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 the following location:

http://docs.trendmicro.com

Your license and use of the product is governed by the terms and conditions of the Trend Micro License Agreement. Review the latest Trend Micro License Agreement for your language, region, and product group at the following location:


© 2015 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, the Smart Protection Network, Deep Discovery Advisor, Deep Discovery Analyzer, Deep Discovery Inspector, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM37072/150722

Release Date: September 2015

Protected by U.S. Patent No.: Patents pending.
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Support Portal.

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

Evaluate this documentation at the following location:

# Table of Contents

## Preface

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>ix</td>
</tr>
<tr>
<td>Documentation</td>
<td>x</td>
</tr>
<tr>
<td>Audience</td>
<td>xi</td>
</tr>
<tr>
<td>Document Conventions</td>
<td>xii</td>
</tr>
</tbody>
</table>

## Chapter 1: Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Deep Discovery Inspector</td>
<td>1-2</td>
</tr>
<tr>
<td>What's New</td>
<td>1-2</td>
</tr>
<tr>
<td>Features and Benefits</td>
<td>1-3</td>
</tr>
<tr>
<td>Threat Management Capabilities</td>
<td>1-4</td>
</tr>
<tr>
<td>APT Attack Sequence</td>
<td>1-4</td>
</tr>
<tr>
<td>Host Severity</td>
<td>1-6</td>
</tr>
<tr>
<td>Advanced Threat Scan Engine</td>
<td>1-9</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>1-9</td>
</tr>
</tbody>
</table>

## Chapter 2: Get Started

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preconfiguration Console</td>
<td>2-2</td>
</tr>
<tr>
<td>Get Started Tasks</td>
<td>2-2</td>
</tr>
<tr>
<td>Management Console</td>
<td>2-3</td>
</tr>
<tr>
<td>Management Console Requirements</td>
<td>2-4</td>
</tr>
<tr>
<td>Opening the Management Console</td>
<td>2-4</td>
</tr>
<tr>
<td>Management Console Account Passwords</td>
<td>2-6</td>
</tr>
<tr>
<td>Network</td>
<td>2-8</td>
</tr>
<tr>
<td>Network Format Rules</td>
<td>2-9</td>
</tr>
</tbody>
</table>

## Chapter 3: Dashboard

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Overview</td>
<td>3-2</td>
</tr>
</tbody>
</table>
Chapter 4: Detections

About the Detections Screen ................................................................. 4-2

Affected Hosts .................................................................................. 4-3
  Display Options and Search Filters ................................................. 4-4
  Viewing Affected Hosts ................................................................. 4-7
  Viewing Affected Hosts - Host Details .......................................... 4-11
  Affected Hosts - Detection Details ............................................... 4-17
  Affected Hosts Advanced Search Filter ....................................... 4-23

Hosts with Notable Event Detections ................................................ 4-39
  Viewing C&C Callback Attempts .................................................. 4-40
  Viewing Deny List Detections ....................................................... 4-41
  Viewing Suspicious Objects .......................................................... 4-41
### Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C Callback Addresses</td>
<td>4-42</td>
</tr>
<tr>
<td>Viewing C&amp;C Callback Addresses</td>
<td>4-42</td>
</tr>
<tr>
<td>Suspicious Objects</td>
<td>4-43</td>
</tr>
<tr>
<td>Viewing Suspicious Objects</td>
<td>4-44</td>
</tr>
<tr>
<td>Retro Scan</td>
<td>4-45</td>
</tr>
<tr>
<td>Retro Scan and the Smart Protection Network</td>
<td>4-46</td>
</tr>
<tr>
<td>Enabling Retro Scan</td>
<td>4-46</td>
</tr>
<tr>
<td>Retro Scan Screen</td>
<td>4-48</td>
</tr>
<tr>
<td>Retro Scan Report Details Screen</td>
<td>4-49</td>
</tr>
<tr>
<td>Disable Retro Scan</td>
<td>4-49</td>
</tr>
<tr>
<td>All Detections</td>
<td>4-50</td>
</tr>
<tr>
<td>Display Options and Search Filters</td>
<td>4-51</td>
</tr>
<tr>
<td>Viewing All Detections</td>
<td>4-53</td>
</tr>
<tr>
<td>All Detections - Detection Details</td>
<td>4-57</td>
</tr>
<tr>
<td>All Detections Advanced Search Filter</td>
<td>4-63</td>
</tr>
</tbody>
</table>

### Chapter 5: Reports

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Reports</td>
<td>5-2</td>
</tr>
<tr>
<td>Scheduled Reports</td>
<td>5-4</td>
</tr>
<tr>
<td>Schedules</td>
<td>5-6</td>
</tr>
<tr>
<td>Scheduling a Report</td>
<td>5-7</td>
</tr>
<tr>
<td>Deleting a Report Schedule</td>
<td>5-10</td>
</tr>
<tr>
<td>On-demand Reports</td>
<td>5-10</td>
</tr>
<tr>
<td>Generating an On-demand Report</td>
<td>5-12</td>
</tr>
<tr>
<td>Deleting an On-demand Report</td>
<td>5-14</td>
</tr>
<tr>
<td>Customization</td>
<td>5-14</td>
</tr>
<tr>
<td>Customizing Reports</td>
<td>5-15</td>
</tr>
</tbody>
</table>

### Chapter 6: Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates</td>
<td>6-2</td>
</tr>
<tr>
<td>Component Updates</td>
<td>6-2</td>
</tr>
<tr>
<td>Product Updates</td>
<td>6-7</td>
</tr>
<tr>
<td>Notifications</td>
<td>6-14</td>
</tr>
<tr>
<td>Configuring Threat Detection Notifications</td>
<td>6-15</td>
</tr>
</tbody>
</table>
Configuring High Risk Hosts Detections Notifications .......... 6-17
Configuring Suspicious Hosts Detections Notifications .......... 6-20
Configuring High Network Traffic Notifications ................. 6-22
Configuring Unanalyzed Sample Detections Notifications .... 6-24
Configuring Virtual Analyzer Detections Notifications ......... 6-26
Configuring Deny List Notifications ...................................... 6-28
Configuring Retro Scan Detections Notifications ................. 6-30
Delivery Options .................................................................. 6-32

Monitoring / Scanning .......................................................... 6-34
Hosts / Ports ......................................................................... 6-34
Threat Detections ................................................................. 6-36
Smart Protection Technology ................................................ 6-38
Web Reputation ................................................................. 6-41
Application Filters .............................................................. 6-45
Deny List / Allow List ........................................................ 6-47
Detection Rules ................................................................. 6-60
Exceptions ......................................................................... 6-60

Virtual Analyzer ................................................................. 6-63
Virtual Analyzer Setup ........................................................ 6-63
File Submissions ............................................................... 6-65
Internal Virtual Analyzer ................................................... 6-71

Network Groups and Assets .................................................. 6-79
Adding Network Groups ..................................................... 6-79
Adding Registered Domains .............................................. 6-81
Adding Registered Services ............................................... 6-82
Importing/Exporting Configuration Settings ....................... 6-84

Integrated Products/Services ............................................... 6-85
Trend Micro Integrated Products/Services ......................... 6-85
Service Addresses and Ports .............................................. 6-87
Control Manager .............................................................. 6-90
Threat Management Services Portal ................................ 6-95
Syslog .............................................................................. 6-99
Third-Party Products/Services ......................................... 6-102
Mitigation Products/Services ............................................ 6-131

Accounts .......................................................................... 6-134
About Accounts .............................................................. 6-134
Chapter 7: Troubleshoot

Frequently Asked Questions (FAQs) ......................................................... 7-2
FAQs - Activation ................................................................................. 7-2
FAQs - Configuration ........................................................................... 7-2
FAQs - Detections ................................................................................ 7-4
FAQs - Documentation ......................................................................... 7-4
FAQs - Installation .............................................................................. 7-4
FAQs - Upgrade ..................................................................................... 7-5
FAQs - Virtual Analyzer Image ............................................................. 7-6
FAQs - Widgets ...................................................................................... 7-7

Troubleshooting ...................................................................................... 7-8
Slow Management Console Response ................................................ 7-8
Detections ................................................................................................ 7-9
Messages and Alerts ................................................................................ 7-14
Virtual Analyzer ..................................................................................... 7-15
VirtualBox .............................................................................................. 7-16
Diagnostics ............................................................................................ 7-21

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 ............................................................... 8-4

Sending Suspicious Content to Trend Micro ........................................ 8-4
File Reputation Services ......................................................................... 8-4
Email Reputation Services ..................................................................... 8-5
Web Reputation Services ........................................................................ 8-5

Other Resources ..................................................................................... 8-5
Download Center .................................................................................. 8-5
TrendLabs .............................................................................................. 8-6

Documentation Feedback ........................................................................ 8-6

Appendix A: Create a Custom Virtual Analyzer Image

VMware to VirtualBox Conversion ....................................................... A-2
Required Applications ........................................................................... A-3
Modifying the Image Environment ....................................................... A-5
Verifying and Exporting VMware Images .......................................... A-14
Converting VMware ESXi Images ....................................................... A-20
Creating a Custom Virtual Analyzer Image ......................................... A-27
Configuring Virtual Analyzer Images in VirtualBox .......................... A-40
Packaging an Image as an OVA File ................................................... A-45
Importing an OVA File .......................................................................... A-49
Troubleshooting Common Issues ......................................................... A-49

Manually Creating a Custom Image Overview ...................................... A-50
Preparing the Operating System Installer .......................................... A-51
Manually Creating Custom Images ................................................... A-52
Preface

This Administrator’s Guide introduces Trend Micro™ Deep Discovery Inspector™ 3.8 SP1 and walks you through configuring Deep Discovery Inspector.

Learn more about the following topics:

•  Documentation on page x
•  Audience on page xi
•  Document Conventions on page xii
Documentation

The documentation set for Deep Discovery Inspector includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator's Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. 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.</td>
</tr>
<tr>
<td>Installation and Deployment Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. 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.</td>
</tr>
<tr>
<td>User's Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The User's Guide contains general information about Deep Discovery Inspector concepts and features. It introduces selected sections of the management console to users who have been assigned viewer accounts.</td>
</tr>
<tr>
<td>Syslog Content Mapping Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Inspector to your network and on performing the initial configuration.</td>
</tr>
</tbody>
</table>
**DOCUMENT** | **DESCRIPTION**
--- | ---
Readme | The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.

Online Help | Web-based documentation that is accessible from the Deep Discovery 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: [http://esupport.trendmicro.com](http://esupport.trendmicro.com)


**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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UPPER CASE</strong></td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>References to other documents</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td>For example, File &gt; Save means, click File and then click Save on the interface</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Note]</td>
<td>Configuration notes</td>
</tr>
<tr>
<td>![Tip]</td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td>![Important]</td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td>![WARNING!]</td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

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

- *About Deep Discovery Inspector on page 1-2*
- *Threat Management Capabilities on page 1-4*
- *Features and Benefits on page 1-3*
- *APT Attack Sequence on page 1-4*
- *Host Severity on page 1-6*
- *Advanced Threat Scan Engine on page 1-9*
- *Virtual Analyzer on page 1-9*
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.

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

What's New

This version of Deep Discovery Inspector updates the hardware platform and offers a range of product enhancements that improve usability and detections.

**TABLE 1-1. Deep Discovery Inspector 3.8 SP1 New Features**

<table>
<thead>
<tr>
<th><strong>KEY FEATURE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated hardware</td>
<td>Deep Discovery Inspector 3.8 SP1 introduces the following new appliances:</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Inspector 510/1100</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Inspector 4100</td>
</tr>
<tr>
<td></td>
<td>An integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller is embedded in each appliance and provides remote update, management, and support functionality.</td>
</tr>
</tbody>
</table>
Introduction

<table>
<thead>
<tr>
<th><strong>Key Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Third-party integration | Deep Discovery Inspector 3.8 SP1 improves threat insight by sharing suspicious object and C&C communication lists with the following third-party products and services:  
  • Check Point Open Platform for Security (OPSEC)  
  • HP TippingPoint Security Management System (SMS)  
  • IBM® Security Network Protection (XGS)  
  • Palo Alto Firewalls                                                                                                                                 |

**Note**  
You must obtain proper licensing for such third-party products and services.

| **Role-based administration** | **Description**  
A new administrator role allows multiple administrator access and management. System event logs now display usage by user to facilitate activity auditing. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host-based report search filters</strong></td>
<td>Administrators can leverage preset <strong>Affected Hosts</strong> search filters and easily create granular reports that focus on desired threat information.</td>
</tr>
<tr>
<td><strong>Threats at a Glance</strong></td>
<td>The new <strong>Threats at a Glance</strong> widget displays actionable information about six key metrics and provides administrators with streamlined access to attack and threat activity on their networks.</td>
</tr>
</tbody>
</table>

**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 1-4**
• *APT Attack Sequence on page 1-4*
• *Host Severity on page 1-6*
• *Advanced Threat Scan Engine on page 1-9*
• *Virtual Analyzer on page 1-9*

**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 1-2. Threat Management Capabilities**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded APT and targeted attack detection</td>
<td>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.</td>
</tr>
<tr>
<td>Visibility, analysis, and action</td>
<td>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.</td>
</tr>
<tr>
<td>High capacity platforms</td>
<td>Deep Discovery Inspector features a high-performance architecture that meets the demanding and diverse capacity requirements of large organizations.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 1-3. APT Attack Sequence**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence Gathering</td>
<td>Identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack</td>
</tr>
<tr>
<td>Point of Entry</td>
<td>An initial compromise typically from zero-day malware delivered via social engineering (email/IM or drive-by download)</td>
</tr>
<tr>
<td></td>
<td>A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.</td>
</tr>
<tr>
<td>Command &amp; Control (C&amp;C)</td>
<td>Communications used throughout an attack to instruct and control the malware used</td>
</tr>
<tr>
<td>Communication</td>
<td>C&amp;C communication allows the attacker to exploit compromised machines, move laterally within the network, and exfiltrate data.</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>An attack that compromises additional machines</td>
</tr>
<tr>
<td></td>
<td>Once inside the network, an attacker can harvest credentials, escalate privilege levels, and maintain persistent control beyond the initial target.</td>
</tr>
<tr>
<td>Asset/Data Discovery</td>
<td>Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest</td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td>Unauthorized data transmission to external locations</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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 1-4. Host Severity Scale**

<table>
<thead>
<tr>
<th>Host Severity</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical</strong></td>
<td>Host shows evidence of compromise including but not limited to the following:</td>
</tr>
<tr>
<td></td>
<td>• Data exfiltration</td>
</tr>
<tr>
<td></td>
<td>• Multiple compromised hosts/servers</td>
</tr>
<tr>
<td>10</td>
<td>9 Host exhibits an indication of compromise from APTs including but not limited to the following:</td>
</tr>
<tr>
<td></td>
<td>• Connection to an IP address associated with a known APT</td>
</tr>
<tr>
<td></td>
<td>• Access to a URL associated with a known APT</td>
</tr>
<tr>
<td></td>
<td>• A downloaded file associated with a known APT</td>
</tr>
<tr>
<td></td>
<td>• Evidence of lateral movement</td>
</tr>
<tr>
<td>8</td>
<td>Host may exhibit the following:</td>
</tr>
<tr>
<td></td>
<td>• A high severity network event</td>
</tr>
<tr>
<td></td>
<td>• Connection to a C&amp;C Server detected by Web Reputation Services</td>
</tr>
<tr>
<td></td>
<td>• A downloaded file rated as high risk by Virtual Analyzer</td>
</tr>
<tr>
<td>Host Severity</td>
<td>Examples</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| **Major**     | Host may exhibit the following:  
|               | Host with inbound malware downloads; no evidence of user infection  
|               | • An inbound Exploit detection |
| 7             | Host may exhibit the following:  
|               | • Connection to a dangerous site detected by Web Reputation Services |
| 6             | Host may exhibit the following:  
|               | • A downloaded medium- or low-risk potentially malicious file with no evidence of user infection |
| 5             | Host may exhibit the following:  
|               | • A medium severity network event  
|               | • A downloaded file rated as medium risk by Virtual Analyzer |
| **Minor**     | 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 |
| 3             | Host may exhibit the following:  
|               | • A low severity network event  
|               | • Evidence of receiving an email message that contains a dangerous URL  
<p>|               | • A downloaded file rated as low risk by Virtual Analyzer |</p>
<table>
<thead>
<tr>
<th><strong>HOST SEVERITY</strong></th>
<th><strong>EXAMPLES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivial</td>
<td>1</td>
</tr>
<tr>
<td>Host exhibits normal behavior that may be benign or indicate a threat in future identification of malicious activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 used to manage and analyze samples submitted by Trend Micro products. Sandbox images allow for observation of file and network behavior in a natural setting without any risk of compromising the network.

Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.

Virtual Analyzer includes the following features:

- Threat execution and evaluation summary
• In-depth tracking of malware actions and system impact, including the following:
  • Network connections initiated
  • System file/registry modification
  • System injection behavior detection
  • Identification of malicious destinations and command-and-control (C&C) servers
  • Exportable forensic reports, PCAP, and OpenIOC files
  • Generation of complete malware intelligence for immediate local protection
  • Generation of suspicious objects list
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 2-8
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.

---

**Procedure**

1. **Add Network Groups**.
   
   For details, see *Adding Network Groups on page 6-79*.

2. **Configure Registered Domains**.

   For details, see *Adding Registered Domains on page 6-81*.

3. **Configure Registered Services**.

   For details, see *Adding Registered Services on page 6-82*.

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

   For details, see *Configuring a Proxy Server on page 6-144*.

5. **Update components**.

   For details, see *Performing Manual Updates on page 6-5*.
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.

![Deep Discovery Inspector Management Console](image)

**Figure 2-1. Deep Discovery Inspector Management Console**

The management console includes the following user interface elements:

<table>
<thead>
<tr>
<th>#</th>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
  - Log Off |
| 2. | Appliance information at a glance        | Appliance information at a glance includes the following:  
  - Time zone  
  - Appliance IP address  
  - Network traffic |
### Management Console Requirements

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

**Table 2-1. Management Console Requirements**

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google™ Chrome™</td>
<td>43.0 or later</td>
</tr>
<tr>
<td>Mozilla™ Firefox™</td>
<td>38.0 or later</td>
</tr>
<tr>
<td>Microsoft™ Internet Explorer™</td>
<td>10.0 and 11.0</td>
</tr>
</tbody>
</table>

Adobe® Flash® Player 8.0 or later is also required to view the management console.

Recommended resolution rate: 1024x768

### 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:
     
     ```
     ```
   
   **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.

7. Change the default password.
   
   See *Management Console Account Passwords on page 2-6.*

8. Set system time.
   
   See *Configuring Time Options on page 6-150.*

   
   See *Activating or Renewing a Product License on page 6-164.*
Management Console Account Passwords

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

The management console accepts passwords that contain the following:

- 6 to 32 characters
- Characters from at least three of the following categories:
  - Uppercase (A-Z)
  - Lowercase (a-z)
  - Numeric (0-9)
  - Special characters: ` ~ ! @ # $ % ^ & * ( ) - _ + = \ { } \ | < > , . / ? : ; '

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

---

Note

To reset a password, see *Resetting an Account Password on page 6-142*

---

Changing an Administrator Account Password

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

---

Tip

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

1. To change an administrator account password, do one of the following:
   - a. On any Deep Discovery Inspector main screen, at the top-right corner, open the drop-down menu under your account name.
   - b. Click Change Password.
   - c. Type the old password.
   - d. Type the new password and confirm it.
   - e. Click Save.
   - a. Go to Administration > Accounts.
   - b. Under the Reset Password column for the target account, click Change Password.
   - c. Type the old password.
   - d. Type the new password and confirm it.
   - e. Click Save.

Deep Discovery Inspector logs off.

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

Changing a Viewer Account Password

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 logs off.

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

---

**Network**

Use the *Network* screen to manage the Deep Discovery Inspector appliance IP address and network interface ports.

Deep Discovery Inspector uses a management port and several data ports. Go to *Administration > System Settings > Network* to do the following:

- View the status of these ports
• Change the network speed and duplex mode for each of the data ports
• Capture packets for debugging and troubleshooting purposes

Network Format Rules

Go to Administration > System Settings > Network.

