status in the **Status** column.

      Click the right arrow
      (

) at the beginning of the row to display additional information about the connection status.

2. If the link status of the inline port is not connected, then verify that the following applicable items are correct.
   - Interface speed setting
   - Interface duplex setting
   - Interface and transceiver compatibility (particularly for fiber connections)
3. Verify that the there is network activity.

a. In the top-right corner of the management console, hover over the throughput to get more information about the network activity.



4. If there is no network activity, then verify that TLS traffic inspection is enabled in Deep Discovery Inspector and verify that the cable is securely connected to Deep Discovery Inspector and the network device.

5. (Optional) To monitor when traffic bypass unexpectedly occurs, configure agent mode or trap mode for SNMP in Deep Discovery Inspector.

   For details, see *Network Interface* and *SNMP* in the Administrator's Guide.

TLS connection issue

Procedure

1. Identify the reason for the TLS connection issue.

   a. In the management console, go to **Administration** > **Monitoring / Scanning** > **TLS Traffic Inspection** > **Inspection Settings** > **Domain Tunneling** > **Configure tunneled domain**.

   b. If you understand and are able to resolve the issue, then do so. Otherwise, use the steps below to continue troubleshooting.

2. If you are unable to find the issue in **Domain Tunneling**, then view abnormal connection information in the **TLS Connection Monitoring** troubleshooting screen.

a. Go to `https://<appliance IP address>/html/troubleshooting.htm` and then click **TLS Connection Monitoring**.

   The **TLS Connection Monitoring** screen appears.

b. Type a client IP address and then click **Monitor**.

c. After sufficient data is monitored, stop the monitoring.

Note

The monitoring can only save up to 10 minutes of data.

d. If you understand and are able to resolve the issue, then do so. Otherwise, use the steps below to continue troubleshooting.

3. If you are unable to find the issue in **TLS Connection Monitoring**, then collect more details and contact your support provider.

   a. Go to `https://<appliance IP address>/html/troubleshooting.htm` and then click **TLS Network Traffic Dump**.

      The **TLS Network Traffic Dump** screen appears.

   b. Type a client IP address and optionally type the server IP address and port, and then click **Capture Packets**.

   c. After sufficient data is captured, stop the capture.

   d. If the client application that you are using has a log file with TLS connection information, take a screen shot of the client application log.

   e. Take screen shots of your TLS traffic inspection settings.

   f. Send the traffic dump and screen shots to your support representative.

Chapter 8

Technical support

Learn about the following topics:

- *Troubleshooting resources on page 8-2*
- *Contacting Trend Micro on page 8-3*
- *Sending suspicious content to Trend Micro on page 8-4*
- *Other resources on page 8-5*

Troubleshooting resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the support portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.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:

   https://success.trendmicro.com/en-US/contactus/

   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 https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#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:

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	• https://www.trendmicro.com • https://success.trendmicro.com/en-US/contactus/

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  https://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://servicecentral.trendmicro.com/en-us/ers/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0001177

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0002449

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):

https://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

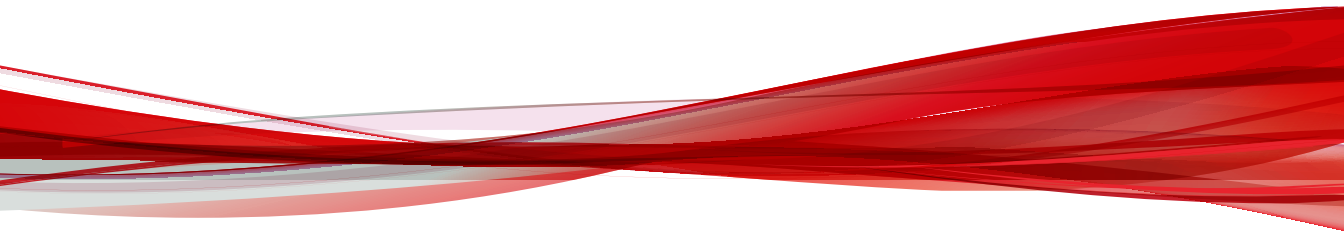
From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://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.

Appendices

Appendices



Appendix A

Virtual analyzer supported file types

TABLE A-1. File Types

FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
Adobe™ Portable Document Format (PDF)	`.pdf`
Adobe™ Shockwave™ Flash file	`.swf`

AMD™ 64-bit DLL file
 	
Note
64-bit DLL files are analyzed only in images that use a 64-bit operating system.
 	