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

**Table 2-2. Network Setting Format Rules**

<table>
<thead>
<tr>
<th><strong>FORMAT SETTING</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Host Name Format</td>
<td>The host name can contain alphanumeric characters and dashes (&quot;A-Z&quot;, &quot;a-z&quot;, &quot;0-9&quot;, &quot;,&quot;).</td>
</tr>
<tr>
<td>Dynamic IP Address</td>
<td>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 <em>Deep Discovery Inspector 3.8 SP1 Installation and Deployment Guide</em>.</td>
</tr>
</tbody>
</table>
### Static IP Address Format

<table>
<thead>
<tr>
<th>Format Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The IP address cannot be the broadcast or network address.</td>
</tr>
</tbody>
</table>

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]

### Subnet Mask Format

<table>
<thead>
<tr>
<th>Format Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The subnet mask cannot be the broadcast or network address.</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Format Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Prefix Format</td>
<td>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 &quot;prefix&quot;. Use &quot;/N&quot; 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.</td>
</tr>
<tr>
<td>Default Gateway Address Format</td>
<td>The gateway must be in the same subnet as the IP address.</td>
</tr>
<tr>
<td>DNS</td>
<td>IPv4 or IPv6 address</td>
</tr>
</tbody>
</table>

Configuring the Appliance IP Settings

Procedure

1. Go to Administration > System Settings > Network.
2. Specify the **Appliance Host Name**.

3. Configure IP address settings.
   a. Select one of the following:
      - Dynamic IP Address (DHCP)
      - Static IP Address
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**.

4. Specify the following:
   - **IP address**: The numeric address specifically for Deep Discovery Inspector
   - **Subnet Mask**: Indicates the subnet mask for the network that includes the Deep Discovery Inspector IP address
   - **Gateway**: The IP address of the network gateway
   - **DNS Server 1**: The IP address of the primary server that resolves host names to an IP address
   - **DNS Server 2 (optional)**: The IP address of the secondary server that resolves host names to an IP address

5. (Optional) Configure an IPv6 address for the management console.
   a. Select **Enable IPv6 address for management console**.
      
      IPv6 Address Settings options appear.
   b. Specify the following IPv6 address settings:
      - **IPv6 Address**: The alphanumeric address specifically for Deep Discovery Inspector
      - **Subnet Prefix Length**: Indicates the prefix length for the network that includes the Deep Discovery Inspector IP address
      - **Gateway**: The IP address of the network gateway
      - **(Optional) DNS Server**: The IP address of the server that resolves host names to an IP address

6. Click **Save**.
Managing Network Interface Ports

Procedure

1. Go to Administration > System Settings > Network.
2. View the status for each port.
3. To change the port’s network speed and duplex mode, select from Connection Type options.
4. (Optional) If using VLAN tags, select Check VLAN tags to differentiate TCP connections.
5. To capture packets on each port, click Start.
   The date and time of the packet capture session displays next to the button. The total amount of packets captured dynamically displays on the lower section of the screen.

   Note
   Do not run multiple capture sessions. Wait for a session to finish before starting a new one.

6. Click Stop when the packet capture session is done.

   Note
   The maximum size for files containing packet data is 30 MB.

7. Click View.
   The Packet Capture Information window opens.
8. Click Export to export the most recent packet capture data to a log file, and specify the target location of the log file tcpdump.tgz.

   Tip
   Send the network capture file to Trend Micro for troubleshooting assistance.
9. Click **Reset** to remove files containing packet data.
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 3-3
• Widgets on page 3-8
• About Deep Discovery Inspector Widgets on page 3-10
• Deep Discovery Inspector Widgets on page 3-11
• Deep Discovery Inspector Default Widget Tabs on page 3-14
• Optional Widgets on page 3-48
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 3-3
- Widgets on page 3-8
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>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a tab</td>
<td>Click the plus icon at the top of the dashboard. For details, see Adding/Modifying Tabs on page 3-4.</td>
</tr>
<tr>
<td>Edit tab settings</td>
<td>Click Tab Settings. For details, see Adding/Modifying Tabs on page 3-4.</td>
</tr>
<tr>
<td>Move tab</td>
<td>Drag-and-drop to change a tab's position. For details, see Moving Tabs on page 3-6.</td>
</tr>
<tr>
<td>Task</td>
<td>Steps</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Close/delete tab</td>
<td>Default tabs can be closed but not deleted.</td>
</tr>
<tr>
<td></td>
<td>Customized tabs can be deleted but not closed.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deleting a tab deletes all the widgets contained in the tab.</td>
</tr>
<tr>
<td></td>
<td>For details, see <em>Closing/Deleting Tabs on page 3-7</em></td>
</tr>
</tbody>
</table>

### 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.

![New Tab Window](image)

**Figure 3-2. New Tab**

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

![Tab Settings Window]

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

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.

Restoring the Dashboard

Procedure

1. Go to the Dashboard screen.
2. Click the Restore link.
A warning message appears.

![Warning message](image)

**FIGURE 3-3. Dashboard Restore Message**

3. Click **OK**.

Any custom tabs and widgets previously created are removed and the **Dashboard** is restored to its default settings.

---

**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 3-8**.

---

**Widget Tasks**

**TABLE 3-2. Widget Tasks**

<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td>Close a widget and remove it from view.</td>
</tr>
</tbody>
</table>
| Edit    | • Rename a widget.  
          | • Modify display options.  
<pre><code>      | • Modify data options. |
</code></pre>
<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Download a .csv file containing information about widget data.</td>
</tr>
<tr>
<td>Help</td>
<td>View information about a widget, widget data, and configuration or editable options.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Display the latest information on the screen.</td>
</tr>
</tbody>
</table>

**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**.

![Add Widgets](image)

**Figure 3-4. Add Widget**
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**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>This tab contains widgets that display hosts requiring priority attention and other detailed, actionable information. For details, see Summary on page 3-15.</td>
</tr>
<tr>
<td>Threat Monitoring</td>
<td>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 3-21.</td>
</tr>
</tbody>
</table>
### Deep Discovery Inspector Widgets

Deep Discovery Inspector includes the following widgets:

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

Optional, undisplayed widgets may be added to any widget tab. For details, see *Adding Widgets to the Dashboard on page 3-9.*

For widgets that display threat data, see *All Detections - Detection Details - Header on page 4-57* to view a list of displayed threat types.
**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**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts with C&amp;C Callback Attempts</td>
<td>This widget displays hosts with C&amp;C callback attempts, suspicious object matches, and deny list matches.</td>
</tr>
<tr>
<td>Monitored Network Traffic</td>
<td>This widget displays the total size of network traffic across the mirrored switch in real time.</td>
</tr>
<tr>
<td>Threat Geographic Map</td>
<td>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.</td>
</tr>
<tr>
<td>Watch List</td>
<td>This widget displays the origin of malware attempting access to your network and allows you to configure a watch list. The watch list shows the hosts that need constant monitoring.</td>
</tr>
</tbody>
</table>

---

**Table 3-6. Virtual Analyzer Status Widgets**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Hosts with Virtual Analyzer Detections</td>
<td>This widget displays the top affected hosts analyzed by Virtual Analyzer as detection count by IP address, in the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malicious Sites Analyzed by Virtual Analyzer</td>
<td>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.</td>
</tr>
<tr>
<td>Top Suspicious Files</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Analyzer Detections</td>
<td>This widget displays information about suspicious files that pass through other scan engines but are detected by Virtual Analyzer.</td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 3-7. Top Trends Widgets**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Disruptive Applications</td>
<td>This widget displays the most detected disruptive applications within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Exploited Hosts</td>
<td>This widget displays the most detected exploited hosts within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Grayware-infected Hosts</td>
<td>This widget displays the most grayware-infected hosts within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Hosts with Events Detected</td>
<td>This widget displays hosts which triggered the most events within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malicious Content Detected</td>
<td>This widget displays the most detected threats within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malware-infected Hosts</td>
<td>This widget displays the hosts most affected by malware within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Suspicious Behaviors Detected</td>
<td>This widget displays the most detected suspicious behaviors within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malicious URLs Detected</td>
<td>This widget displays the most detected malicious URLs within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
</tbody>
</table>

**Table 3-8. System Status Widgets**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>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%.</td>
</tr>
</tbody>
</table>
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.

For details, see Viewing Device Information and Status in the Deep Discovery Inspector Installation and Deployment Guide.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Usage</td>
<td>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).</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>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. For details, see Viewing Device Information and Status in the Deep Discovery Inspector Installation and Deployment Guide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scanned Traffic</td>
<td>This widget displays total scanned traffic volume for the past 24 hours by HTTP, SMTP, and other traffic, in seconds.</td>
</tr>
<tr>
<td>Malicious Real-time Network Traffic</td>
<td>This widget displays real-time total and malicious traffic volume detected by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in seconds.</td>
</tr>
<tr>
<td>Monitored Network Alerts</td>
<td>This widget displays any host affected by threats within the past 24 hours. A circle represents an affected host and a row represents a monitored network group.</td>
</tr>
<tr>
<td>Real-time Scanned Traffic</td>
<td>This widget displays real-time total traffic volume scanned by Deep Discovery Inspector by HTTP, SMTP, and other traffic, in seconds.</td>
</tr>
</tbody>
</table>

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 3-15*
- *Top Affected Hosts on page 3-17*
- *Threat Summary on page 3-18*
- *Malicious Scanned Network Traffic on page 3-19*
- *Scanned Traffic by Protocol Type on page 3-20*

**Threats at a Glance**

![Threats at a Glance Widget](image)

**FIGURE 3-5. Threats at a Glance Widget**

This widget displays actionable information about six key metrics and links to the corresponding detection logs.
### Table 3-10. Threats at a Glance

<table>
<thead>
<tr>
<th>Metric</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| Potential threats             | All Detections     | • Counts detections  
• Associated with the **Potential Threats** preset search  
Click a value to drill down to the **All Detections** screen. |
| Known threats                 | All Detections     | • Counts detections  
• Associated with the **Known Threats** preset search  
Click a value to drill down to the **All Detections** screen. |
### Email threats

**Source:** 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

**Figure 3-6. Top Affected Hosts Widget**

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 1-6.*
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 **Edit** to filter the types of threats displayed in the graph.
Malicious Scanned Network Traffic

![Malicious Scanned Network Traffic Widget](image.png)

**Figure 3-8. Malicious Scanned Network Traffic Widget**

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**

![Scanned Traffic by Protocol Type](image)

**Figure 3-9. 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:

- **Hosts with C&C Callback Attempts on page 3-21**
- **Monitored Network Traffic on page 3-22**
- **Threat Geographic Map on page 3-22**
- **Watch List on page 3-25**

**Hosts with C&C Callback Attempts**

![Figure 3-10. Hosts with C&C Callback Attempts Widget](image)

This widget displays all hosts with C&C callbacks detected by network scanning, Deny List matches, and Virtual Analyzer detections.

Viewing hosts with C&C callbacks in 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, isolating computers according to IP address) in order to prevent malicious operations from affecting hosts.

Click the number for each detected callback type to view detailed information about the hosts and the callbacks.
Monitored Network Traffic

![Monitored Network Traffic Widget](image)

**Figure 3-11. Monitored Network Traffic Widget**

This widget displays total traffic monitored by Deep Discovery Inspector, 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.

**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 concentric red circle.

**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.
4. Click any threat in the pop-up window.
   A table appears with details about a specific data point.

5. Click the total number of threats located at the bottom of the pop-up window.
   A table populated with details about all threats (related to the indicated threat and
   the country or city selected) appears.

---

**Note**

The right pane displays information about affected hosts organized by country.

6. Click any country in the list to display relevant information.

7. Click **View Cities** in the pop-up window.

8. City-specific information is generated.

9. Click **View Countries** in the pop-up to return to the country list.
Watch List

![Image of Watch List widget]

Figure 3-13. Watch List Widget

The widget’s left pane contains two tabs: Watch List and High Risk Hosts. Each tab contains a list of hosts. Click a host in either tab to investigate the threats on that host. For details, see Investigating Threats on page 3-27.

Viewing High Risk Host Data

The High Risk Hosts tab shows all high risk hosts, in the last 7 days, and can be sorted by IP address, hostname, event total, and last detected event time.

Procedure

1. Click the icon beside a host to view high risk host data.
Adding Hosts to the Watch List

If a host requires additional monitoring add it to the **Watch List** tab.

Procedure

1. Type the host’s full IP address in the search text box (a partial IP address is not accepted).
A field containing the IP address appears.

![Watch List](image)

**Figure 3-15. Adding Hosts to the Watch List**

2. In the IP address *(Configuration)* field, type a note for that host and click *Save & Watch*.

   The note is saved and the host is added to the *Watch List*.

----------

**Investigating Threats**

**Procedure**

1. Go to either the *Watch List* or *High Risk Hosts* tab and click the host to investigate.

   The time-series line graph to the right plot is populated with the threat count on that host by threat type and for a particular time period (past 24 hours, 7 days, and 30 days).
Threat types include known malicious content, malicious behavior, suspicious behavior, exploit, and grayware. For known malware and exploits, all detections are counted in the graph. For malicious behavior, suspicious behavior, and grayware, only those that are considered high risk are displayed in the graph.

If you select **Past 24 hours** and the current time is 4:15 pm, the graph shows the threat count for each threat type from 5:00pm of the previous day to 4:00pm of the current day.

2. Click a data point in the graph.

The **Detection** screen with detailed threat information opens.

### Editing the Watch List

**Procedure**

1. Sort the **Watch List** by desired criteria.

2. Click the icon for the host to edit.

3. Edit the note for this host and click **Save & Watch**.

The note is saved and the host is added to the **Watch List**.
4. To remove hosts from the Watch List, click the icon and select **Remove**.

---

**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 3-30*
- *Top Malicious Sites Analyzed by Virtual Analyzer on page 3-31*
- *Top Suspicious Files on page 3-32*
- *Virtual Analyzer Detections on page 3-33*
- *Using the Virtual Analyzer Widget on page 3-35*

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 as detection count by IP address.

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 **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**

![Top Malicious Sites Analyzed by Virtual Analyzer](image)

**Figure 3-18. Top Malicious Sites Analyzed by Virtual Analyzer Widget**

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/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 chart. Click any cell to obtain additional details about the site.

**Top Suspicious Files**

**FIGURE 3-19. Top Suspicious Files Widget**

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

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

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).

**Virtual Analyzer Detections**

This widget displays information about suspicious files detected by Virtual Analyzer.

![Virtual Analyzer Detections](image)

**FIGURE 3-20. Virtual Analyzer Detections**

Use this widget to:

- Discover unknown threats (not detected by signature-based technology)
• Find potentially compromised hosts using detection information
• Download file samples for further analysis

The widget also allows you to perform the following actions:

• Configure the following settings:
  • Chart type: Display information in table, bar, or pie chart format.
  • Title: Modify the widget name.
  • Display: Specify the number of values to display (Top 5, 10, 20).
• Export information to a .csv file.

By default, the widget displays a table chart with the following information for each detected file:

• File name or SHA-1
• Number of detections
• Number of affected hosts
• Name of associated malware
• Severity level
Using the Virtual Analyzer Widget

![Virtual Analyzer Widget](image)

**FIGURE 3-21. Virtual Analyzer Widget**

**Procedure**

1. Select a time period *(Past 1 hour, Past 24 hours, Past 7 days, Past 30 days)*.

2. Hover over a section of the chart to view the percentage of Malicious or Not Malicious analyzed files.

3. View Virtual Analyzer status on the left pane.
   - For Virtual Analyzer:
     - Analysis Module: Internal
     - Virtual Analyzer Status: Enabled

---

**Note**

Virtual Analyzer must be enabled in order to view results.
• Last file analyzed: last scanned file name or SHA-1
• Last file analysis date:
• # of files to be analyzed:
• Average files count per hour:
• Cache hit rate:

• For Deep Discovery Analyzer and Deep Discovery Advisor:
  • 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:
  • Cache hit rate:

---

**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 3-37*
• *Top Exploited Hosts on page 3-38*
• *Top Grayware-infected Hosts on page 3-39*
• *Top Hosts with Events Detected on page 3-40*
Top Disruptive Applications

**Figure 3-22. Top Disruptive Applications Widget**
This widget displays disruptive applications within the past 1 hour, 24 hours, 7 days, or 30 days. Clicking on a table cell provides additional details.

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 Exploited Hosts

![Top Exploited Hosts Widget](image)

**FIGURE 3-23. Top Exploited Hosts Widget**

This widget shows which hosts on your network(s) 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 bar graph relating the IP addresses of the top exploited hosts and total detections.

Mouse over an area on the graph to see the exact number of exploits on a host. Clicking this point will open a detection list with details about the type and severity of a threat, the hostname, the timestamps, and the total detected exploits.

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

![Top Grayware-infected Hosts Widget](image)

**Figure 3-24. Top Grayware-infected Hosts Widget**

This widget displays the most detected grayware on your network(s) 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 pie chart. Mouseover an area to see the name of the top grayware-infected hosts. Clicking
this point opens a detection list with details about the date, type, source/destination IP, protocol, direction or file name.

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 Hosts with Events Detected**

![Top Hosts with Events Detected Widget](image)

**FIGURE 3-25. Top Hosts with Events Detected Widget**
This widget displays events affecting hosts within the past 1 hour, 24 hours, 7 days, or 30 days. By default, all events within the selected time frame are shown in a bar graph relating the IP addresses of the top exploited hosts and total detections.

Mouseover an area on the graph to see the exact number of hosts with events detected. Clicking this point opens a detection list with details about the severity and type of threat, the hostname, the timestamps, and the total detections.

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

![Top Malicious Content Detected Widget](image)

**Figure 3-26. Top Malicious Content Detected Widget**

This widget displays the most-detected known malware on your network(s) 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 pie chart. Mouseover an area to see the name of the malware detected on a host. Clicking the malware name opens a detection list with details about the date, type, source/destination IP, protocol, direction or file name.
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**

![Top Malware-infected Hosts Widget](image)

**Figure 3-27. Top Malware-infected Hosts Widget**

This widget displays the most malware-infected hosts on your network(s) 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 bar graph relating the IP addresses of the infected hosts and total detections.

Mouseover an area on the graph to see the exact number of malware-infected hosts. Clicking this point opens a detection list with details about the type and severity of a threat, the hostname, the timestamps, and the total detected infections.

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**

![Top Suspicious Behaviors Detected Widget](image)

**Figure 3-28. Top Suspicious Behaviors Detected Widget**

This widget displays the most detected suspicious behavior on your network(s) 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 bar graph relating the IP addresses of the top suspicious behaviors and total detections. Mouseover an area on the graph to see the exact number of exploits on a host. Clicking this point will open a detection list with details about the type and severity of a threat, the hostname, the timestamps, and the total detected exploits.

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).

**Top Malicious URLs Detected**

![Figure 3-29. Top Malicious URLs Detected Widget](image-url)
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 relating URL and total detections. Clicking any data point opens a detection list with details about the threat, timestamp, source/destination IP, and the malicious URL hostname.

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 3-46**
- **Disk Usage on page 3-47**
- **Memory Usage on page 3-48**

**CPU Usage**

![CPU Usage Widget](image)

**FIGURE 3-30. CPU Usage Widget**

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

**Figure 3-31. Disk Usage Widget**

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 3.8 SP1, but may be added to any widget tab.

- *All Scanned Traffic on page 3-49*
- *Malicious Real-time Network Traffic on page 3-50*
- *Monitored Network Alerts on page 3-51*
- *Real-time Scanned Traffic on page 3-51*
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

**Figure 3-33. All Scanned Traffic Widget**
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.
Monitored Network Alerts

![Monitored Network Alerts Widget](image1.png)

**Figure 3-35. Monitored Network Alerts Widget**

This widget displays all threats affecting network hosts within a 24-hour period as a circle, grouped within its network. The size of the circle represents the total number of threats. Hovering over a circle displays recent threat events. High-risk hosts are highlighted in red.

Clicking a circle displays a pop-up with additional threat information for either the past 24 hours or 30 days. Threat totals are shown for: Malicious Content, Malicious Behaviors, Suspicious Behaviors, Exploits, Grayware, along with Malicious URLs and Disruptive Applications (if selected).

Real-time Scanned Traffic

![Real-time Scanned Traffic Widget](image2.png)

**Figure 3-36. Real-time Scanned Traffic Widget**
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.
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*
- *Hosts with Notable Event Detections on page 4-39*
- *C&C Callback Addresses on page 4-42*
- *Suspicious Objects on page 4-43*
- *Retro Scan on page 4-45*
- *All Detections on page 4-50*
About the Detections Screen

The Detections tab provides access to realtime information about the following detection categories.