Microsoft™ Windows™ 16-bit DLL file
Microsoft™ Windows™ 32-bit DLL file
	`.dll`
	`.ocx`
	`.drv`

Full File Type	Example File Extensions

AMD™ 64-bit EXE file
ARJ compressed EXE file
ASPACK 1.x compressed 32-bit EXE file
ASPACK 2.x compressed 32-bit EXE file
DIET DOS EXE file
GNU UPX compressed EXE file
IBM™ OS/2 EXE file
LZEXE DOS EXE file
LZH compressed EXE file
LZH compressed EXE file for ZipMail
MEW 0.5 compressed 32-bit EXE file
MEW 1.0 compressed 32-bit EXE file
MEW 1.1 compressed 32-bit EXE file
Microsoft™ Windows™ 16-bit EXE file
Microsoft™ Windows™ 32-bit EXE file
MIPS EXE file
MSIL Portable executable file
PEPACK compressed executable
PKWARE™ PKLITE™ compressed DOS EXE file
PETITE compressed 32-bit executable file
PKZIP compressed EXE file
WWPACK compressed executable file
	`.cpl`
	`.exe`
	`.sys`
	`.crt`
	`.scr`

ALZip compressed file	`.alz`
ALZip archive file	`.egg`

Full File Type	Example File Extensions
Apple QuickTime media	.mov
Compiled HTML (CHM) help file	.chm
Comma-separated values (CSV) file	.csv
Hancom™ Hancell spreadsheet	.cell
Hancom™ Hangul Word Processor (2014 or later) (HWPX) document	.hwpx
Hancom™ Hangul Word Processor (HWP) document	.hwp
HTML Application file	.hta
Java™ Archive **Note** Virtual Analyzer does not support the java library.	.jar
Java™ Applet	.class .cla
Hypertext Markup Language file	.htm .html
JavaScript™ encoded script file	.jse
JavaScript™ file	.js
JungUm™ Global document	.gul
JustSystems™ Ichitaro™ document	.jtd
OpenDocument	.odt .odp .ods
MHTML web archive file	.mht

Full File Type	Example File Extensions
Microsoft™ DOS COM file	.com
Microsoft™ Excel™ spreadsheet	.xls .xla .xlt .xlm
Microsoft™ Excel™ Web Query file	.iqy
Microsoft™ Office 2003 XML file Microsoft™ Word™ 2003 XML document Microsoft™ Excel™ 2003 XML spreadsheet Microsoft™ PowerPoint™ 2003 XML presentation	.xml
Microsoft™ Office Excel™ (2007 or later) spreadsheet Microsoft™ Office Excel™ (2007 or later) macro-enabled spreadsheet	.xlsx .xlsb .xltx .xlsm .xlam .xltm
Microsoft™ Office PowerPoint™ (2007 or later) presentation Microsoft™ Office PowerPoint™ (2007 or later) macro-enabled presentation	.pptx .ppsx
Microsoft™ Office Publisher™ (2016) file	.pub
Microsoft™ Office Word™ (2007 or later) document Microsoft™ Office Word™ (2007 or later) macro-enabled document	.docx .dotx .docm .dotm

Full File Type	Example File Extensions
Microsoft™ Powerpoint™ presentation	.ppt .pps
Microsoft™ Rich Text Format (RTF) document	.rtf
Microsoft™ Windows™ batch file	.bat
Microsoft™ Windows™ command script file	.cmd
Microsoft™ Windows™ PowerShell script file	.ps1
Microsoft™ Windows™ Script File	.wsf
Microsoft™ Windows™ Shell Binary Link shortcut Microsoft™ Windows™ 95/NT shortcut	.lnk
Microsoft™ Word™ 1.0 document Microsoft™ Word™ 2.0 document	.doc .dot
Scalable Vector Graphics file	.svg
Visual Basic™ encoded script file	.vbe
Visual Basic™ script file	.vbs
Extensible Hypertext Markup Language file	.xht .xhtml

Table A-2. Mac File Types

Full File Type	Example File Extensions
Apple disk image	.dmg
Mac OS X Installer Package	.pkg
Mach-O x86/x64	No extension for most executables

Note

Deep Discovery Inspector also supports the submission of Java Archive (.jar) and class (.class) files to Sandbox for macOS.