TABLE 4-1. Deep Discovery Inspector Detections

<table>
<thead>
<tr>
<th>DETECTION CATEGORIES</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected Hosts</td>
<td>Hosts that have been involved in one or more phases of a targeted attack&lt;br&gt;For details, see <em>Affected Hosts on page 4-3.</em>&lt;br&gt;For details about the Host Severity scale, see <em>Host Severity on page 1-6.</em></td>
</tr>
<tr>
<td>Hosts with Notable Event Detections</td>
<td>Hosts with C&amp;C callback attempts, suspicious object matches, and deny list matches&lt;br&gt;For details, see <em>Hosts with Notable Event Detections on page 4-3.</em></td>
</tr>
</tbody>
</table>
### Detection Categories

<table>
<thead>
<tr>
<th>Detection Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C Callback Addresses</td>
<td>Hosts with C&amp;C callback attempts to known C&amp;C addresses For details, see <em>C&amp;C Callback Addresses on page 4-42.</em></td>
</tr>
<tr>
<td>Suspicious Objects</td>
<td>Hosts with suspicious objects identified by Virtual Analyzer or synchronized from an external source For details, see <em>Suspicious Objects on page 4-43.</em></td>
</tr>
<tr>
<td>Retro Scan</td>
<td>A cloud-based service that scans historical web access logs for callback attempts to C&amp;C servers and other related activities in your network For details, see <em>Retro Scan on page 4-45.</em></td>
</tr>
<tr>
<td>All Detections</td>
<td>Hosts with detections from all event logs, including global intelligence, user-defined lists, and other sources For details, see <em>All Detections on page 4-50.</em></td>
</tr>
</tbody>
</table>

### 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 1-6.*

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 **Interested IP** and **Interested 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 4-2. Display Options and Search Filters: Affected Hosts

<table>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection severity</td>
<td>Filter options include the following detection severity settings:</td>
</tr>
<tr>
<td>High only</td>
<td>Displays High severity detections only</td>
</tr>
<tr>
<td></td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>Displays High and medium severity detections</td>
</tr>
<tr>
<td></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>Displays High, medium, and low severity detections</td>
</tr>
<tr>
<td></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
<tr>
<td>All</td>
<td>Displays All detections, including informational detections</td>
</tr>
<tr>
<td></td>
<td><img src="image4.png" alt="Image" /></td>
</tr>
<tr>
<td>Period</td>
<td>Past 1 hour</td>
</tr>
<tr>
<td></td>
<td>Past 24 hours (default)</td>
</tr>
<tr>
<td></td>
<td>Past 7 days</td>
</tr>
<tr>
<td></td>
<td>Past 30 days</td>
</tr>
<tr>
<td></td>
<td>Custom range</td>
</tr>
<tr>
<td></td>
<td>Specify a custom range from the current day to the past 31 days.</td>
</tr>
<tr>
<td><strong>FILTER OPTIONS</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Customize Columns</td>
<td>Display optional columns.</td>
</tr>
<tr>
<td><strong>Basic Search</strong></td>
<td>Search an IP address or host name.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Type a case-insensitive keyword in the basic search field to search a partial host match.</td>
</tr>
<tr>
<td><strong>Preset Search Filters</strong></td>
<td>Search by preset search criteria.</td>
</tr>
<tr>
<td>• Affected Hosts view includes the following preset searches:</td>
<td></td>
</tr>
<tr>
<td>• Hosts with Targeted Attack detections</td>
<td></td>
</tr>
<tr>
<td>• Hosts with C&amp;C Communications detections</td>
<td></td>
</tr>
<tr>
<td>• Hosts with Lateral Movement detections</td>
<td></td>
</tr>
<tr>
<td>• Affected Hosts - Host Details view includes the following preset searches:</td>
<td></td>
</tr>
<tr>
<td>• Threats</td>
<td></td>
</tr>
<tr>
<td>• Known Threats</td>
<td></td>
</tr>
<tr>
<td>• Potential Threats</td>
<td></td>
</tr>
<tr>
<td>• Ransomware</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Search Filter</strong></td>
<td>Search by user-defined criteria sets.</td>
</tr>
<tr>
<td></td>
<td>Each set includes one or more of the following:</td>
</tr>
<tr>
<td>• Attributes</td>
<td></td>
</tr>
<tr>
<td>• Operators</td>
<td></td>
</tr>
<tr>
<td>• Associated values</td>
<td></td>
</tr>
<tr>
<td>For details, see <em>Affected Hosts Advanced Search Filter on page 4-23.</em></td>
<td></td>
</tr>
</tbody>
</table>
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 to select optional columns for display and click Apply to return to the modified Affected Hosts screen.
**Figure 4-3. Customize Columns**

**Table 4-3. Host Information Columns**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Preselected</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>X</td>
<td>IP address of the affected host</td>
</tr>
<tr>
<td>Host Name</td>
<td>X</td>
<td>Computer name of the host</td>
</tr>
<tr>
<td>MAC Address</td>
<td></td>
<td>Media Access Control address of a network node</td>
</tr>
<tr>
<td>Network Group</td>
<td>X</td>
<td>Network group that an IP address/host is assigned</td>
</tr>
<tr>
<td>Host Severity</td>
<td>X</td>
<td>Highest impact on a host determined from aggregated detections by Trend Micro products and services. For details about the Host Severity scale, see <em>Host Severity on page 1-6</em>.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>X</td>
<td>Most recent detection, based on timestamp</td>
</tr>
</tbody>
</table>
Note

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

### TABLE 4-4. Notable Statistics Columns

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Attack</td>
<td></td>
<td>A threat that aims to exfiltrate data from a target system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>APT Attack Sequence on page 1-4</em></td>
</tr>
</tbody>
</table>

### TABLE 4-5. Attack Phase Columns

<table>
<thead>
<tr>
<th>COLUMNS</th>
<th>PRESELECTED</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence Gathering</td>
<td>X</td>
<td>Attackers identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack.</td>
</tr>
<tr>
<td>Point of Entry</td>
<td>X</td>
<td>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.</td>
</tr>
<tr>
<td>C&amp;C Communication</td>
<td>X</td>
<td>C&amp;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.</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>X</td>
<td>Once inside the network, an attacker compromises additional machines to harvest credentials, escalate privilege levels, and maintain persistent control.</td>
</tr>
</tbody>
</table>
### Columns

<table>
<thead>
<tr>
<th>Asset/Data Discovery</th>
<th>X</th>
<th>Several techniques (such as port scanning) are used to identify the noteworthy servers and the services that house the data of interest.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Exfiltration</td>
<td>X</td>
<td>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.</td>
</tr>
<tr>
<td>Unknown Attack Phase</td>
<td>X</td>
<td>Detection is triggered by a rule that is not associated with an attack phase.</td>
</tr>
</tbody>
</table>

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 **Interested IP** and **Interested Host Name**.

6. To run a saved search, go to **Detections > Affected Hosts**, open the **Saved Searches** drop-down menu, and click a saved search.
Deep Discovery Inspector provides the following preset saved search filters.

**TABLE 4-6. Preset Search Filters**

<table>
<thead>
<tr>
<th>PRESET FILTER</th>
<th>FILTER OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts with Targeted Attack detections</td>
<td>Notable events in Targeted Attack</td>
</tr>
<tr>
<td>Hosts with C&amp;C Communication detections</td>
<td>Notable events in C&amp;C Communication</td>
</tr>
<tr>
<td>Hosts with Lateral Movement detections</td>
<td>Notable events in Lateral Movement</td>
</tr>
</tbody>
</table>

7. To create and apply an advanced search filter, click **Advanced**.
   
   For details, see *Affected Hosts Advanced Search Filter on page 4-23*.

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.

![Host Details: 10.1.152.26](image)

**Figure 4-4. 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 then click Apply to return to the modified Affected Hosts screen.

**Table 4-7. Affected Hosts - Host Details Columns**

<table>
<thead>
<tr>
<th>Columns</th>
<th>Preselected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>X</td>
</tr>
<tr>
<td>Timestamp</td>
<td>X</td>
</tr>
<tr>
<td>Source Host</td>
<td></td>
</tr>
<tr>
<td>Destination Host</td>
<td></td>
</tr>
<tr>
<td>Interested Host</td>
<td></td>
</tr>
<tr>
<td>Peer Host</td>
<td>X</td>
</tr>
<tr>
<td><strong>Columns</strong></td>
<td><strong>Preselected</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Sender</td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td></td>
</tr>
<tr>
<td>Email Subject</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Detection Name</td>
<td>X</td>
</tr>
<tr>
<td>Detection Type</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>X</td>
</tr>
<tr>
<td>Detection Severity</td>
<td>X</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>X</td>
</tr>
<tr>
<td>Direction</td>
<td>X</td>
</tr>
<tr>
<td>Notable Object</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note**

The default Timestamp and Detection Name 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 Saved Searches drop-down menu, and click a saved search.
Deep Discovery Inspector provides the following preset saved search filters on the Affected Host - Host Details screen.

**TABLE 4-8. Preset Search Filters**

<table>
<thead>
<tr>
<th>Preset Filter</th>
<th>Filter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td>Known Threats</td>
<td>File Detection Types: Known Malware</td>
</tr>
<tr>
<td>Potential Threats</td>
<td>• Virtual Analyzer Result: Has analysis results</td>
</tr>
<tr>
<td></td>
<td>• File Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Detection name options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Ransomware-related detections</td>
</tr>
</tbody>
</table>

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

For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-30.*

11. Click **Export**.

A zip folder with the following files downloads:

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

- Affected Hosts - Detection Details - Header on page 4-17
- Affected Hosts - Detection Details - Connection Details on page 4-18
- Affected Hosts - Detection Details - File Analysis Results on page 4-20

Affected Hosts - Detection Details - Header

The following information is provided in the header at the top of the Detections Details window:

- Detection Name: Detection name
  
  For details about the threat, click the detection name.

  Deep Discovery Inspector connects with Threat Connect, where you can search for current information about the threat.

- Severity: Detection severity

- Type: Detection type

- Description: Description of detection type

Table 4-9. Detection Types

<table>
<thead>
<tr>
<th>Detection Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlated Incident</td>
<td>Events/detections that occur in a sequence or reach a threshold and define a pattern of activity</td>
</tr>
<tr>
<td>Detection Types</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 |
| 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 Details**

Based on search criteria, **Connection Details** may include the following:

- Detection direction
- Host details
- Protocol details
• File details
• Additional event details

A graphical display includes the direction of the event and other information depending on the detection event search criteria.

Host details may include the following:
• IP Address
• Port
• MAC Address
• Network Group
• Network Zone

<table>
<thead>
<tr>
<th>TABLE 4-10. Protocol Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAME</strong></td>
</tr>
<tr>
<td>Channel name</td>
</tr>
<tr>
<td>Message ID</td>
</tr>
<tr>
<td>Recipient</td>
</tr>
<tr>
<td>Sender</td>
</tr>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>Target share</td>
</tr>
<tr>
<td>User agent</td>
</tr>
<tr>
<td>User name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 4-11. File Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAME</strong></td>
</tr>
<tr>
<td>File name</td>
</tr>
</tbody>
</table>
## Additional Event Details

<table>
<thead>
<tr>
<th>Event Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Phase</td>
<td>Identifies the attack phase</td>
</tr>
<tr>
<td>Authentication</td>
<td>Indicates if the protocol requires authentication</td>
</tr>
<tr>
<td>BOT command</td>
<td>Command used in IRC for BOTs</td>
</tr>
<tr>
<td>BOT URL</td>
<td>URL used in IRC for BOTs</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the engine that detected the threat (Network Content Inspection Engine, Advanced Threat Scan Engine, Network Content Correlation Engine, and/or URL Filtering Engine)</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>Defined in Network Content Correlation Pattern, used by the Network Content Correlation Engine</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Indicates if any mitigation action is needed</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used by the threat traffic</td>
</tr>
<tr>
<td>Outbreak Containment Services</td>
<td>Indicates if containment services are needed when an outbreak is detected</td>
</tr>
<tr>
<td>URL</td>
<td>Link included in the email or instant message content</td>
</tr>
</tbody>
</table>

### Affected Hosts - Detection Details - File Analysis Results

Based on search criteria, **File Analysis Results** may include the following:

- File Name
- File Size
• File Type
• MD5
• Parent File
• Risk Level
• SHA-1
• Threat
• Virtual Analyzer Images

**TABLE 4-13. File Analysis Results Tabs**

<table>
<thead>
<tr>
<th><strong>Tab Title</strong></th>
<th><strong>Columns</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Behavior by Category</td>
<td>Displays one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No threat behavior detected</td>
</tr>
<tr>
<td></td>
<td>• Name of threat behavior</td>
</tr>
<tr>
<td>Threat Events by Sequence</td>
<td>Displays any of the following:</td>
</tr>
<tr>
<td></td>
<td>• PID</td>
</tr>
<tr>
<td></td>
<td>• Parent PID</td>
</tr>
<tr>
<td></td>
<td>• Action</td>
</tr>
<tr>
<td></td>
<td>• Detail Information</td>
</tr>
<tr>
<td>Network Traffic</td>
<td>Displays any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Remote Host</td>
</tr>
<tr>
<td></td>
<td>• Protocol</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Requests</td>
</tr>
</tbody>
</table>

The following information is available for download:

• Parent File
• Raw Analysis Data
• Report

Viewing Affected Hosts - Detection Details

Procedure

1. To display Affected Hosts detection details, click any detection link associated with an affected host.

   Details about the host are displayed.

2. To view detection details for a host event, click Show under the Details column.

3. On the Detection Details window, do the following:
   a. Click the detection name for details about the threat.

      Deep Discovery Inspector connects with Threat Connect, where you can search for current information about the threat.

      
      Note
      To access Threat Connect, an internet connection is required.

   b. View the detection severity.

   c. View the detection type.

      For details, see Affected Hosts - Detection Details - Header on page 4-17.

4. Click Export Connection Details to open or save the results.

5. Click Connection Details to view the direction of the event and host, file, and additional event details.

   For details, see Affected Hosts - Detection Details - Connection Details on page 4-18.

6. Click Download Detected File to export the connection details log.

7. For detection events from Virtual Analyzer, click File Analysis Results.
For details, see Affected Hosts - Detection Details - File Analysis Results on page 4-20.

a. Select a parent file from the Select File dropdown menu.
b. (Optional) Click Download Parent File.
c. (Optional) Click Download Raw Analysis Data.
d. (Optional) Click Download Report.
e. Click the Threat Behaviours by Category tab to view event categories.
f. Click the Remote Host tab to view PID, Parent PID, Action, and Detail Information data.
g. Click the Network Traffic tab to view Remote Host, Protocol, Port, and Requests data.

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 4-24.

- Affected Hosts - Host Details view
  For details, see About Affected Hosts - Host Details Advanced Search Filter on page 4-30.

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 20 advanced search filters.
About Affected Hosts Advanced Search Filter

![Figure 4-5. Affected Hosts Advanced Search Filter](image)

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

**Table 4-14. Search Filter Criteria: Affected Hosts**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP address</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>MAC address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td>Notable Events</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Targeted Attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered Services</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Active Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication Servers - Kerberos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Content Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Database Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Domain Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTP Proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Audit Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMTP Open Relay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Software Update Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Server</td>
</tr>
</tbody>
</table>

For details, see *Adding an Affected Hosts Advanced Search Filter on page 4-25* and *Editing an Affected Hosts Saved Search on page 4-27.*

### 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 4-24.*

---

**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

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.

![Advanced search (Unsaved)](image)

**Figure 4-6. Saving an Affected Hosts Search**

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 **edit** 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.
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.

     ![Saved Searches window](image)

     **Figure 4-7. Saving an Affected Hosts Search**

     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

Attention
Deleting a saved search will also permanently delete any scheduled reports 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.

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 4-15. Search Filter Criteria: Affected Hosts - Host Details**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP address</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>MAC address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered Services</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Active Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Authentication Servers - Kerberos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Content Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Database Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Domain Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- File Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- FTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HTTP Proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Audit Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SMTP Open Relay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software Update Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Server</td>
</tr>
<tr>
<td>Protocol</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- All protocol types</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Desired protocol type(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Other</td>
</tr>
<tr>
<td>Direction</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Internal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- External</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resolved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unresolved</td>
</tr>
<tr>
<td>Detection Name</td>
<td>Contains/Does not contain Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Correlation Rule ID (ICID)</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Type</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruptive Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Correlated Incident</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intelligence Gathering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Point of Entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset/Data Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Exfiltration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown Attack Phase</td>
</tr>
<tr>
<td>C&amp;C List Source</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Global Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User-defined</td>
</tr>
<tr>
<td>Virtual Analyzer Result</td>
<td>Has analysis results/No analysis results</td>
<td></td>
</tr>
<tr>
<td>Is Targeted Attack Related</td>
<td>Yes/No</td>
<td></td>
</tr>
<tr>
<td>File Detection Type</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Known Malware</td>
</tr>
<tr>
<td>File Name</td>
<td>Has file name/No file name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
### Attribute, Operator, Action Table

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File SHA-1</td>
<td>Has file SHA-1/No file SHA-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP Address/Domain/URL</td>
<td>Has network object/No network object</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Address</td>
<td>Has email address/No email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Message ID (Email)</td>
<td>Has message ID/No message ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Subject (Email)</td>
<td>Has subject/No subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>

For details, see Adding an Affected Hosts - Host Details Advanced Search Filter on page 4-34 and Editing an Affected Hosts - Host Details Saved Search on page 4-36.

### 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 4-24.*

---

**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 20 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.

![Saved Searches](image)

**Figure 4-9. Saving an Affected Hosts Search**

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 4-24.*
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 20 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.

  ![Advanced search (Unsaved)](image)

  **Figure 4-10. Saving an Affected Hosts Search**

  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.
Hosts with Notable Event Detections

The **Hosts with Notable Event Detections** screen displays hosts with C&C callback attempts, suspicious object matches, and deny list matches.

**Table 4-16. Hosts with Notable Event Detections Tabs**

<table>
<thead>
<tr>
<th>Tabs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C Callback Attempts</td>
<td>Information about hosts with C&amp;C callback attempts from scan engine patterns and rule matches</td>
</tr>
<tr>
<td>Deny List</td>
<td>Detections from Deny List matches</td>
</tr>
</tbody>
</table>
TABLES

| **Suspicious Objects** | Information about hosts with suspicious objects detections that are identified by Virtual Analyzer or synchronized from an external source |

**Viewing C&C Callback Attempts**

**Procedure**

1. Go to **Detections > Hosts with Notable Event Detections > C&C Callback Attempts**.

2. (Optional) Type an IP address or host name in the search text box, and click the **Search** icon.

3. Select a time period.

4. To view detection details for a host, click any detection link.

5. To view detection details for an event, click **Show** under the **Detail** column.
6. To export a displayed list, click Export.

---

Viewing Deny List Detections

Procedure

1. Go to Detections > Hosts with Notable Event Detections > Deny List.
2. (Optional) Type an IP address or host name in the search text box, and click the Search icon.
3. Select a time period.
4. To view detection details for a host, click any detection link.
5. To view detection details for an event, click a detection link under the Total Detections or Unresolved Detections columns.
6. To export a displayed list, click Export.

---

Viewing Suspicious Objects

Procedure

1. Go to Detections > Hosts with Notable Event Detections > Suspicious Objects.
2. (Optional) Type an IP address or host name in the search text box, and click the Search icon.
3. Select a time period.
4. To view detection details for a host, click any detection link.
5. To view detection details for an event, click a detection link under the Total Detections or Unresolved Detections columns.
6. To export a displayed list, click Export.
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**, **Severity**, **Type**, **Latest Callback**, and **Callbacks**.

**Figure 4-11. C&C Callback Addresses**

### Viewing C&C Callback Addresses

**Procedure**

1. Go to **Detections > C&C Callback Addresses**.
2. Click **View** and select one of the following detection types:
   - All
   - IP Addresses/Domains
3. (Optional) Move 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**.

4. To delete any detection, select the item and click **Delete**.

5. (Optional) To sort the list of C&C callback addresses, click the column titles.
   - **Callback Address**: Ascending/descending alphanumeric
   - **Severity**: Ascending/descending alphabetical
   - **Type**: Ascending/descending alphabetical
   - **Latest Callback**: Earliest/latest date
   - **Callbacks**: Ascending/descending numerical

---

**Suspicious Objects**

The **Suspicious Objects** screen displays a list of suspicious files, IP addresses, URLs, and domains identified by Virtual Analyzer or synchronized from an external source.
Suspicious objects can be sorted by **Suspicious Objects, Risk, Type, and Expiration Date**.

**Figure 4-12. Suspicious Objects**

**Viewing Suspicious Objects**

**Procedure**

1. Go to **Detections > Suspicious Objects**.
2. Click **View** and select one of the following detection types:
   - **All**
   - **Files**
   - **IP Addresses**
   - **URLs**
   - **Domains**
3. (Optional) Move an object to the Deny List or the Allow List.
Detections

a. Select a suspicious object detection.
b. Click either Move to Deny List or Move to Allow List.