TABLE A-3. Linux File Types

FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
Executable and Linkable Format (ELF) file	`.elf`
Shell script file	`.sh`

Appendix B

Settings replicated by Deep Discovery Director and Trend Vision One

Deep Discovery Director and Trend Vision One replicate settings from the following screens:

Main Menu Location	Sub-menu Location	Settings
Administration > **Accounts**		All settings
Administration > **Integrated Products / Services**	**Microsoft Active Directory**	All settings
	Syslog	All settings
	Threat Intelligence Sharing	All settings
Administration > **Monitoring / Scanning**	**Hosts / Ports**	All settings
	Threat Detections	All settings

Main Menu Location	Sub-menu Location	Settings
	Web Reputation	All settings **Important** When Deep Discovery Inspector is connected to a Service Gateway with Smart Protection Services enabled, only the settings under **Enable Web Reputation** and **Detection Filters** are replicated.
	Application Filters	All settings
	Deny List / Allow List	All settings
	Detection Rules	All settings
	Detection Exceptions	All settings
	Packet Capture	All settings
	TLS Traffic Inspection > **Certificate Management**	Only Trusted CA Certificate settings
	TLS Traffic Inspection > **Decryption Policy**	All settings
Administration > **Network Groups and Assets**	**Network Groups**	All settings
	Registered Domains	All settings
	Registered Services	All settings
Administration > **Notifications**	**Notification Settings** > **Threat Detections**	All settings

Main Menu Location	Sub-menu Location	Settings
	Notification Settings > **High Risk Host Detections**	All settings
	Notification Settings > **Suspicious Hosts Detections**	All settings
	Notification Settings > **High Network Traffic**	All settings
	Notification Settings > **Unanalyzed Sample Detections**	All settings
	Notification Settings > **Virtual Analyzer Detections**	All settings
	Notification Settings > **Deny List**	All settings
	Notification Settings > **Retro Scan Detections**	All settings
	Delivery Options > **Email Settings**	All settings
Administration > **System Maintenance**	**Storage Maintenance**	Only **File Size Settings**
Administration > **System Settings**	**Network**	Only **Secure Protocol** setting
	Proxy	All settings
	SMTP	All settings
	SNMP	All settings
	Time	All settings
	Session Timeout	All settings
Administration > **Virtual Analyzer**	**File Submissions**	All settings

Main Menu Location	Sub-menu Location	Settings
	Internal Virtual Analyzer > **Sandbox Management** > **Passwords**	All settings
	Setup	Only the internal Virtual Analyzer proxy settings and the sandbox for macOS setting.
Administration > **Updates** > **Component Updates**	**Scheduled**	All settings
	Source	All settings
Detections > **Affected Hosts**		Only **Saved Searches**
Detections > **Affected Hosts - Host Details**		Only **Saved Searches**
Detections > **All Detections**		Only **Saved Searches**
Reports > **Schedules**		All settings
Reports > **Customization**		All settings

Appendix C

TLS support for integrated products/ services

The following integrated products/services use TLS 1.2 or later when the secure protocol option is enabled. For details, see *Configuring the appliance IP settings on page 2-9*.

- Active Directory
- Check Point Open Platform for Security (OPSEC) version R81 or later

Note

A hotfix may be required on Check Point Open Platform for Security for TLS 1.2 or later support. See the official support website of Check Point for details.

- IBM Security Network Protection (XGS) version 5.5 or later
- Internal Virtual Analyzer services
- Trend Micro Apex Central 2019 or later

Note

TLS 1.2 or later must be enabled in the operating system of the Apex Central server, and only Microsoft Windows Server 2008 R2 or later is supported.

See the Microsoft Windows documentation for details about enabling TLS 1.2 or later on Microsoft Windows.