4. To delete any detection, select the item and click Delete.
5. After deleting a detection, click Reload to apply updates.
6. To sort the list of suspicious objects, click the column titles.

- **Suspicious Objects**: Ascending/descending alphanumeric
- **Risk**: Ascending/descending alphabetical
- **Type**: Ascending/descending alphabetical
- **Expiration Date**: Earliest/latest date

---

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.

![Web Reputation](image)

**Figure 4-13. Web Reputation**

2. Click Enable Web Reputation.


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

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Generated</td>
<td>Date and time the scan report was completed</td>
</tr>
<tr>
<td>Compromised Hosts</td>
<td>Number of hosts that attempted to connect to C&amp;C callback addresses during the scan period</td>
</tr>
<tr>
<td>Callback Attempts</td>
<td>Number of C&amp;C callback attempts found in the logs during the scan period</td>
</tr>
</tbody>
</table>

---

**Note**

Click the number to display the details for a specific report. For details, see **Retro Scan Report Details Screen on page 4-49**.

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

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Callback Attempted</strong></td>
<td>Date and time of each C&amp;C callback attempt</td>
</tr>
<tr>
<td><strong>Monitored Network Group</strong></td>
<td>Monitored network group to which the compromised host belongs</td>
</tr>
<tr>
<td><strong>Compromised Hosts</strong></td>
<td>Name of the compromised host</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address of the compromised host</td>
</tr>
<tr>
<td><strong>Callback Address</strong></td>
<td>URL or IP address of the C&amp;C server</td>
</tr>
<tr>
<td><strong>Related Malware Families</strong></td>
<td>Malware families associated with the C&amp;C callback address</td>
</tr>
<tr>
<td><strong>Related Attacker Groups</strong></td>
<td>Attacker groups associated with the C&amp;C callback address</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter by Severity</td>
<td>Filter options include the following severity settings:</td>
</tr>
<tr>
<td>High only</td>
<td>Displays High severity detections only</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="High severity detections" /></td>
</tr>
<tr>
<td></td>
<td>Displays High and medium severity detections</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="High and medium severity detections" /></td>
</tr>
<tr>
<td></td>
<td>Displays High, medium, and low severity detections</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="High, medium, and low severity detections" /></td>
</tr>
<tr>
<td>All</td>
<td>Displays All detections, including informational detections</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="All detections" /></td>
</tr>
<tr>
<td><strong>FILTER OPTIONS</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Period</strong></td>
<td></td>
</tr>
<tr>
<td>Past 1 hour</td>
<td></td>
</tr>
<tr>
<td>Past 24 hours</td>
<td>(default)</td>
</tr>
<tr>
<td>Past 7 days</td>
<td></td>
</tr>
<tr>
<td>Past 30 days</td>
<td></td>
</tr>
<tr>
<td><strong>Custom Range</strong></td>
<td></td>
</tr>
<tr>
<td>Specify a custom range from the current day to the past 31 days.</td>
<td></td>
</tr>
<tr>
<td><strong>Customize Columns</strong></td>
<td>Display optional columns.</td>
</tr>
<tr>
<td><strong>Basic Search</strong></td>
<td>Search an IP address or host name.</td>
</tr>
<tr>
<td><strong>Preset Search Filters</strong></td>
<td>Search by preset search criteria.</td>
</tr>
<tr>
<td>All Detections view includes the following preset searches:</td>
<td></td>
</tr>
<tr>
<td>• Threats</td>
<td></td>
</tr>
<tr>
<td>• Known Threats</td>
<td></td>
</tr>
<tr>
<td>• Potential Threats</td>
<td></td>
</tr>
<tr>
<td>• Email Threats</td>
<td></td>
</tr>
<tr>
<td>• Ransomware</td>
<td></td>
</tr>
</tbody>
</table>
**Detections**

<table>
<thead>
<tr>
<th><strong>FILTER OPTIONS</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Search Filter</td>
<td>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 <em>All Detections Advanced Search Filter on page 4-63.</em></td>
</tr>
</tbody>
</table>

**Viewing All Detections**

**Procedure**

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

![All Detections](image)

**FIGURE 4-14. 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** then click **Apply** to return to the modified **All Detections** screen.

**Table 4-18. All Detections Columns**

<table>
<thead>
<tr>
<th>Columns</th>
<th>Preselected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>X</td>
</tr>
<tr>
<td>Timestamp</td>
<td>X</td>
</tr>
<tr>
<td>Source Host</td>
<td>X</td>
</tr>
<tr>
<td>Destination Host</td>
<td>X</td>
</tr>
<tr>
<td>Interested Host</td>
<td>X</td>
</tr>
<tr>
<td>Peer Host</td>
<td></td>
</tr>
<tr>
<td>Sender</td>
<td></td>
</tr>
<tr>
<td>Recipients</td>
<td></td>
</tr>
<tr>
<td>Email Subject</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Detection Name</td>
<td>X</td>
</tr>
<tr>
<td>Detection Type</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>X</td>
</tr>
<tr>
<td>Detection Severity</td>
<td>X</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>X</td>
</tr>
<tr>
<td>Direction</td>
<td></td>
</tr>
<tr>
<td>Notable Object</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note**

The default **Timestamp** and **Detection Name** columns cannot be removed.
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 4-15. All Detections Basic Search**

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

Deep Discovery Inspector provides the following preset saved search filters.
TABLE 4-19. Preset Search Filters

<table>
<thead>
<tr>
<th>Preset Filter</th>
<th>Filter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td>Known Threats</td>
<td>File Detection Types: Known Malware</td>
</tr>
<tr>
<td>Potential Threats</td>
<td>• Virtual Analyzer Result: Has analysis results</td>
</tr>
<tr>
<td></td>
<td>• File Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td>Email Threats</td>
<td>Protocol options include the following:</td>
</tr>
<tr>
<td></td>
<td>• IMAP4</td>
</tr>
<tr>
<td></td>
<td>• POP3</td>
</tr>
<tr>
<td></td>
<td>• SMTP</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Detection name options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Ransomware-related detections</td>
</tr>
</tbody>
</table>

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

For details, see *All Detections Advanced Search Filter on page 4-63*.

9. Click **Export**.

A zip folder with the following files downloads:

• threats.csv

• malicious_url.csv
All Detections - Detection Details

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

- **Header on page 4-57**
- **Connection Details on page 4-58**
- **File Analysis Results on page 4-60**

All Detections - Detection Details - Header

The following information is provided in the header at the top of the Detections Details window:

- **Detection Name**: For details about the threat, click the detection name.
  
  Deep Discovery Inspector connects with Threat Connect, where you can search for current information about the threat.

- **Severity**: Detection severity

- **Type**: Detection type

- **Description**: Description of detection type

**Table 4-20. Detection Types**

<table>
<thead>
<tr>
<th>Detection Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlated Incident</td>
<td>Events/detections that occur in a sequence or reach a threshold and define a pattern of activity</td>
</tr>
</tbody>
</table>
### Detection Types

<table>
<thead>
<tr>
<th>Detection Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruptive Application</td>
<td>Any peer-to-peer, instant messaging, or streaming media applications considered to be disruptive because they may do the following:</td>
</tr>
<tr>
<td></td>
<td>• Affect network performance</td>
</tr>
<tr>
<td></td>
<td>• Create security risks</td>
</tr>
<tr>
<td></td>
<td>• Distract employees</td>
</tr>
<tr>
<td>Exploit</td>
<td>Network and file-based attempts to access information</td>
</tr>
<tr>
<td>Grayware</td>
<td>Adware/grayware detections of all types and confidence levels</td>
</tr>
<tr>
<td>Malicious Behavior</td>
<td>Behavior that definitely indicates compromise with no further correlation needed, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Positively-identified malware communications</td>
</tr>
<tr>
<td></td>
<td>• Known malicious destination contacted</td>
</tr>
<tr>
<td></td>
<td>• Malicious behavioral patterns and strings</td>
</tr>
<tr>
<td>Malicious Content</td>
<td>File signature detections</td>
</tr>
<tr>
<td>Malicious URL</td>
<td>Websites that try to perform malicious activities</td>
</tr>
<tr>
<td>Suspicious Behavior</td>
<td>Behavior that could indicate compromise but requires further correlation to confirm, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Anomalous behavior</td>
</tr>
<tr>
<td></td>
<td>• False or misleading data</td>
</tr>
<tr>
<td></td>
<td>• Suspicious and malicious behavioral patterns and strings</td>
</tr>
</tbody>
</table>

### All Detections - Detection Details - Connection Details

Based on search criteria, **Connection Details** may include the following:

- Detection direction
- Host details
- Protocol details
• File details

• Additional event details

A graphical display includes the direction of the event and other information depending on the detection event search criteria.

Host details may include the following:

• IP Address

• Port

• MAC Address

• Network Group

• Network Zone

Table 4-21. Protocol Details

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel name</td>
<td>Name of the IRC channel</td>
</tr>
<tr>
<td>Message ID</td>
<td>Unique identifier of an email message</td>
</tr>
<tr>
<td>Recipient</td>
<td>Email address of the suspicious file recipient</td>
</tr>
<tr>
<td>Sender</td>
<td>Email address that sent the suspicious file</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the suspicious email</td>
</tr>
<tr>
<td>Target share</td>
<td>Shared folder where the malicious file is dropped</td>
</tr>
<tr>
<td>User agent</td>
<td>Client application used with a particular network protocol</td>
</tr>
<tr>
<td>User name</td>
<td>Name of the logged on user</td>
</tr>
</tbody>
</table>

Table 4-22. File Details

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of the file tagged as a potential/known risk</td>
</tr>
<tr>
<td><strong>NAME</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File size</td>
<td>Size of the file tagged as a potential/known risk</td>
</tr>
<tr>
<td>File extension</td>
<td>Extension of the file tagged as potential/known risk</td>
</tr>
<tr>
<td>File name in archive</td>
<td>Name of the file in the archive tagged as potential/known risk</td>
</tr>
</tbody>
</table>

**TABLE 4-23. Additional Event Details**

<table>
<thead>
<tr>
<th><strong>EVENT DETAIL</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Phase</td>
<td>Identifies the attack phase</td>
</tr>
<tr>
<td>Authentication</td>
<td>Indicates if the protocol requires authentication</td>
</tr>
<tr>
<td>BOT Command</td>
<td>Command used in IRC for BOTs</td>
</tr>
<tr>
<td>BOT URL</td>
<td>URL used in IRC for BOTs</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the engine that detected the threat (Network Content Inspection Engine, Advanced Threat Scan Engine, and/or Network Content Correlation Engine)</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>Defined in Network Content Correlation Pattern, used by the Network Content Correlation Engine</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Indicates if any mitigation action is needed</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used by the threat traffic</td>
</tr>
<tr>
<td>Outbreak Containment</td>
<td>Indicates if containment services are needed when an outbreak is detected</td>
</tr>
<tr>
<td>Services</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Link included in the email or the instant message content</td>
</tr>
</tbody>
</table>

**All Detections - Detection Details - File Analysis Results**

Based on search criteria, **File Analysis Results** may include the following:

- File Name
• File Size
• File Type
• MD5
• Parent File
• Risk Level
• SHA-1
• Threat
• Virtual Analyzer Images

**Table 4-24. File Analysis Results Tabs**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Behavior by Category</td>
<td>Displays one of the following:</td>
</tr>
<tr>
<td></td>
<td>• No threat behavior detected</td>
</tr>
<tr>
<td></td>
<td>• Name of threat behavior</td>
</tr>
<tr>
<td>Threat Events by Sequence</td>
<td>Displays any of the following:</td>
</tr>
<tr>
<td></td>
<td>• PID</td>
</tr>
<tr>
<td></td>
<td>• Parent PID</td>
</tr>
<tr>
<td></td>
<td>• Action</td>
</tr>
<tr>
<td></td>
<td>• Detail Information</td>
</tr>
<tr>
<td>Network Traffic</td>
<td>Displays any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Remote Host</td>
</tr>
<tr>
<td></td>
<td>• Protocol</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Requests</td>
</tr>
</tbody>
</table>

The following information is available for download:

• Parent File
• Raw Analysis Data
• Report

**Viewing All Detections - Detection Details**

**Procedure**

1. To view *All Detections* detection details for any event, click *Show* under the *Detail* column.

   Detection details about the event are displayed.

![Detection Details Window](image)

**FIGURE 4-16. All Detections - Detection Details**

2. On the *Detection Details* window, do the following:
   
   a. Click the detection name for details about the threat.
Deep Discovery Inspector connects with Threat Connect, where you can search for current information about the threat.

b. View the detection severity.

c. View the detection type.

For details, see All Detection Details - Header on page 4-57.

3. Click Export Connection Details to open or save the results.

4. Click Connection Details to view the direction of the event and host, file, and additional event details.

For details, see All Detection Details - Connection Details on page 4-58.

5. Click Download Detected File to export the connection details log.

6. For detection events from Virtual Analyzer, click File Analysis Results.

For details, see All Detection Details - File Analysis Results on page 4-60.

a. Select a parent file from the Select File dropdown menu.

b. (Optional) Click Download Parent File.

c. (Optional) Click Download Raw Analysis Data.

d. (Optional) Click Download Report.

e. Click the Threat Behaviours by Category tab to view event categories.

f. Click the Remote Host tab to view PID, Parent PID, Action, and Detail Information data.

g. Click the Network Traffic tab to view Remote Host, Protocol, Port, and Requests data.

---

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 20 advanced search filters.

For details, see Adding an All Detections Advanced Search Filter on page 4-68 and Editing an All Detections Advanced Search Filter on page 4-70.

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

**Table 4-25. Search Filter Criteria: All Detections**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP address</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>MAC address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered Services</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Active Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication Servers - Kerberos</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Content Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Database Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Domain Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTP Proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Audit Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SMTP Open Relay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Software Update Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Server</td>
</tr>
<tr>
<td>Protocol</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All protocol types</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Desired protocol type(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>Direction</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resolved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unresolved</td>
</tr>
<tr>
<td>Detection Name</td>
<td>Contains/Does not contain Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Correlation Rule ID (ICID)</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Type</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruptive Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Correlated Incident</td>
</tr>
<tr>
<td><strong>ATTRIBUTE</strong></td>
<td><strong>OPERATOR</strong></td>
<td><strong>ACTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intelligence Gathering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Point of Entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset/Data Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Exfiltration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown Attack Phase</td>
</tr>
<tr>
<td>C&amp;C List Source</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Global Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User-defined</td>
</tr>
<tr>
<td>Virtual Analyzer Result</td>
<td>Has analysis results/No analysis results</td>
<td></td>
</tr>
<tr>
<td>Is Targeted Attack Related</td>
<td>Yes/No</td>
<td></td>
</tr>
<tr>
<td>File Detection Type</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Known Malware</td>
</tr>
<tr>
<td>File Name</td>
<td>Has file name/No file name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File SHA-1</td>
<td>Has file SHA-1/No file SHA-1</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td></td>
</tr>
<tr>
<td>IP Address/Domain/URL</td>
<td>Has network object/No network object</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Address</td>
<td>Has email address/No email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Message ID (Email)</td>
<td>Has message ID/No message ID</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td></td>
</tr>
<tr>
<td>Subject (Email)</td>
<td>Has subject/No subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
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 the Search Filter Criteria: All Detections table *All Detections Advanced Search Filter on page 4-63.*

---

**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 20 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 **edit** 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 4-63.*

---

**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 20 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.

  ![Figure 4-20. Saving an All Detections Search](image)

  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.
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 5-6
- Scheduling a Report on page 5-7
- Deleting a Report Schedule on page 5-10
- On-demand Reports on page 5-10
- Generating On-demand Reports on page 5-12
- Deleting an On-demand Report on page 5-14
- Customization on page 5-14
- Customizing Reports on page 5-15
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**

<table>
<thead>
<tr>
<th>REPORT TYPE AND FORMAT</th>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Report</td>
<td>Detection Overview</td>
</tr>
<tr>
<td>Compressed archive</td>
<td>• Detection Overview</td>
</tr>
<tr>
<td>with the following</td>
<td>• Virtual Analyzer Summary</td>
</tr>
<tr>
<td>formats:</td>
<td>• Custom Deny List Events Summary</td>
</tr>
<tr>
<td>1. PDF file</td>
<td>• High Severity Hosts</td>
</tr>
<tr>
<td>2. CSV files</td>
<td>• High Severity Hosts Details</td>
</tr>
<tr>
<td></td>
<td>• Virtual Analyzer Result Details</td>
</tr>
<tr>
<td></td>
<td>• Deny List Detection Details</td>
</tr>
<tr>
<td></td>
<td>• Threat Statistics</td>
</tr>
<tr>
<td></td>
<td>• Top 20 Hosts Visiting Malicious Sites</td>
</tr>
<tr>
<td></td>
<td>• Malicious Content Statistics</td>
</tr>
<tr>
<td></td>
<td>• Informational Detections</td>
</tr>
<tr>
<td></td>
<td>• Disruptive Application Usage</td>
</tr>
<tr>
<td></td>
<td>• Recommendations</td>
</tr>
<tr>
<td></td>
<td>• Glossary</td>
</tr>
<tr>
<td></td>
<td>• Appendix A: Report Scope</td>
</tr>
<tr>
<td><strong>REPORT TYPE AND FORMAT</strong></td>
<td><strong>TABLE OF CONTENTS</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Executive Report PDF</td>
<td>• Highlights</td>
</tr>
<tr>
<td></td>
<td>• Business Risk Profile</td>
</tr>
<tr>
<td></td>
<td>• Affected Assets</td>
</tr>
<tr>
<td></td>
<td>• Infection Sources</td>
</tr>
<tr>
<td></td>
<td>• Detection Technology Used</td>
</tr>
<tr>
<td></td>
<td>• Threat Statistics</td>
</tr>
<tr>
<td></td>
<td>• Virtual Analyzer Statistics</td>
</tr>
<tr>
<td></td>
<td>• Disruptive Applications</td>
</tr>
<tr>
<td></td>
<td>• Deny List Entities</td>
</tr>
<tr>
<td></td>
<td>• Potential Impact</td>
</tr>
<tr>
<td></td>
<td>• Recommendations</td>
</tr>
<tr>
<td></td>
<td>• Appendices</td>
</tr>
<tr>
<td></td>
<td>• Appendix A: Report Scope</td>
</tr>
<tr>
<td></td>
<td>• Appendix B: Most-affected Host Summary</td>
</tr>
<tr>
<td>Host Severity Report PDF</td>
<td>• Summary</td>
</tr>
<tr>
<td></td>
<td>• Affected Hosts</td>
</tr>
<tr>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td>• Potential Threats</td>
</tr>
<tr>
<td></td>
<td>• Known Threats</td>
</tr>
<tr>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td></td>
<td>• Appendices</td>
</tr>
<tr>
<td></td>
<td>• Appendix A: Report Scope</td>
</tr>
<tr>
<td></td>
<td>• Appendix B: Host Severity of Affected Hosts</td>
</tr>
</tbody>
</table>
### Table of Contents

<table>
<thead>
<tr>
<th><strong>Report Type and Format</strong></th>
<th><strong>Table of Contents</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary Report PDF</td>
<td>• Overview</td>
</tr>
<tr>
<td></td>
<td>• Discovery Highlights</td>
</tr>
<tr>
<td></td>
<td>• Recommendations</td>
</tr>
<tr>
<td></td>
<td>• Appendix A: Report Scope</td>
</tr>
<tr>
<td>Threat Detection Report PDF</td>
<td>• Summary</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Threats detected exclusively by Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Threats detected by Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td>• Detected Known Malware Types</td>
</tr>
<tr>
<td></td>
<td>• Infection Channels</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Attack Sources Per Group</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Cross Group Attacks</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Attack Sources</td>
</tr>
<tr>
<td></td>
<td>• Top 10 Threat Types</td>
</tr>
<tr>
<td></td>
<td>• Threat Trends</td>
</tr>
<tr>
<td></td>
<td>• Virtual Analyzer Statistics</td>
</tr>
<tr>
<td></td>
<td>• Appendices</td>
</tr>
<tr>
<td></td>
<td>• Appendix A: Report Scope</td>
</tr>
<tr>
<td></td>
<td>• Appendix B: Recommendations</td>
</tr>
</tbody>
</table>

### Scheduled Reports

The **Scheduled Reports** screen displays user-scheduled daily, weekly, and monthly reports on a calendar.
Table 5-2. Calendar Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Frequency</th>
<th>User</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Daily</td>
<td>Administrator</td>
<td>Track threat status</td>
</tr>
<tr>
<td>W</td>
<td>Weekly</td>
<td>Executive</td>
<td>Overview of organization's security posture</td>
</tr>
<tr>
<td>M</td>
<td>Monthly</td>
<td>Executive</td>
<td>Overview of organization's security posture</td>
</tr>
</tbody>
</table>

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

Figure 5-1. Scheduled Reports
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**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Generic report period, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
<tr>
<td>Name</td>
<td>Customized or default report name</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Type       | Report types, including the following:  
  - Advanced  
  - Executive  
  - Host Severity  
  - Summary  
  - Threat Detection |
| 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.


**Table 5-4. Report Frequency**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td></td>
<td>Midnight to 23:59</td>
</tr>
<tr>
<td>Weekly</td>
<td><strong>Start week on:</strong></td>
<td>Default: Sunday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configurable: Sunday through Saturday</td>
</tr>
<tr>
<td>Frequency</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Monthly</td>
<td>Start month on day:</td>
<td>Default: Day 01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configurable: 01 through 31</td>
</tr>
</tbody>
</table>

**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 6-155.

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

![Image of On-demand Reports interface]

**Figure 5-4. On-demand Reports**

**Table 5-5. Column Names: On-demand Reports Tab**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated</td>
<td>Date and time a report was generated</td>
</tr>
<tr>
<td>Name</td>
<td>Customized or default report name</td>
</tr>
<tr>
<td>Type</td>
<td>Report types, including the following:</td>
</tr>
<tr>
<td></td>
<td>• Advanced</td>
</tr>
<tr>
<td></td>
<td>• Executive</td>
</tr>
<tr>
<td></td>
<td>• Host Severity</td>
</tr>
<tr>
<td></td>
<td>• Summary</td>
</tr>
<tr>
<td></td>
<td>• Threat Detection Report</td>
</tr>
<tr>
<td>Scope</td>
<td>Included hosts, including the following:</td>
</tr>
<tr>
<td></td>
<td>• All monitored hosts</td>
</tr>
<tr>
<td></td>
<td>• Filtered hosts</td>
</tr>
<tr>
<td>Period</td>
<td>Time range covered by the report</td>
</tr>
<tr>
<td>Created By</td>
<td>Name of the user account that generated the report</td>
</tr>
<tr>
<td>Download</td>
<td>Save or open a generated report</td>
</tr>
</tbody>
</table>
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 filter from Affected Hosts.

Note
Selectable saved search filters 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 5-15.*

![Customization Screen](image)

**FIGURE 5-5. Report Customization**
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 6-14
- Monitoring / Scanning on page 6-34
- Virtual Analyzer on page 6-63
- Network Groups and Assets on page 6-79
- Integrated Products/Services on page 6-85
- About Accounts on page 6-134
- System Settings on page 6-143
- System Logs on page 6-152
- System Maintenance on page 6-155
- Licenses on page 6-162
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**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Threat Scan Engine</td>
<td>Advanced Threat Scan Engine uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks.</td>
</tr>
<tr>
<td>Deep Discovery Memory Inspection Pattern</td>
<td>This technology provides enhanced virus scanning for polymorphic and mutation viruses, and augments virus-pattern-based scans by emulating file execution. The results are then analyzed in a controlled environment for evidence of malicious intent with little impact on system performance.</td>
</tr>
<tr>
<td>Deep Discovery Inspector Firmware</td>
<td>The program file used by Deep Discovery Inspector.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Trend Micro recommends using the Firmware Update screen when updating the firmware.</td>
</tr>
<tr>
<td>IntelliTrap Pattern</td>
<td>IntelliTrap Pattern identifies real-time compressed executable file types that commonly hide malware and other potential threats.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IntelliTrap Exception Pattern</td>
<td>IntelliTrap Exception Pattern contains a list of real-time compressed executable file types that are commonly safe from malware and other potential threats.</td>
</tr>
<tr>
<td>Network Content Correlation Pattern</td>
<td>Network Content Correlation Pattern implements detection rules defined by Trend Micro.</td>
</tr>
<tr>
<td>Network Content Inspection Engine</td>
<td>The engine used to perform network scanning.</td>
</tr>
<tr>
<td>Network Content Inspection Pattern</td>
<td>The pattern is used by the Network Content Inspection Engine to perform network scanning.</td>
</tr>
<tr>
<td>Spyware Active-monitoring Pattern</td>
<td>The Spyware Active-monitoring 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.</td>
</tr>
<tr>
<td>Threat Correlation Pattern</td>
<td>The pattern used by Deep Discovery Inspector to perform threat correlation.</td>
</tr>
<tr>
<td>Threat Knowledge Base</td>
<td>The database used to provide information for threat correlation.</td>
</tr>
<tr>
<td>Virtual Analyzer Sensors</td>
<td>Virtual Analyzer Sensors is a module on sandbox instances used for analyzing samples.</td>
</tr>
<tr>
<td>Virus Pattern</td>
<td>Virus Scan Engine detects Internet worms, mass-mailers, Trojans, phishing sites, spyware, network exploits and viruses in messages and attachments.</td>
</tr>
<tr>
<td>Widget Framework</td>
<td>Provides a template for Deep Discovery Inspector widgets.</td>
</tr>
</tbody>
</table>

**Component Update Methods**

Use one of the following methods to update components:
## Table 6-2. Update Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual update</td>
<td>To check the availability of new components, go to Administration &gt; Updates &gt; Component Updates on the management console. For details, see Manual Updates on page 6-4.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Inspector updates all components. You cannot update components individually.</td>
</tr>
<tr>
<td></td>
<td>To update Deep Discovery Inspector components, go to Administration &gt; Updates &gt; Component Updates &gt; Source. For details, see Update Source on page 6-6.</td>
</tr>
<tr>
<td>Scheduled update</td>
<td>To configure an update schedule, go to Administration &gt; Updates &gt; Component Updates &gt; Scheduled. Deep Discovery Inspector automatically checks the update source at the specified frequency. For details, see Scheduled Updates on page 6-5.</td>
</tr>
</tbody>
</table>

### Component Update Tasks

To update all components, review the following procedures:

- Proxy on page 6-144
- Manual Updates on page 6-4
- Scheduled Updates on page 6-5
- Update Source on page 6-6
- Service Packs / Version Upgrade on page 6-11

### 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**

<table>
<thead>
<tr>
<th>DETAILS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Component name</td>
</tr>
<tr>
<td>Current Version</td>
<td>Version number of each component currently used by the product</td>
</tr>
<tr>
<td>Latest Version</td>
<td>Latest version available on the server</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Date and time of the last update</td>
</tr>
</tbody>
</table>

**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 **Minute, 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.

---

**Note**

Configure Deep Discovery Inspector to download directly from Trend Micro Control Manager. For details on how a Control Manager server can act as an update source, see the *Trend Micro Control Manager 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.mycompany.com
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.

  Upgrading the firmware updates existing application files and enhances features.

  For details, see *Service Packs / Version Upgrade on page 6-11.*

- Rescue the application.

  Rescuing the application replaces application files that monitor traffic and create logs. Rescue the application if Deep Discovery Inspector files become corrupted.

  Before rescuing the application, create a backup of your settings. You can choose to retain your current data, logs, and configuration settings after the rescue, or revert to the product’s default settings.

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

- 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 6-158.*

**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**

<table>
<thead>
<tr>
<th>System Update</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot fix</td>
<td>A hot fix 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 hot fixes, applying a hot fix typically requires stopping program daemons, copying the hot fix file to overwrite its counterpart in your installation, and restarting the daemons.</td>
</tr>
<tr>
<td>Security patch</td>
<td>A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.</td>
</tr>
<tr>
<td>Patch</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:


**Applying a Hot Fix / Patch**

**Procedure**

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

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.

   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. 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 Hot Fix / 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 versions 3.6, 3.7, and 3.8 can be upgraded to version 3.8 SP1. Deep Discovery Inspector versions older than version 3.6 must perform a fresh installation.

You can choose to retain existing data, logs, and configuration settings after the upgrade, or revert to the product’s default settings.

<table>
<thead>
<tr>
<th>TABLE 6-5. Service Pack / Version Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM UPGRADE</strong></td>
</tr>
<tr>
<td>Service Pack</td>
</tr>
<tr>
<td>Version Upgrade</td>
</tr>
</tbody>
</table>

Applying a Service Pack / Version Upgrade

FIGURE 6-1. Service Packs / Version Upgrade
Procedure

1. Back up appliance configuration settings. For details, see Backup / Restore on page 6-158.

2. If you have registered Deep Discovery Inspector to Control Manager, record the Control Manager registration details.

   **Note**
   
   You can choose to migrate your current product settings after the service pack / version upgrade is complete so that you do not need to reconfigure settings.
   
   - If Migrate Configuration is selected during the service pack / version upgrade, Deep Discovery Inspector re-registers to Control Manager automatically after the firmware update completes.
   
   - If Migrate Configuration is not selected, you must manually re-register to Control Manager after the service pack / version upgrade 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 extension.

7. Click Upload.

   The Migrate configuration? option appears.

8. Enable this option to retain the current product settings after the upgrade, or disable it to revert to the product’s default settings.
**WARNING!**
Performing the next step restarts Deep Discovery Inspector. Make sure that you have finished all product console tasks before continuing.

9. Click **Continue**.

10. Click **OK**.

Deep Discovery Inspector updates the firmware and restarts.

11. Clear the browser cache. For details, see *Clearing the Browser Cache on page 6-13*.

12. Log back on to the management console.

13. If Deep Discovery Inspector is registered to Control Manager, register the product again. For details, see *Registering to Control Manager on page 6-92*.

---

**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 Internet Explorer:
   a. Go to Tools > Internet Options > General.
   b. Under Browsing history, click Delete.
      The Delete Browsing History window opens.
   c. Select Temporary Internet files and website files, and Cookies and Website data.
   d. Click Delete.
      The Delete Browsing History window closes.
   e. On the Internet Options window, click OK.

Notifications

Deep Discovery Inspector can send email notifications for threshold-based network events.

Configure the following:

• Notification settings
  Enable notifications and customize the subject and content of each notification using the message tokens provided.

• Delivery options
  Configure sender and recipient information for all notifications on the Delivery Options screen. For details, see Delivery Options on page 6-32.
### Table 6-6. Notifications for Threshold-based Network Events

<table>
<thead>
<tr>
<th><strong>Event</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detections</td>
<td>The number of threat detections reached the configured threshold. For details, see <em>Configuring Threat Detection Notifications on page 6-15</em>.</td>
</tr>
<tr>
<td>High Risk Hosts Detections</td>
<td>Deep Discovery Inspector identified a high-risk host on your network. For details, see <em>Configuring High Risk Hosts Detections Notifications on page 6-17</em>.</td>
</tr>
<tr>
<td>Suspicious Hosts Detections</td>
<td>The number of suspicious hosts reached the threshold. For details, see <em>Configuring Suspicious Hosts Detections Notifications on page 6-20</em>.</td>
</tr>
<tr>
<td>High Network Traffic</td>
<td>The network traffic volume reached the threshold. For details, see <em>Configuring High Network Traffic Notifications on page 6-22</em>.</td>
</tr>
<tr>
<td>Unanalyzed Sample Detections</td>
<td>Virtual Analyzer was unable to analyze files. For details, see <em>Configuring Unanalyzed Sample Detections Notifications on page 6-24</em>.</td>
</tr>
<tr>
<td>Virtual Analyzer Detections</td>
<td>Virtual Analyzer detected malicious content in a sample. For details, see <em>Configuring Virtual Analyzer Detections Notifications on page 6-26</em>.</td>
</tr>
<tr>
<td>Deny List</td>
<td>A detection matched an object in the user-defined Deny List. For details, see <em>Configuring Deny List Notifications on page 6-28</em>.</td>
</tr>
<tr>
<td>Retro Scan Detections</td>
<td>Retro Scan detected historical callback attempts to C&amp;C servers in the TM Global Intelligence List. For details, see <em>Configuring Retro Scan Detections Notifications on page 6-30</em>.</td>
</tr>
</tbody>
</table>

### Configuring Threat Detection Notifications

Deep Discovery Inspector can send this notification when the number of detections reaches the configured threshold. The notification specifies the number of detections for each threat type.
Procedure

1. Go to Administration > Notifications > Notification Settings > Threat Detections.

   The Threat Detections Notification screen appears.

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

   **Tip**
   Trend Micro recommends using the default settings.

4. Select the types of threats to detect.

5. (Optional) Configure the notification recipients.

   For details, see Configuring Email Notification Settings on page 6-32.

6. (Optional) Modify the default message content.

   a. Type a subject that does not exceed 256 characters.
   b. Type message content that does not exceed 4,096 characters.

   Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>MESSAGE TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOOP_END</strong></td>
<td>End of message token loop</td>
</tr>
<tr>
<td><strong>LOOP_RISKS_COUNT</strong></td>
<td>Detection count</td>
</tr>
<tr>
<td><strong>LOOP_RISKS_DIRECTION</strong></td>
<td>Direction of network traffic</td>
</tr>
<tr>
<td><strong>LOOP_RISKS_NAME</strong></td>
<td>Detection type</td>
</tr>
<tr>
<td><strong>LOOP_RISKS_THRESHOLD</strong></td>
<td>Detection threshold</td>
</tr>
</tbody>
</table>
### Configuring High Risk Hosts Detections Notifications

Deep Discovery Inspector can send this notification when it detects a high-risk host. The notification contains information that can help determine the cause of the increased detections.

**Procedure**

1. Go to Administration > Notifications > Notification Settings > High Risk Hosts Detections.
The *High Risk Hosts Detections* screen appears.

![High Risk Hosts Detections](image)

**Figure 6-2. High Risk Hosts Detections**

2. Select **Notify Administrator for high risk hosts**.

3. 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.

4. (Optional) Configure the notification recipients.
   For details, see *Configuring Email Notification Settings on page 6-32*.

5. (Optional) Modify the default message content.
a. Type a subject that does not exceed 256 characters.

b. Type message content that does not exceed 4,096 characters.

Use any of the following message tokens to customize the notification template.

<table>
<thead>
<tr>
<th>MESSAGE_TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AFFECTED_HOST</strong></td>
<td>Affected host</td>
</tr>
<tr>
<td><strong>BEHAVIOR</strong></td>
<td>Description of suspicious behavior</td>
</tr>
<tr>
<td><strong>DATE</strong></td>
<td>Threat detection date and time</td>
</tr>
<tr>
<td><strong>DIRECTION</strong></td>
<td>Network traffic direction</td>
</tr>
<tr>
<td><strong>DST_ACCOUNT</strong></td>
<td>Destination account</td>
</tr>
<tr>
<td><strong>DST_GROUP</strong></td>
<td>Destination group</td>
</tr>
<tr>
<td><strong>DST_IP_ADDR</strong></td>
<td>Destination IP</td>
</tr>
<tr>
<td><strong>DST_MAC_ADDR</strong></td>
<td>Destination MAC address</td>
</tr>
<tr>
<td><strong>DST_PORT</strong></td>
<td>Destination port</td>
</tr>
<tr>
<td><strong>DST_ZONE</strong></td>
<td>Destination zone</td>
</tr>
<tr>
<td><strong>HOSTNAME</strong></td>
<td>Host name</td>
</tr>
<tr>
<td><strong>HOST_IP</strong></td>
<td>High-risk host IP address</td>
</tr>
<tr>
<td><strong>INCIDENT_COUNT</strong></td>
<td>Number of high risk hosts</td>
</tr>
<tr>
<td><strong>LOG_QUERY_URL</strong></td>
<td>Link to the All Detections screen on the management console</td>
</tr>
<tr>
<td><strong>NETWORK_PROTOCOL</strong></td>
<td>Network protocol</td>
</tr>
<tr>
<td><strong>SRC_ACCOUNT</strong></td>
<td>Source account</td>
</tr>
<tr>
<td><strong>SRC_GROUP</strong></td>
<td>Source group</td>
</tr>
<tr>
<td><strong>SRC_IP_ADDR</strong></td>
<td>Source IP address</td>
</tr>
<tr>
<td><strong>SRC_MAC_ADDR</strong></td>
<td>Source MAC address</td>
</tr>
</tbody>
</table>
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.

Configuring Suspicious Hosts Detections Notifications

Deep Discovery Inspector can send this notification when detecting suspicious hosts. A host is considered suspicious when the number of detections associated with it reaches the configured threshold. The notification contains information that can help determine the cause of the increased detections.
Procedure

1. Go to Administration > Notifications > Notification Settings > Suspicious Hosts Detections.

   The Suspicious Hosts Detections screen appears.

   ![Suspicious Hosts Detections](image)

   **Figure 6-3.** 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 6-32.
5. (Optional) Modify the default message content.
   a. Type a subject that does not exceed 256 characters.
   b. Type message content that does not exceed 4,096 characters.

Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>MESSAGE_TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOOP_END</strong></td>
<td>End of message token loop</td>
</tr>
<tr>
<td><strong>LOOP_HOST_IP</strong></td>
<td>Host IP address</td>
</tr>
<tr>
<td><strong>LOOP_INCIDENT_NUMBER</strong></td>
<td>Incident count</td>
</tr>
<tr>
<td><strong>LOOP_INCIDENT_THRESHOLD</strong></td>
<td>Incident threshold</td>
</tr>
<tr>
<td><strong>LOOP_START</strong></td>
<td>Start of message token loop</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Notification date and time</td>
</tr>
</tbody>
</table>

**Note**

When a __LOOP_[variable]__ message token is applied, the LOOP variable will repeat continuously between the LOOP start time and the LOOP end time.

6. Click **Save**.

---

**Configuring High Network Traffic Notifications**

Deep Discovery Inspector can send this notification when the amount of network traffic reaches the configured threshold. Increased activity may indicate an attack on your network.

**Procedure**

1. Go to Administration > Notifications > Notification Settings > High Network Traffic.
The **High Network Traffic** screen appears.

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.
4. (Optional) Configure the notification recipients.

For details, see Configuring Email Notification Settings on page 6-32.

5. (Optional) Modify the default message content.

a. Type a subject that does not exceed 256 characters.

b. Type message content that does not exceed 4,096 characters.

Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>MESSAGE_TOKENS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Notification date and time</td>
</tr>
<tr>
<td><strong>TRAFFIC_END_TIME</strong></td>
<td>Traffic monitoring end date and time</td>
</tr>
<tr>
<td><strong>TRAFFIC_START_TIME</strong></td>
<td>Traffic monitoring start date and time</td>
</tr>
<tr>
<td><strong>TRAFFIC_THRESHOLD</strong></td>
<td>Network traffic threshold</td>
</tr>
</tbody>
</table>

6. Click Save.

Configuring Unanalyzed Sample Detections Notifications

Deep Discovery Inspector can send this notification when Virtual Analyzer is unable to analyze samples. The notification provides 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.
The **Unanalyzed Sample Detections** screen appears.

![Unanalyzed Sample Detections Screen](image)

**Figure 6-5. Unanalyzed Sample Detections**

1. Select **Notify Administrator for unanalyzed sample detections**.
2. 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 6-32*.

5. (Optional) Modify the default message content.
   a. Type a subject that does not exceed 256 characters.
   b. Type message content that does not exceed 4,096 characters.
Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>MESSAGE_TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP_ADDRESS</strong></td>
<td>Deep Discovery Inspector IP address</td>
</tr>
<tr>
<td><strong>LOOP_END</strong></td>
<td>End of message token loop</td>
</tr>
<tr>
<td><strong>LOOP_SAMPLE_FILE_ANALYZETIME</strong></td>
<td>Sample analysis date and time</td>
</tr>
<tr>
<td><strong>LOOP_SAMPLE_FILE_DOWNLOAD_URL</strong></td>
<td>Sample download URL</td>
</tr>
<tr>
<td><strong>LOOP_SAMPLE_FILE_SHA1</strong></td>
<td>File SHA-1</td>
</tr>
<tr>
<td><strong>LOOP_SAMPLE_FILE_SIZE</strong></td>
<td>File size</td>
</tr>
<tr>
<td><strong>LOOP_SAMPLE_FILE_TYPE</strong></td>
<td>File type</td>
</tr>
<tr>
<td><strong>LOOP_START</strong></td>
<td>Start of message token loop</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Notification date and time</td>
</tr>
<tr>
<td><strong>TOTAL_FAILED_COUNT</strong></td>
<td>Number of unanalyzed samples</td>
</tr>
</tbody>
</table>

**Note**

When a __LOOP__[variable]__ message token is applied, the LOOP variable will repeat continuously between the LOOP start time and the LOOP end time.