- Management console access
- Palo Alto Panorama and Firewalls
  - PAN-OS version 10.2 or later
  - Panorama version 10.2 or later
- SMTP
- Syslog over SSL
- Threat Intelligence Sharing
- Trend Micro ActiveUpdate
- Trend Micro Certified Safe Software Service
- Trend Micro Community Domain/IP Reputation Service
- Trend Micro Community File Reputation service
- Trend Micro Customer Licensing Portal
- Trend Micro Deep Discovery Analyzer version 5.5 or later
- Trend Micro Deep Discovery Director - On-premises version
- Trend Micro Deep Discovery Director - Cloud version
- Trend Micro Deep Discovery Director - Network Analytics
- Trend Micro Deep Discovery Director - Network Analytics as a Service
- Trend Micro Mobile App Reputation Service
- Trend Micro Predictive Machine Learning engine

- Trend Micro RetroScan
- Trend Micro Sandbox as a Service
- Trend Micro Service Gateway
- Trend Micro Smart Feedback
- Trend Micro Smart Protection Server version 3.3 or later
- Trend Micro Threat Investigation Center
- Trend Micro TippingPoint Security Management System (SMS) version 4.4 or later
- Trend Micro TXOne OT Defense Console
- Trend Micro Web Inspection Service
- Trend Micro Web Reputation Service
- Trend Vision One
- Web Service (SOAP)

Appendix D

Service addresses and ports

Deep Discovery Inspector accesses several Trend Micro services to obtain information about emerging threats and to manage your existing Trend Micro products. The following table describes each service and provides the required address and port information accessible to the product version in your region.

Note

All services connect using HTTPS with TLS 1.2 or above. If your environment has man-in-the-middle devices, verify that the devices support TLS 1.2 or above.

Trend Micro recommends using the **Network Service Diagnostics** screen to troubleshoot the connection to all services. For details, see *Cannot connect to network services on page 7-11*.

TABLE D-1. Service Addresses and Ports

SERVICE	DESCRIPTION	ADDRESS AND PORT	NOTES
ActiveUpdate Server	Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.	`ddi68-p.activeupdate.trendmicro.com/activeupdate:443`	Related to product version and region
Certified Safe Software Service (CSSS)	Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources.	`ctapi.trendmicro.com:443`	
Community Domain/IP Reputation Service	Determines the prevalence of detected domains and IP addresses. Prevalence is a statistical concept referring to the number of times a domain or IP address was detected by Trend Micro sensors at a given time.		Related to product version and region
Community File Reputation	Determines the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time.		Related to product version and region
Customer Licensing Portal	Manages your customer information, subscriptions, and product or service license.	`licenseupdate.trendmicro.com:443`	

Service	Description	Address and Port	Notes
Dynamic URL Scanning	Performs real-time analysis of URLs to detect zero-day attacks.	`ctapi.trendmicro.com:443`	Related to product version and region Disabled when using Smart Protection Server
Mobile App Reputation Service (MARS)	Collects data about detected threats in mobile devices. Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories.		
Predictive Machine Learning engine	Through use of malware modeling, Predictive Machine Learning compares samples to the malware models, assigns a probability score, and determines the probable malware type that a file contains.		Related to product version and region
Retro Scan	A cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network.	`intelliconnect.trendmicro.com:443` `ddi681.retroscan.trendmicro.com:443`	Related to product version and region
Sandbox as a Service (for macOS)	A hosted service that analyzes possible threats for macOS.	`ddaaas.trendmicro.com:443`	

Service	Description	Address and Port	Notes
Sandbox as a Service	A hosted service that analyzes possible threats.	`*.ddcloud.trendmicro.com:443`	Related to product version and region If the product was registered to the service before a product upgrade was performed, Trend Micro recommends that you re-register to the service to connect to the new address.
Smart Feedback	Shares threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains.	`gp.fbs.trendmicro.com:443`	Related to product version and region

Service	Description	Address and Port	Notes
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.	`ddi681.threatconnect.trendmicom:443`	Related to product version and region
Trend Vision One	Extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With Trend Vision One, you can respond more effectively to threats, minimizing the severity and scope of a breach.	`*.xdr.trendmicro.com:443`	Related to product version and region
Trend Vision One - Network Inventory	Enables connection to Trend Vision One.	`*.xdr.trendmicro.com:443` `*.dddxdr.trendmicro.com:443`	Related to product version and region
Web Inspection Service	Web Inspection Service is an auxiliary service of Web Reputation Services, providing granular levels of threat results and comprehensive threat names to users. The threat name and severity can be used as filtering criteria for proactive actions and further intensive scanning.	`ctapi.trendmicro.com:443`	Related to product version and region

Service	Description	Address and Port	Notes
Web Reputation Services	Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis.		Related to product version and region

Index

S

support
resolve issues faster, 8-3

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

www.trendmicro.com
Item Code: APEM6810069/251027