6. Click **Save**.

---

**Configuring Virtual Analyzer Detections Notifications**

Deep Discovery Inspector can send this notification when a file does not match any pattern but is recognized as suspicious by Virtual Analyzer within the specified period.

**Procedure**

1. Go to **Administration > Notifications > Notification Settings > Virtual Analyzer Detections**.
The Virtual Analyzer Detections screen appears.

![Virtual Analyzer Detections](image)

**FIGURE 6-6. 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 6-32*. 
5. (Optional) Modify the default message content.
   a. Type a subject that does not exceed 256 characters.
   b. Type message content that does not exceed 4,096 characters.

   Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DETECTION_DETAIL</strong></td>
<td>Virtual Analyzer detection details</td>
</tr>
<tr>
<td><strong>HTTPURL</strong></td>
<td>Deep Discovery Inspector management console URL</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Notification date and time</td>
</tr>
<tr>
<td><strong>XHOURS</strong></td>
<td>Notification sending interval</td>
</tr>
</tbody>
</table>

6. Click Save.

---

**Configuring Deny List Notifications**

Deep Discovery Inspector can send this notification when it detects a threat that matches an object in the Deny List within the specified period.

---

**Procedure**

1. Go to Administration > Notifications > Notification Settings > Deny List.
The **Deny List** screen appears.

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 6-32*.

5. (Optional) Modify the default message content.
   
   a. Type a subject that does not exceed 256 characters.
   
   b. Type message content that does not exceed 4,096 characters.
Use any of the following message tokens when customizing the notification.

<table>
<thead>
<tr>
<th>MESSAGE_TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTPURL</strong></td>
<td>Deep Discovery Inspector management console URL</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Notification date and time</td>
</tr>
<tr>
<td><strong>XHOURS</strong></td>
<td>Notification sending interval</td>
</tr>
</tbody>
</table>

6. Click **Save**.

### Configuring Retro Scan Detections Notifications

Deep Discovery Inspector can send this notification when Retro Scan detects historical callback attempts to C&C servers in the Trend Micro Global Intelligence List.

**Procedure**

1. Go to **Administration > Notifications > Retro Scan Detections**.
The **Retro Scan Detections** screen appears.

**FIGURE 6-7. 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 6-32*.

5. (Optional) Modify the default message content.
   a. Type a subject that does not exceed 256 characters.
b. Type message content that does not exceed 4,096 characters.

Use any of the following message tokens to customize the notification template.

<table>
<thead>
<tr>
<th>MESSAGE_TOKEN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTPURL</strong></td>
<td>Deep Discovery Inspector management console URL</td>
</tr>
<tr>
<td><strong>RETRO_SCAN_COMPROMISED_HOST_NUM</strong></td>
<td>Number of compromised hosts</td>
</tr>
<tr>
<td><strong>RETRO_SCAN_C_AND_C_CALLBACK_NUM</strong></td>
<td>Number of C&amp;C callback attempts found</td>
</tr>
<tr>
<td><strong>TIMESTAMP</strong></td>
<td>Retro Scan report run date and time</td>
</tr>
</tbody>
</table>

**Delivery Options**

Use the **Email Settings** screen to configure the following for all notifications:

- Recipient email address
- Sender email address
- SMTP server settings

**Configuring Email Notification Settings**

**Procedure**

1. Go to **Administration > Notifications > Delivery Options > Email Settings**.
Figure 6-8. Email Notification Settings

2. Type at least one notification recipient email address.
   Use a semicolon “;” to separate multiple addresses.

3. Type the sender's email address.

4. Type the SMTP server name or IP address.

5. Type a valid SMTP server port number.

6. If the SMTP server requires authentication, type a valid SMTP user name and password.

   Important
   Make sure to add the Deep Discovery Inspector IP address to the SMTP relay list.

7. Specify the maximum number of notifications and the number of minutes to check the mail queue.

   Tip
   Trend Micro recommends using the default settings.

8. Click Save.

9. (Optional) Click Test Mail.
If the SMTP server settings are correctly configured, Deep Discovery Inspector sends a test email message to all recipient addresses.

Monitor the Monitoring / Scanning module to 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 6-41

For more information, see Smart Protection Technology on page 6-38

- Application Filters on page 6-45
- Deny List / Allow List on page 6-47
- Detection Rules on page 6-60
- 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 / Ports**

**Procedure**

1. Go to **Administration > Monitoring / Scanning > Hosts / Ports.**

![Hosts / Ports](image)

**Figure 6-9. 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.**
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 threat information to the Trend Micro Smart Protection Network.

When enabled, Trend Micro Smart Feedback shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats.

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 Technology**

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. These two sources provide the same reputation services and can be integrated individually or in combination. The following table provides a comparison.
### Table 6-7. Smart Protection Sources

<table>
<thead>
<tr>
<th>Basis of Comparison</th>
<th>Trend Micro Smart Protection Network</th>
<th>Smart Protection Server</th>
</tr>
</thead>
</table>
| **Purpose**         | A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology | • 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 |
| Administration      | Hosted and maintained by Trend Micro | Installed and managed by Trend Micro product administrators |
| Connection protocol | HTTP                                  | HTTP                    |
| **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

<table>
<thead>
<tr>
<th>CONSIDERATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Trend Micro recommends installing multiple Smart Protection Servers for failover purposes. Deep Discovery Inspector checks the Smart Protection Server list configured in the management console to determine which server to connect to first, and the alternative servers if the first server is unavailable.</td>
</tr>
<tr>
<td>Version</td>
<td>For details on the Smart Protection Server versions compatible with Deep Discovery Inspector, see <em>Trend Micro Integrated Products/Services on page 6-85.</em></td>
</tr>
<tr>
<td>IP Address</td>
<td>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.</td>
</tr>
</tbody>
</table>

Setting Up Smart Protection Server

**Procedure**

1. Install Smart Protection Server 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.

## Managing the Smart Protection Server List

### 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. 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, and uploads the logs to the Threat Management Services Portal for report generation.

---

**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, see *Smart Protection Technology on page 6-38.*

## Configuring Web Reputation Settings

**Procedure**

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

![Web Reputation Screen](image)

**Figure 6-11. Web Reputation Screen**

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 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 4-46.*
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 to connect to Smart Protection Server:
- 5274
- 4343
- 80
- 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 6-8. Application Types**

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging</td>
<td>Communicate and share information and files between contacts</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P Traffic</td>
<td>Share files from one computer to another</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>Play audio-visual content while downloading</td>
</tr>
</tbody>
</table>

Configuring Application Filter Settings

Procedure

1. Go to Administration > Monitoring / Scanning > Application Filters.

![Application Filters]

**Figure 6-12. Application Filter**

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.
   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.
   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 6-9. Deny List / Allow List Tabs

<table>
<thead>
<tr>
<th>TAB</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **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. |
| **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 6-10. Deny List / Allow List Format Rules

<table>
<thead>
<tr>
<th>Format Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>Syntax</td>
</tr>
<tr>
<td>• Single IP:</td>
<td></td>
</tr>
<tr>
<td>IP addresses must be in the format: XXX.XXX.XXX.XXX, where X is a whole number between 0 and 255.</td>
<td></td>
</tr>
<tr>
<td>IPv4 example: 192.168.1.1</td>
<td></td>
</tr>
<tr>
<td>IPv6 example: fd00:1:1111:200::1000</td>
<td></td>
</tr>
<tr>
<td>• IP Range:</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>IPv4 example: 192.168.1.0-192.168.1.255</td>
<td></td>
</tr>
<tr>
<td>IPv6 example: fd00:1:1111:200::1000-fd00:1:1111:200::1fff</td>
<td></td>
</tr>
<tr>
<td>• Subnet:</td>
<td></td>
</tr>
<tr>
<td>IP addresses must be in the format: XXX.XXX.XXX.XXX/&lt;Mask Bit&gt;, where X is a whole number between 0 and 255, and &lt;Mask Bit&gt; is a whole number between 1 and 32.</td>
<td></td>
</tr>
<tr>
<td>IPv4 example: 192.168.1.0/24</td>
<td></td>
</tr>
<tr>
<td>IPv6 example: fd00:1:1111:200::1000/116</td>
<td></td>
</tr>
</tbody>
</table>

**Maximum IP Address Entities**

Add up to 1000 Deny / Allow List IP Address entities.
<table>
<thead>
<tr>
<th>Format Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td><strong>Supported Characters</strong>&lt;br&gt;Each domain name must have at least one character.&lt;br&gt;Deep Discovery Inspector supports the following characters for domain names:&lt;br&gt;ASCII&lt;br&gt;• 0x2D (-), 0x2E (.)&lt;br&gt;• 0x30 (0) ~ 0x39 (9)&lt;br&gt;• 0x41 (A) ~ 0x5A (Z)&lt;br&gt;• 0x61 (a) ~ 0x7A (z)&lt;br&gt;UTF-8 characters (ASCII code &gt;=0x80)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>&lt;br&gt;Convert non-UTF8 characters to Punycode.</td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Length</strong>&lt;br&gt;Maximum length of each domain name: 63 characters&lt;br&gt;Maximum length of domain: 255 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Wildcards (*)</strong>&lt;br&gt;Wildcards are only allowed in a prefix. When a wildcard is used in a prefix, it must be connected with &quot;. &quot;. Only one wildcard may be used in a domain.&lt;br&gt;Domain matching is case-sensitive.</td>
</tr>
<tr>
<td>Maximum Domain Entities</td>
<td>Add up to 1000 Deny List / Allow List <strong>Domain</strong> entities.</td>
</tr>
</tbody>
</table>
### Format Rule | Description
--- | ---
**URL** | **Syntax**
[http://]<Domain>[:<Port>][/<URI-prefix>]
- [http://]
  Accepted and ignored
- <Domain>
  Follow the syntax of Domain deny list for DNS.
- [:<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.

**Maximum URL Entities** | Add up to 1000 Deny / Allow List URL entities.
<table>
<thead>
<tr>
<th>FORMAT RULE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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 / 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**.

**Figure 6-13. Deny List**

**Figure 6-14. Allow List**
Configuring Deny Lists / 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.

<table>
<thead>
<tr>
<th>LIST TYPE</th>
<th>NAME TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>SHA-1</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>IP Address</td>
</tr>
<tr>
<td>URLs</td>
<td>URL</td>
</tr>
<tr>
<td>Domains</td>
<td>Domain</td>
</tr>
</tbody>
</table>

   c. (Deny List only) Set an Action to manage the connection to the new entity.

<table>
<thead>
<tr>
<th>LIST TYPE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>Monitor</td>
</tr>
</tbody>
</table>
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 6-11. Format Rules for Importing Deny Lists / Allow Lists

<table>
<thead>
<tr>
<th>FORMAT RULE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Comments are limited to 64 characters.</td>
</tr>
<tr>
<td>Duplicate Files</td>
<td>You can import duplicate files.</td>
</tr>
<tr>
<td>CSV Format</td>
<td>Deep Discovery Inspector supports only standard .csv format. Use comma separation and UTF-8 encoding.</td>
</tr>
</tbody>
</table>

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

FIGURE 6-15. Import/Export Tab

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

**Figure 6-16. Import/Export Tab**

**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.

Configuring Detection Rules Settings

Procedure

1. Go to Administration > Monitoring / Scanning > Detection Rules.
2. Use the Change all rules to drop-down menu to change detection rules to one of the following:
   - Default Status
     (Recommended) Select to set detection rules to default settings.
   - Enabled
     Select to enable all detection rules.
   - Disabled
     Select to disable all detection rules.
3. Click Save Changes.

Detection rules are either activated or disabled.

Exceptions

Exceptions contains a list of IP addresses and protocols. Threats detected on any of the IP addresses with the specified protocols are not recorded in the logs.

Important

Outbreak Containment Service will not block activities on the IP addresses that may lead to an outbreak. When configuring the exceptions list, include only trusted IP addresses.
**Configuring Host Exceptions**

**Procedure**

1. Go to Administration > Monitoring / Scanning > Exceptions.
2. Select the Host Exceptions tab.
3. Select a protocol from the drop-down menu.
4. Specify a unique name for easy identification.
5. Specify an IP address or IP address range in the text field.
   a. Use a dash to specify an IP address range.

   The Host Exceptions tab supports IPv4 and IPv6:
   - IPv4 example: 192.168.1.1
   - IPv4 example: 192.168.1.0-192.168.1.255
   - IPv6 example: 2620:1005::123-2620:1005::460
   b. Use a slash to specify the subnet mask/prefix for IP addresses.
- IPv4 subnet mask example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24
- IPv6 subnet prefix example: fd00:1:1111:200::1000/116

6. Click Add.

7. To remove an item from the Exceptions List, select the item and click Delete.

---

**Configuring Outbreak Containment Service Exceptions**

**Procedure**

1. Go to Administration > Monitoring / Scanning > Exceptions.

2. Select the Outbreak Containment Service tab.

3. Specify a unique name for easy identification.

4. Specify an IP address or IP address range in the text field.
   a. Use a dash to specify an IP address range.
      
      The Outbreak Containment Service tab supports IPv4 and IPv6:
      
      - IPv4 example: 192.168.1.0-192.168.1.255
      - IPv6 example: 2620:1005::123

   b. Use a slash to specify the subnet mask for IP addresses.
      
      - IPv4 example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24
      - IPv6 example: fd00:1:1111:200::1000/116

5. Click Add.

6. To remove an item from the Exceptions List, select the item and click Delete.
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.

Virtual Analyzer is built into Deep Discovery Inspector and can be enabled at any time. Deep Discovery Inspector can also connect to an external Virtual Analyzer built into other Trend Micro Deep Discovery products.

This section includes the following categories:

• Virtual Analyzer Setup on page 6-63
• File Submissions on page 6-65
• Internal Virtual Analyzer on page 6-71
• Modifying Instances on page 6-76

Virtual Analyzer Setup

Submit files to one of the following Virtual Analyzer types:

• **Internal**: Built into Deep Discovery Inspector
• **External**: Built into other Trend Micro Deep Discovery 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.

Enabling Virtual Analyzer

Procedure

1. Go to Administration > Virtual Analyzer > Setup.
2. Select **Submit files to Virtual Analyzer**.

3. Select a **Virtual Analyzer** type:
   - **Internal**
   - **External**

4. (Optional) For **Internal** Virtual Analyzer, select a network type.

The selected network type determines the Internet connectivity of Virtual Analyzer.

<table>
<thead>
<tr>
<th>Network Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network</td>
<td>Direct Virtual Analyzer traffic through a management port. Virtual Analyzer connects to the Internet using the Deep Discovery Inspector management port.</td>
</tr>
<tr>
<td>Specified Network</td>
<td>Configure a specific port for Virtual Analyzer traffic. Make sure that the port is able to connect directly to an outside network. Virtual Analyzer connects to the Internet using another port. Specify an open port and make sure that there are no port conflicts.</td>
</tr>
<tr>
<td>Isolated Network</td>
<td>Isolate Virtual Analyzer traffic within Virtual Analyzer. The environment has no connection to an outside network. Virtual Analyzer has no Internet connection and relies only on its analysis engine.</td>
</tr>
</tbody>
</table>

**Note**

Virtual Analyzer requires an Internet connection to query Trend Micro cloud-based services (for example, WRS and CSSS) for available threat data.

5. (Optional) For **External** Virtual Analyzer, do the following.
   a. Type the IP address of the Virtual Analyzer appliance.
   b. Type the API key from the external Virtual Analyzer.
Log onto the external Virtual Analyzer to obtain the API key.

c. Click **Test Connection**.

6. Click **Save**.

**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>
<thead>
<tr>
<th>TABLE 6-12. Default Submission Rule Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RULE TYPE</strong></td>
</tr>
<tr>
<td>Basic</td>
</tr>
<tr>
<td>Advanced</td>
</tr>
<tr>
<td>Basic</td>
</tr>
<tr>
<td>Basic</td>
</tr>
</tbody>
</table>

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 and 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

3. File Extension

<table>
<thead>
<tr>
<th>FILE TYPE</th>
<th>FILE EXTENSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash File</td>
<td>.swf</td>
</tr>
<tr>
<td>JAVA Applet</td>
<td>.jar</td>
</tr>
<tr>
<td>Java Archive</td>
<td>.jar</td>
</tr>
<tr>
<td>Microsoft Compiled HTML Help</td>
<td>.chm</td>
</tr>
<tr>
<td>Microsoft Office files</td>
<td>as applicable</td>
</tr>
<tr>
<td>Microsoft Windows Shortcut File</td>
<td>.lnk</td>
</tr>
<tr>
<td>Portable Document Format</td>
<td>.pdf</td>
</tr>
<tr>
<td>RAR Compressed Archive File</td>
<td>.rar</td>
</tr>
<tr>
<td>Tape Archive (Tar) File</td>
<td>.tar</td>
</tr>
<tr>
<td>Windows Executable File</td>
<td>.exe</td>
</tr>
<tr>
<td>7zip</td>
<td>.7z</td>
</tr>
<tr>
<td><strong>FILE TYPE</strong></td>
<td><strong>FILE EXTENSION</strong></td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Bzip Compressed Archive File</td>
<td>.bz2</td>
</tr>
<tr>
<td>Zip Compressed Archive File</td>
<td>.zip</td>
</tr>
</tbody>
</table>

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**

**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.
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
   - **Any of the following**:

---

**Note**

Select this option to search for files that meet certain criteria but do not have detections.
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: Specify a file extension.
   - 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

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 **Save**.

---

**Internal Virtual Analyzer**

Deep Discovery Inspector provides 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 on this screen apply to an external Virtual Analyzer. For details about external analysis modules, refer to the applicable product Administrator’s Guide.

---

The **Internal Virtual Analyzer screen** contains the following tabs:

• Status

• Images

• Passwords

---

**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

To allow Virtual Analyzer to analyze files, import custom OVA files that are between 1 GB and 20 GB in size.

Tip
Use the Trend Micro Virtual Analyzer Image Preparation Tool to prepare a custom sandbox image from scratch.

Obtain a copy of the Image Preparation Tool from your support provider. The tool comes as a zip package (SandboxWizard.zip).


Manually create a custom image using VirtualBox. For details, see Manually Creating Custom Images on page A-52.

The hardware specifications of your Deep Discovery Inspector appliance 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 > Images.

2. Click Import.

   The Import Image screen appears.

3. Select one of the following image sources and configure the applicable settings.
## Source

<table>
<thead>
<tr>
<th>Source</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Local or network folder | a. Type an image name with a maximum of 260 characters.  
                           b. Click **Connect**.  
                           c. Once connected, import the image using the Virtual Analyzer Image Import Tool.  
                           For details, see *Importing an Image Using the Virtual Analyzer Image Import Tool on page 6-74*.  
                           **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.  
                          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**. |

### Importing an Image Using the Virtual Analyzer Image Import Tool

Virtual Analyzer supports OVA files that are between 1 GB and 20 GB in size.

**Procedure**

1. Before importing, verify that your computer has established a connection to Deep Discovery Inspector.
Go to Administration > Virtual Analyzer > Internal Virtual Analyzer > Status to check the connection status.

2. Go to Administration > Virtual Analyzer > Internal Virtual Analyzer > Images and click Import.

3. For Source, select Local or network folder.

4. Connect to Deep Discovery Inspector.

5. Click Download image import tool.

6. Open the file VirtualAnalyzerImageImportTool.exe.

7. Type the IP address for Deep Discovery Inspector.

Deep Discovery Inspector deploys instances immediately after an image uploads. Wait for the instance deployment to complete.

The image import process may stop or be considered unsuccessful because of the following reasons:

- No connection is 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 added or deleted, or when instances are modified. All instances are also automatically redistributed whenever you add or delete images.

Modify Images

FIGURE 6-18. Modify Images

Modifying Instances

Procedure

1. Go to Administration > Virtual Analyzer > Internal Virtual Analyzer > 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 > 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 with the following extensions:

- .bzip
- .rar
- .tar
- .zip
- .7zip

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 6-69.

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 > Passwords.
2. Under **Archive File Passwords**, type a password.
3. (Optional) Click **Add password**... and type another password.
4. Click **Save**.
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.

See the following topics for details:

- Adding Network Groups on page 6-79
- Adding Registered Domains on page 6-81
- Adding Registered Services on page 6-82

To replicate network configuration settings from one Deep Discovery Inspector appliance to another, export the settings to a file and then import the file to other Deep Discovery Inspector appliances.

For details, see Importing/Exporting Configuration Settings on page 6-84.

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.

Procedure

1. Go to Administration > Network Groups and Assets > Network Groups.
2. Click Add.
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).

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**: fc00::fdff: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: 192.168.1.0/255.255.255.0 or 192.168.1.0/24
- **IPv6** subnet prefix example: fd00:1:1111:200:1000/116
5. Select the **Network zone**.

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 1,000 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`.

---

**Procedure**

1. Go to **Administration > Network Groups and Assets > Registered Domains**.

2. Specify a domain name to be registered.

3. (Optional) Click **Analyze** to display a list of domains that can be added to the list.

---

**Note**

Registered domain names appear in the **Defined Registered Domains** section.
4. Click Add.

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 1,000 services. More than one server may be dedicated to each service.

---

**Procedure**

1. Go to Administration > Network Groups and Assets > Registered Services.
2. Select a service from the drop-down list.

**Table 6-13. Service Types**

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>NETWORK SERVER DESCRIPTION</th>
</tr>
</thead>
</table>
| 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                                   |
## Table: Network Server Description

<table>
<thead>
<tr>
<th>Service</th>
<th>Network Server Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td>Responds to security authentication requests and allows host access to domain resources</td>
</tr>
<tr>
<td></td>
<td>Configure the same server as the Active Directory.</td>
</tr>
<tr>
<td>File Server</td>
<td>Provides a location for shared file access</td>
</tr>
<tr>
<td>FTP</td>
<td>Used as an FTP server</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>Used as an HTTP Proxy server</td>
</tr>
<tr>
<td>Radius Server</td>
<td>Used as the Radius authentication server</td>
</tr>
<tr>
<td>Security Audit Server</td>
<td>Detects vulnerabilities and insecure configurations</td>
</tr>
<tr>
<td>SMTP</td>
<td>Used as an SMTP server</td>
</tr>
<tr>
<td>SMTP Open Relay</td>
<td>Used as an SMTP Open Relay server</td>
</tr>
<tr>
<td>Software Update Server</td>
<td>Used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Responsible for Windows Server Update Services (WSUS)</td>
</tr>
<tr>
<td></td>
<td>• Performs remote deployment</td>
</tr>
<tr>
<td>Web Server</td>
<td>Used as a web server</td>
</tr>
</tbody>
</table>

3. (Optional) Click **Analyze** to display a list of detected services and domains on your network.

4. Specify a server name.

5. Specify an IP address.

### Note

The **Add Registered Services** screen supports IPv4 and IPv6. IP address ranges cannot be specified.

6. Click **Add**.
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 6-158.

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.
Integrated Products/Services

Deep Discovery Inspector integrates with other Trend Micro products and services.

This section includes the following categories:

• Trend Micro Integrated Products/Services on page 6-85
• Service Addresses and Ports on page 6-87
• Control Manager on page 6-90
• Threat Management Services Portal on page 6-95
• Syslog on page 6-99
• Third-Party Products/Services on page 6-102
• Mitigation Products/Services on page 6-131

Trend Micro Integrated Products/Services

For seamless integration, make sure that the products and services that integrate with Deep Discovery Inspector run the required or recommended versions.

Table 6-14. Trend Micro Products and Services that Integrate with Deep Discovery Inspector

<table>
<thead>
<tr>
<th>PRODUCT/ SERVICE</th>
<th>DESCRIPTION</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network VirusWall Enforcer</td>
<td>Regulates network access based on the security posture of endpoints.</td>
<td>• 3.0 with Patch 1 or later</td>
</tr>
<tr>
<td></td>
<td>For details, see Mitigation Products/Services on page 6-131.</td>
<td>• 2.0 Service Pack 1 with Patch 1</td>
</tr>
<tr>
<td>PRODUCT/ SERVICE</td>
<td>DESCRIPTION</td>
<td>VERSION</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Smart Protection Network</td>
<td>Provides Web Reputation Services to determine the reputation of websites that users attempt to access. Smart Protection Network is hosted by Trend Micro. For details, see <em>Smart Protection Technology on page 6-38.</em></td>
<td>Not applicable</td>
</tr>
<tr>
<td>Smart Protection Server</td>
<td>Provides the same Web Reputation Service offered by Smart Protection Network. Smart Protection Server localizes the service to the corporate network to optimize efficiency. For details, see <em>Smart Protection Technology on page 6-38.</em></td>
<td></td>
</tr>
<tr>
<td>Threat Connect</td>
<td>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.</td>
<td>Phase 7 Patch 2</td>
</tr>
<tr>
<td>Threat Management Services Portal</td>
<td>Receives and processes logs from Deep Discovery Inspector to build intelligence about your network. The Threat Management Services Portal generates reports that contain information about the latest threats and your network's overall security posture. For details, see <em>Threat Management Services Portal on page 6-95.</em></td>
<td>2.6 SP2 (for the on-premise edition of Threat Management Services Portal) Not applicable for Trend Micro hosted service</td>
</tr>
</tbody>
</table>
### Product/Service Description

<table>
<thead>
<tr>
<th>Product/Service</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Mitigator</td>
<td>Receives mitigation requests from Deep Discovery Inspector after a threat is detected. Threat Mitigator then notifies the Threat Management Agent installed on a host to run a mitigation task. For details, see Mitigation Products/Services on page 6-131.</td>
<td>2.6 (recommended)</td>
</tr>
<tr>
<td>Trend Micro Control Manager</td>
<td>Provides centralized management to control antivirus and content security programs, regardless of the platform or the physical location of the program. For details, see Control Manager on page 6-90 and the Trend Micro Control Manager Administration Guide.</td>
<td>• 6.0 SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 6.0 SP2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 6.0 SP3</td>
</tr>
<tr>
<td>Trend Micro Deep Discovery Advisor</td>
<td>Provides advanced visualization and investigation tools and collects, aggregates, manages, and analyzes logs into a centralized storage space. For details, see the Deep Discovery Advisor Administrator's Guide.</td>
<td>• 3.0 SP1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3.0</td>
</tr>
<tr>
<td>Trend Micro Deep Discovery Virtual Analyzer</td>
<td>Provides an isolated virtual environment to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.</td>
<td>• 5.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5.1</td>
</tr>
</tbody>
</table>

### 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.
<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Address and Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveUpdate Server</td>
<td>Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.</td>
<td>ddi38p.activeupdate.trendmicro.com/activeupdate:80</td>
<td>Related to product version and region</td>
</tr>
<tr>
<td>Certified Safe Software Service (CSSS)</td>
<td>Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources.</td>
<td>grid-global.trendmicro.com</td>
<td></td>
</tr>
<tr>
<td>Community File Reputation</td>
<td>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.</td>
<td>ddi380en.census.trendmicro.com:80</td>
<td>Related to product version and region</td>
</tr>
<tr>
<td>Customer Licensing Portal</td>
<td>Manages your customer information, subscriptions, and product or service license.</td>
<td>licenseupdate.trendmicro.com:80</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Address and Port</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile App Reputation Service</td>
<td>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.</td>
<td>rest.mars.trendmicro.com:443</td>
<td></td>
</tr>
<tr>
<td>(MARS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Feedback</td>
<td>Shares anonymous 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.</td>
<td>ddi380-en.fbs20.trendmicro.com:443</td>
<td>Related to product version and region</td>
</tr>
<tr>
<td>Threat Connect</td>
<td>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.</td>
<td>ddi38-threatconnect.trendmicro.com/portal/search:443</td>
<td>Related to product version and region</td>
</tr>
</tbody>
</table>
**Threat Management Services Portal**

Receives and processes logs to build intelligence about your network. The Threat Management Services Portal generates reports that contain information about the latest threats and your network's overall security posture.

- **Log Server**: Port 443
- **Status Server**: Port 443
- **SSH**: Port 22

**Notes**: User-defined; no default value

**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.

- **ddi38-en.url.trendmicro.com**: 80

**Related to**: product version and region

---

### Control Manager

Trend Micro Control Manager is a software management solution that simplifies the administration of your corporate antivirus and content security policies. Control Manager 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 on the Control Manager versions compatible with Deep Discovery Inspector, see *Trend Micro Integrated Products/Services on page 6-85.*
For information about managing products using Control Manager, see the *Trend Micro Control Manager Administrator’s Guide*.

Use the **Control Manager** screen on the Deep Discovery Inspector management console to perform the following:

- Verify that Deep Discovery Inspector can register to a Control Manager server.
- Register to a Control Manager server.
- Check the connection status between Deep Discovery Inspector and Control Manager.
- Check the latest Management Communication Protocol Agent (MCP) heartbeat with Control Manager.
- Unregister from a Control Manager server.
- Synchronize suspicious objects with Control Manager.

**Note**

Make sure that both Deep Discovery Inspector and the Control Manager server belong to the same network segment. If Deep Discovery Inspector is not in the same network segment as Control Manager, configure the port forwarding settings for Deep Discovery Inspector.

For details, see *Registering to Control Manager on page 6-92*.

### Control Manager Components

**TABLE 6-16. Control Manager Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager server</td>
<td>The appliance with Control Manager installed This server hosts the web-based Control Manager management console.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Management Communication Protocol (MCP) agent</td>
<td>An application installed with Deep Discovery Inspector that allows Control Manager to manage the product. The agent receives commands from the Control Manager server and applies them to Deep Discovery Inspector. It also collects logs from Deep Discovery Inspector and sends them to Control Manager. The Control Manager MCP agent does not communicate with the Control Manager server directly. It interfaces with a component called the Communicator.</td>
</tr>
<tr>
<td>Entity</td>
<td>A representation of a managed product (such as Deep Discovery Inspector) on the Control Manager console's directory tree. The directory tree includes all managed entities.</td>
</tr>
</tbody>
</table>

### Registering to Control Manager

**Procedure**

1. Go to Administration > Integrated Products/Services > Control Manager.

2. Under **Connection Settings**, specify the name that identifies Deep Discovery Inspector in the Control Manager Product Directory.

   **Note**

   Specify a unique and meaningful name to help you quickly identify Deep Discovery Inspector.

3. Under **Control Manager Server Settings**, do the following:

   a. Type the Control Manager server FQDN or IP address.

   b. **Note**

      The Management Communication Protocol (MCP) agent is an application installed with Deep Discovery Inspector that allows Control Manager to manage the product.
Type the port number that the MCP Agent uses to communicate with Control Manager.

c. (Optional) Select **Connect using HTTPS** if Control Manager security is set to the following levels:

- **Medium**: Trend Micro allows HTTPS and HTTP communication between Control Manager and the MCP agent of managed products.
- **High**: Trend Micro allows only HTTPS communication between Control Manager and the MCP agent of managed products.

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 Control Manager.
- 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 Control Manager connections, select **Connect through a proxy server**.

6. (Optional) Under **Suspicious Object Synchronization**, do the following:

a. Select **Synchronize suspicious objects with Control Manager**.

---

**Attention**

You can only choose to synchronize suspicious objects with one source. If you enable Deep Discovery Inspector to sync with Control Manager, 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 Control Manager.
b. Type an API Key.

**Note**
Log on to Control Manager to obtain an API key.

Deep Discovery Inspector synchronizes suspicious object lists with Control Manager every five minutes, and displays the time of the last synchronization.

7. Click **Test Connection** to verify that Deep Discovery Inspector can connect to the Control Manager server.

8. Click **Register** if a connection was successfully established.

### Unregistering from Control Manager

**Procedure**

1. Go to **Administration > Integrated Products/Services > Control Manager**.

2. Under **Connection Status**, click **Unregister**.

**Note**
Use this option to unregister Deep Discovery Inspector from Control Manager or to register to another Control Manager.

### Managing the Connection with Control Manager

**Procedure**

1. Go to **Administration > Integrated Products/Services > Control Manager**.

2. Under **Connection Status**, perform the following actions:
   a. Verify that the product can connect to Control Manager.
   b. If the product is not connected, restore the connection immediately.
c. **Note**

The Management Communication Protocol (MCP) agent is an application installed with Deep Discovery Inspector that allows Control Manager to manage the product.

Check the MCP heartbeat to verify the last communication between the MCP agent, Deep Discovery Inspector, and the Control Manager server.

3. To update the Control Manager server with changes after registration, click **Update Settings**.

4. To transfer control of Deep Discovery Inspector management to another Control Manager server, click **Unregister** and then register Deep Discovery Inspector to the new Control Manager server.

For details, see *Registering to Control Manager on page 6-92*.

---

**Threat Management Services Portal**

Threat Management Services Portal receives and processes logs to build intelligence about your network.

Threat Management Services Portal generates reports that contain information about the latest threats and your network's overall security posture.

Register Deep Discovery Inspector to Threat Management Services Portal to perform the following operations:

- Analyze the following Deep Discovery Inspector logs and data:
  - Detections
  - Application filters
  - Web Reputation
  - Network groups and assets
- Generate threat reports
Reports contain security threats and suspicious network activities, and recommended preventive and responsive actions. Daily administrative reports enable IT administrators to track the status of threats. Weekly and monthly executive reports keep executives informed about the overall security posture of the organization.

Deep Discovery Inspector sends heartbeat messages to Threat Management Services Portal periodically. A heartbeat message informs Threat Management Services Portal that Deep Discovery Inspector is online.

Deep Discovery Inspector can use proxy server settings configured on the Proxy screen to connect to Threat Management Services Portal.

**Installing Threat Management Services Portal On-premises**

**Procedure**

1. Verify the Threat Management Services Portal versions that are compatible with Deep Discovery Inspector.

   For information about compatible Threat Management Services Portal versions, see *Trend Micro Integrated Products/Services on page 6-85.*

2. Obtain the required information to register Deep Discovery Inspector to Threat Management Services Portal.

   Ask your Trend Micro representative or support provider for the following information:

   - IP address of Threat Management Services Portal log server
   - IP address of Threat Management Services Portal status server
   - Server authentication credentials

3. Install Threat Management Services Portal.

   For installation and configuration instructions, see the *Threat Management Services Portal Administrator’s Guide.*
Registering to Threat Management Services Portal

Procedure

1. Go to Administration > Integrated Products/Services > Threat Management Services Portal.

2. Select Send logs and data to Threat Management Services Portal to register Deep Discovery Inspector to Threat Management Services Portal.

   - To use Threat Management Services Portal as a hosted service, type the IP address or host name.
   - To use Threat Management Services Portal as an on-premises application, type the IP address.

4. Select the protocol.
   - SSH
   - SSL

5. (Optional) If a firewall has been set up, configure the firewall to allow traffic from Deep Discovery Inspector to Threat Management Services Portal, as follows:
   - SSL: Port 443
   - SSH: Port 22

6. (Optional) To use SSH and a Microsoft ISA server, configure the tunnel port ranges on the ISA server to allow traffic from Deep Discovery Inspector to Threat Management Services Portal through port 22.

7. Specify how often to send logs to Threat Management Services Portal.

8. Specify the Threat Management Services Portal status server.
   - To use Threat Management Services Portal as a hosted service, type the IP address or host name.
   - To use Threat Management Services Portal as an on-premises application, type the IP address.
Note

The status server receives the following information from Deep Discovery Inspector:

- Heartbeat: A heartbeat message informs Threat Management Services Portal that Deep Discovery Inspector is online.
- Outbreak Containment Service: A Trend Micro utility that detects both known and unknown malware that can potentially start an outbreak.

9. Specify the server authentication credentials. Threat Management Services Portal authenticates **User name** and **Password** and then accepts logs and data.

10. Type a **Registration email address**.

   **Tip**

   Trend Micro recommends typing your email address.

11. If you have configured proxy settings for Deep Discovery Inspector and want to use these settings for Threat Management Services Portal connections, select **Connect through a proxy server**.

12. Click **Test Connection** to verify that Deep Discovery Inspector can connect to Threat Management Services Portal.

13. Click **Save** if the test connection is successful.

Unregistering from Threat Management Services Portal

Procedure

1. Go to **Administration > Integrated Products/Services > Threat Management Services Portal**.

2. To unregister Deep Discovery Inspector from Threat Management Services Portal, disable **Send logs and data to Threat Management Services Portal**.

3. Do one of the following:
• If Threat Management Services Portal is an on-premises application, manually remove Deep Discovery Inspector from the Threat Management Services Portal Registered Products screen.

• If Threat Management Services Portal is a hosted service, inform your Trend Micro representative about the unregistration.

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.

![Add Syslog Server](image)

**Figure 6-19. Add Syslog Server**

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 6-17. Syslog Severity Levels

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>SEVERITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 0     | Emergency  | • Complete system failure  
Taking immediate action.                                      |
| 1     | Critical   | • Primary system failure  
Taking immediate action.                                      |
| 2     | Alert      | • Urgent failures  
Taking immediate action.                                      |
| 3     | Error      | • Non-urgent failures  
Resolving issues quickly.                                   |
| 4     | Warning    | • Error pending  
Taking 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 HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs.

- **LEEF**

  Log Event Extended Format (LEEF) is a customized event format for IBM® 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**.

---

**Third-Party Products/Services**

To help provide effective detection and blocking at the perimeter, Deep Discovery Inspector can distribute Virtual Analyzer suspicious objects to third-party products and services.

Deep Discovery Inspector integrates with the following third-party inline solutions:

- Check Point Open Platform for Security (OPSEC)
- HP TippingPoint Security Management System (SMS)
- IBM Security Network Protection (XGS)
- Palo Alto Firewalls
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


![Third-Party Products/Services](image)

**Figure 6-20. Install Policies**

2. Type the server name or IP address of your Check Point OPSEC appliance.
Check Point OPSEC SDK only supports IP address suspicious object distribution in the IPv4 address format.

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 third-party product/service, you must accept the **Legal Statement**.

6. On your Check Point firewall appliance, preconfigure a security gateway. For details see *Preconfiguring a Security Gateway on page 6-110*.

7. On the Check Point SmartDashboard console, do the following to configure your Check Point appliance for deploying suspicious objects from Deep Discovery Inspector:

   a. On the **Firewall** tab, go to **Policy**.

   b. To add a rule, click the **Add Rule at the Top** icon.

   c. To configure the new policy, right-click the action.

   d. Change the action to **Accept**.

   e. Click **Install Policy**.
The **Install Policy** window opens.

f. Select the target gateway and click **OK**.
The target gateway installs.

![Installation Process - Standard](image)

**g.** Click **Close**.

The Check Point appliance is enabled to receive suspicious objects from Deep Discovery Inspector.

**8.** On the Deep Discovery Inspector management console, configure the following criteria to send suspicious object information from Deep Discovery Inspector to this third-party product/service:

- **Object type:**
  - C&C Callback Address
  - Suspicious Object

Select **IPv4 address**.
Check Point OPSEC SDK only supports IP address suspicious object distribution in the IPv4 address format.

- **Risk level:**
  - High only
  - High and medium
  - High, medium, and low

9. Under **Advanced Settings**, click 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.

10. Click **Save**.
The **Distribute Now** option appears.

11. (Optional) Click **Distribute Now** to distribute suspicious objects to Check Point immediately.

12. To view suspicious objects distributed by Deep Discovery Inspector on Check Point SmartView Monitor, do the following:
   a. Click the **Launch Menu** icon and go to **Tools > Suspicious Activity Rules**.
The **Enforced Suspicious Activity Rules** window opens.

b. At **Show On**, select the target Check Point appliance name.

c. Click **Close**.

Suspicous objects 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 configure SAM communication mode ports as follows:
   
a. Open the /var/opt/CPsuite-R77/fw1/conf/fwopsec.conf file.
   
b. Configure the following lines:
      
      • sam_server auth_port: 0
      • sam_server port: 18183
c. Restart your Check Point appliance.

HP TippingPoint Security Management System (SMS)

Both Deep Discovery Inspector and Trend Micro Control Manager can send suspicious objects to HP TippingPoint SMS. To align with Control Manager, Deep Discovery Inspector sends each suspicious object with the following optional information:

- Risk level: Severity of each suspicious object or C&C callback attempt
- Product Name: Trend Micro Deep Discovery Inspector (not configurable)
- Appliance Host Name: Trend Micro Deep Discovery Inspector host name (not configurable)

HP TippingPoint Security Management System (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 HP TippingPoint documentation.
Configuring HP TippingPoint Security Management System (SMS)

Procedure


2. Provide the following information:
   - Server name or IP address: Your HP TippingPoint SMS appliance
Note

HP TippingPoint SMS only supports IP address suspicious object distribution in the IPv4 address format.

- User name: Existing authentication credential
- Password: Existing authentication credential

**Table 6-18. Valid Character Sets**

<table>
<thead>
<tr>
<th></th>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>1 character</td>
<td>1 character</td>
</tr>
<tr>
<td>Maximum length</td>
<td>15 characters</td>
<td>15 characters</td>
</tr>
</tbody>
</table>

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 third-party product/service, you must accept the **Legal Statement**.

6. To send object information from Deep Discovery Inspector to this third-party product/service, configure the following criteria:
   - Object type:
     - C&C Callback Address
     - IPv4 address
     - Domain
     - Suspicious Object
     - IPv4 address
• Domain

**Note**
HP TippingPoint SMS only supports IP address suspicious object distribution in the IPv4 address format.

• Risk level:
  • High only
  • High and medium
  • High, medium, and low

7. (Optional) Under **Advanced Settings**, select columns to display in HP TippingPoint SMS.

The following default columns and labels are preselected:

<table>
<thead>
<tr>
<th>Column</th>
<th>Tag Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Host Name</td>
<td>Source</td>
</tr>
<tr>
<td>Risk Level</td>
<td>Severity</td>
</tr>
<tr>
<td>Product Name</td>
<td>Publisher</td>
</tr>
</tbody>
</table>

**Important**
HP TippingPoint only recognizes columns with tag category labels. Make sure that all columns and tag categories configured in Deep Discovery Inspector are configured the same in HP TippingPoint.

8. Specify a tag category name for each column.

Tag category names may include the following:

• Uppercase (A-Z)
• Lowercase (a-z)
• Numeric (0-9)
9. Click **Save**.

10. On the HP TippingPoint SMS console, do the following to add tag category names to the HP reputation database:

   a. Launch HP TippingPoint SMS Client.

   ![Figure 6-21. Profiles (Reputation Database)](image)

   **Figure 6-21. Profiles (Reputation Database)**

   b. On the **Profile** tab, go to **Reputation Database**, select the **Tag Categories** tab, and then click **New**.
The **Create Tag Category** window opens.
c. On the **Create Tag Category** window, configure the following for each tag category:

- **Name**: Type a category name.
  
  Keep the default tag category names (Source, Severity, and Publisher) or add a customized label.

  **Note**
  
  On Deep Discovery Inspector, the default tag categories are Source, Severity, and Publisher.

- **Type**: Select Text.

- **Description**: (Optional) Type a description.

- **Maximum Length**: Type the maximum length of tag category labels.

  **Important**
  
  HP TippingPoint only recognizes columns with tag category labels. Make sure that all columns and tag categories configured in Deep Discovery Inspector are configured the same in HP TippingPoint.

11. Click OK.

The new tag appears in the **Tag Categories** list.

12. (Optional) To view distributed suspicious objects in HP TippingPoint SMS, do the following:

a. On the **Profile** tab, go to **Reputation Database > Search**.
b. On the **Entry Criteria** screen, type search parameters and then click **Search**. Suspicious objects distributed by Deep Discovery Inspector are displayed.

---

**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.
   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
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** > **Third-Party Products/Services** and click **Configuring IBM Security Network Protection (XGS)**.
5. Provide the following information:

   • Server name or IP address: Your IBM XGS appliance

   **Note**
   IBM XGS only supports IP address suspicious object distribution in the IPv4 address format.

   • User name: Existing authentication credential
   • Password: Existing authentication credential
TABLE 6-20. Valid Character Sets

<table>
<thead>
<tr>
<th></th>
<th>USER NAME</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>1 character</td>
<td>1 character</td>
</tr>
<tr>
<td>Maximum length</td>
<td>15 characters</td>
<td>15 characters</td>
</tr>
</tbody>
</table>

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 third-party product/service, you must accept the **Legal Statement**.

9. To send object information from Deep Discovery Inspector to this third-party product/service, configure the following criteria:

   • Object type:
     • C&C Callback Address
       • IPv4 address
       • URL
     • Suspicious Object
       • IPv4 address
       • URL

---

**Note**
IBM XGS only supports IP address suspicious object distribution in the IPv4 address format.

• Risk level:
• High only
• High and medium
• High, medium, and low

10. Click Save.

11. (Optional) On the IBM XGS console, go to Secure Policy Configuration > Security Policies > Active Quarantine Rules to view suspicious objects sent by Deep Discovery Inspector to IBM XGS.

![IBM Security Network Protection](image)

**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 distributed by Deep Discovery Inspector are displayed.
Palo Alto 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 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 Firewalls

Procedure

1. Go to Administration > Integrated Products/Services > Third-Party Products/Services and click Palo Alto Firewalls.
2. Provide the following information:
   - Server name or IP address: Your Palo Alto appliance
Note
Palo Alto products only support IP address suspicious object distribution in the IPv4 address format.

- User name: Existing authentication credential
- Password: Existing authentication credential

Table 6-21. Valid Character Sets

<table>
<thead>
<tr>
<th></th>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>1 character</td>
<td>1 character</td>
</tr>
<tr>
<td>Maximum length</td>
<td>15 characters</td>
<td>15 characters</td>
</tr>
</tbody>
</table>

3. (Optional) Click Test Connection.

The Legal Statement opens.
5. Read and accept the Legal Statement.

Note
To enable integration with this third-party product/service, you must accept the Legal Statement.

6. To send object information from Deep Discovery Inspector to this third-party product/service, configure the following criteria:

- Object type:
  - C&C Callback Address
    - IPv4 address
  - Domain
  - URL
  - Suspicious Object
- IPv4 address
- Domain
- URL

**Note**
Palo Alto products only support IP address suspicious object distribution in the IPv4 address format.

- Risk level:
  - High only
  - High and medium
  - High, medium, and low

7. 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

8. Click **Save**.

9. (Optional) To view suspicious objects sent by Deep Discovery Inspector on the Palo Alto product console, go to **Objects > Custom URL Category**.
Suspicious objects distributed by Deep Discovery Inspector are displayed.

Mitigation Products/Services

Mitigation products and services receive threat information gathered by Deep Discovery Inspector. These products and services work with an agent program installed on an endpoint to resolve threats.

Mitigation products and services that control network access may prevent an endpoint from accessing the network until the endpoint is free of threats.

Enabling/Disabling Mitigation Products/Services Enforcement

Procedure

1. Go to Administration > Integrated Products/Services > Mitigation Products/Services > Registration.

2. Register Deep Discovery Inspector to at least one mitigation product or service.
For details, see Registering to Mitigation Products/Services on page 6-132.

3. Under Mitigation Products/Services Enforcement, enable or disable sending mitigation requests.

Registering to Mitigation Products/Services

Register Deep Discovery Inspector with up to 200 mitigation products and services. For details on versions compatible with Deep Discovery Inspector, see Trend Micro Integrated Products/Services on page 6-85.

Procedure

1. Go to Administration > Integrated Products/Services > Mitigation Products/Services > Registration.

2. Under Mitigation Products/Services Registration, type the mitigation product/service server name or IP address.

3. Type a description for the mitigation product or service.

4. Specify an IP address range.

Note
To save network bandwidth, specify IP address ranges for each mitigation product or service. Deep Discovery Inspector only sends mitigation tasks for specific IP addresses to the mitigation product or service. If the IP address range is empty, all mitigation requests will be sent to the mitigation product or service.

5. Click Register.

The Cleanup Settings screen appears.

6. Select security threat types to send to the mitigation product or service.

7. Click Apply.
Unregistering from Mitigation Products/Services

Procedure

1. Go to Administration > Integrated Products/Services > Mitigation Products/Services > Registration.
2. Under Registered Mitigation Products/Services, select the mitigation products or services to unregister from.
3. Click Delete.

The mitigation product or service is removed from the list and the product or service removes Deep Discovery Inspector from its list of data sources.

Configuring Mitigation Exceptions

You can except IP addresses from mitigation actions. Deep Discovery Inspector still scans these IP addresses but does not send mitigation requests to the mitigation product or service if threats are found.

Before configuring mitigation exceptions, register Deep Discovery Inspector to at least one mitigation product or service. For details, see Enabling/Disabling Mitigation Products/Services Enforcement on page 6-131.

A maximum of 100 entries can be added to the list.

Procedure

1. Go to Administration > Integrated Products/Services > Mitigation Products/Services > Exceptions.
2. Type a name for the exception. Specify a meaningful name for easy identification. Example: "Lab Computers".
3. Specify an IP address or IP address range for exception from mitigation actions. Example: 192.1.1.1-192.253.253.253
4. Click Add.

5. To remove an exception, select the exception and click Delete.

Accounts

This section includes the following topics:

- About Accounts on page 6-134
- User Roles and Menu Item Permissions on page 6-135
- Adding an Account on page 6-139
- Resetting an Account Password on page 6-142
- Deleting an Account on page 6-142

About Accounts

Deep Discovery Inspector allows you to grant access to selected sections of the management console.

Deep Discovery Inspector supports 128 accounts, including the following:

- 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 users who sign on to Deep Discovery Inspector from Trend Micro Control Manager.

### Accounts

<table>
<thead>
<tr>
<th>User Name</th>
<th>Role</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Administrator</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>johnadmin</td>
<td>Administrator</td>
<td>admin(admin)</td>
</tr>
<tr>
<td>user_viewer_37</td>
<td>Viewer</td>
<td>admin</td>
</tr>
<tr>
<td>user_viewer_38</td>
<td>Viewer</td>
<td>admin</td>
</tr>
</tbody>
</table>

**CREATED BY** | **EXAMPLE**
--- | ---
Deep Discovery Inspector system administrator | SYSTEM
Deep Discovery Inspector user name | admin
Trend Micro Control Manager 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 6-22. User Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrator</td>
<td>Accesses all sections of the management console</td>
</tr>
<tr>
<td>ROLE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Administrator</td>
<td>Accesses all sections of the management console</td>
</tr>
<tr>
<td>Viewer</td>
<td>Views detection and system information</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>SECTION</th>
<th>SUBSECTION</th>
<th>SYSTEM ADMINISTRATOR</th>
<th>ADMINISTRATOR</th>
<th>VIEWER</th>
</tr>
</thead>
</table>
| Dashboard| N/A        | Configure            | Configure     | Configure
<p>|          |            |                      |               | Exceptions: Add IP addresses to Network Groups, Registered Domains, and Registered Services |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Subsection</th>
<th>System Administrator</th>
<th>Administrator</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>Affected Hosts</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exceptions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Configure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Add IP addresses to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Groups,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Registered Domains,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and Registered Services</td>
</tr>
<tr>
<td>Hosts with Notable Event Detections</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exceptions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Add IP addresses to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Groups,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Registered Domains,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and Registered Services</td>
</tr>
<tr>
<td>C&amp;C Callback Addresses</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
<td>No access</td>
</tr>
<tr>
<td>Suspicious Objects</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
<td>No access</td>
</tr>
<tr>
<td>Retro Scan</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
<td>View</td>
</tr>
<tr>
<td>All Detections</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Exceptions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Add IP addresses to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Groups,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Registered Domains,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and Registered Services</td>
</tr>
<tr>
<td>Section</td>
<td>Subsection</td>
<td>System Administrator</td>
<td>Administrator</td>
<td>Viewer</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------</td>
<td>----------------------</td>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>Reports</td>
<td>Scheduled Reports</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td></td>
<td>Schedules</td>
<td>Configure</td>
<td>Configure</td>
<td>View</td>
</tr>
<tr>
<td></td>
<td>On-demand Reports</td>
<td>Configure</td>
<td>Configure</td>
<td>View</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
<td>Configure</td>
<td>Configure</td>
<td>View</td>
</tr>
<tr>
<td>Administration</td>
<td>All</td>
<td>Configure</td>
<td>Configure</td>
<td>No access</td>
</tr>
<tr>
<td></td>
<td>Accounts</td>
<td>Configure</td>
<td>Configure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Logs</td>
<td>View</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Maintenance</td>
<td>Configure</td>
<td>Configure</td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>All</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>User Account</td>
<td>Change Password</td>
<td>Configure</td>
<td>Configure</td>
<td>Configure</td>
</tr>
<tr>
<td></td>
<td>Log Off</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
</tbody>
</table>
Adding an Account

Procedure

1. Go to Administration > Accounts.
2. Click Add.
   The Add Account screen appears.
3. Type a user name that contains 4 to 32 alphanumeric characters.

   ![Note]
   The user name can include the following special characters:
   - Underscore (_)
   - Period (.)
   - Hyphen (-)

Deep Discovery Inspector displays the state of each user as follows:
- Online: Green
- Offline: Gray

![Accounts]

---

6-139
4. Configure the account status.
   - **Enabled** (default)
   - **Disabled**

   **Note**
   A user cannot disable their own account.

5. Select a user role.
   - **Viewer** (default)
   - **Administrator**

6. (Optional) For viewer accounts, select **Allow user to mark detections as resolved**.

7. Click **Save**.

   Deep Discovery Inspector adds the account information to the table in the **Accounts** screen and generates a default account password.

---

**What to do next**

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*

---

**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. Configure the account status.
• **Enabled** (default)
• **Disabled**

3. (Optional) To reset a password, 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.*

4. Click on a user name.

   The **Edit Account** screen appears.

5. Select a user role.

   • **Viewer** (default)
   • **Administrator**

6. (Optional) For viewer accounts, select **Allow user to mark detections as resolved**.

7. Click **Save**.

   Deep Discovery Inspector updates the account information in the table in the **Accounts** screen.
Resetting an Account Password

**Note**
The system administrator can reset the password of every account. Other administrators can reset the password of any account except the system administrator account.

**Procedure**

1. Go to Administration > Accounts.

**Important**
Make sure you are targeting the correct account before clicking Reset.

2. 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.

**What to do next**

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 and the logged-on account.

**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. Check the box beside a user name.
3. Click Delete.

Important
Make sure you are targeting the correct account before clicking Delete.

System Settings

Go to Administration > System Settings to configure basic Deep Discovery Inspector settings.

This section includes the following basic settings:

- Network on page 6-143
- Proxy on page 6-144
- SNMP on page 6-145
- HTTPS Certificate on page 6-147
- Configuring Time Options on page 6-150
- Session Timeout on page 6-151

Network

The Network screen enables management of the appliance’s IP address and network interface ports.

Deep Discovery Inspector uses a management port and several data ports. You can view the status of these ports, change the network speed and duplex mode for each of the data ports, and capture packets for debugging and troubleshooting purposes.
Go to Administration > System Settings > Network.

See Configuring the Appliance IP Settings on page 2-11 for details on configuring a dynamic IP address and managing network interface ports.

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 (Threat Management Services Portal, Smart Protection Server, and Control Manager).

Configuring a Proxy Server

Procedure

1. Go to Administration > System Settings > Proxy.
2. Select Use a proxy server for pattern, engine, and license updates.
3. Select HTTP, SOCKS4, or SOCKS5 for the Proxy Protocol.
4. Specify the Server Name or IP address and the Port number.
5. If the proxy server requires authentication, specify a User Name and Password under Proxy Server Authentication.
6. Click Test Connection to verify connection settings.
7. Click Save if the connection was successful.
SNMP

Simple Network Management Protocol (SNMP) is used to manage devices on IP networks.

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

**Procedure**

1. Go to Administration > System Settings > SNMP.
2. Select Send SNMP trap messages to Network Management Station (NMS).
3. Specify the Community Name and NMS IP Address.
4. Click Save.
Configuring SNMP Agent Mode

Note
Deep Discovery Inspector can be monitored from the SNMP Network Management Station.

Procedure

1. Go to Administration > System Settings > SNMP.
2. Select Enable SNMP agent.
3. Specify a System location and System contact.
4. At Accepted Community Name, specify the community name and click Add to >.
   The name is added to the Community Name list.
5. At Accepted Network Management Station, specify an IP Address and click Add to >.
   The IP address is added to the IP Address list.
6. Click Save.
7. (Optional) 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 6-23. HTTPS Certificate Details**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Certificate version number</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Certificate unique identification number</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm used to create the signature</td>
</tr>
<tr>
<td>Issuer</td>
<td>Entity that verified the information and issued the certificate</td>
</tr>
</tbody>
</table>

**Figure 6-22. HTTPS Certificate**
<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid From</td>
<td>Date the certificate is first valid</td>
</tr>
<tr>
<td>Valid To</td>
<td>Certificate expiration date</td>
</tr>
<tr>
<td>Subject</td>
<td>Person or entity identified</td>
</tr>
<tr>
<td>Public Key</td>
<td>The 2048-bit public key used for encryption</td>
</tr>
</tbody>
</table>

### 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:

   ```bash
   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 6-149.

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.
   d. Click Search.

   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.

   • 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. Click **Save**.

---

**Note**

The default management console timeout is 15 minutes.

---

### System Logs

Deep Discovery Inspector maintains system logs that provide summaries of system events, including component updates and appliance restarts.

Logs are stored in the Deep Discovery Inspector database, in the Trend Micro Control Manager database, or on a Syslog server.

Query logs to gather information from log databases. Export queried logs to a .csv file.

For details, see *Querying System Logs on page 6-152*.

### Querying System Logs

Deep Discovery Inspector stores system events and component update results in the system logs.
Deep Discovery Inspector stores system logs in the appliance hard drive.

![System Logs](image)

**Figure 6-23. System Logs**

**Procedure**

1. Go to **Administration > System Logs**.
2. Select a log type.
   - **All**
   - **System Events**
   - **Update Events**

Events display automatically with the following information.

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timestamp</strong></td>
<td>Event date and time</td>
</tr>
<tr>
<td><strong>Log Type</strong></td>
<td>The following options are available:</td>
</tr>
<tr>
<td></td>
<td>- <strong>All</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>System events</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Update events</strong></td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Level</td>
<td>One of the following levels displays:</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td>Outcome</td>
<td>One of the following event results displays:</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failure</td>
</tr>
<tr>
<td>Action By</td>
<td>Activity by account</td>
</tr>
<tr>
<td></td>
<td>Information about the following accounts types may display:</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Inspector user name</td>
</tr>
<tr>
<td></td>
<td>Example: johnadmin</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Inspector system</td>
</tr>
<tr>
<td></td>
<td>Example: SYSTEM</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro Control Manager user name</td>
</tr>
<tr>
<td></td>
<td>Example: admin(admin)</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro Control Manager system</td>
</tr>
<tr>
<td></td>
<td>Example: admin(SYSTEM)</td>
</tr>
<tr>
<td>IP Address</td>
<td>Event IP address</td>
</tr>
<tr>
<td>Description</td>
<td>Event details</td>
</tr>
</tbody>
</table>

3. Specify a period or click the calendar icon to select a specific date and time.
4. Click **Export** to export the system log to a `.csv` file.

---

**System Maintenance**

Go to **System Maintenance** to perform the following operations:

- **Storage Maintenance on page 6-155**
- **Backup / Restore on page 6-158**
- **Power Off / Restart on page 6-161**

**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
• Set up a file purge for Virtual Analyzer
• 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 Querying System Logs on page 6-152.

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 Control Manager. For details, see Syslog on page 6-99 and Registering to Control Manager on page 6-92.

---

### Performing Storage Maintenance

**Procedure**

1. Go to Administration > System Maintenance > Storage Maintenance.


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.
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.

---

**Purging the Virtual Analyzer Queue**

**Procedure**

1. Go to **Administration > System Maintenance > Storage Maintenance**.
2. Under **Virtual Analyzer Queue Purge**, click a purge action.
   - Purge files until queue contains `<type number>` samples
   - Purge queue files older than `<type number>` days
3. Click **Purge**.

---

**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.

Most or all settings of the following screens cannot be backed up:

- Appliance IP Settings
- Control Manager Settings
- Licenses and Activation Codes
- Mitigation Device Settings
- Retro Scan Settings
- Smart Protection Settings in the Web Reputation screen
- Threat Management Services Portal
- Virtual Analyzer Settings
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 backup settings from Deep Discovery Inspector 3.7 to 3.8, advanced filter settings will not be overwritten because they are not a feature of Deep Discovery Inspector 3.7 and are not included in the encrypted file.
- An encrypted file can also be used to replicate settings on another Deep Discovery Inspector.

Backing Up Encrypted 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.

Importing Encrypted File Settings

Procedure
1. Before importing a file, back up the current configurations. For details, see Backing Up Encrypted File Settings on page 6-159.
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 the configuration file.

**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**.

**Important**

After importing the configuration file, Deep Discovery Inspector disables Virtual Analyzer, even if it was enabled in the encrypted file.

6. To manually enable Virtual Analyzer, go to Administration > Virtual Analyzer > Setup.

---

**Restoring Default Settings**

**Procedure**

1. Before restoring settings, back up the current configurations. For details, see *Backing Up Encrypted File Settings on page 6-159*.

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.
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.

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.

The trial license limits some of the available on-screen information for the following widgets:

- All Scanned Traffic
- Malicious Network Activities
- Malicious Scanned Traffic
- Monitored Network Traffic
- Real-time Scanned Traffic
- Virtual Analyzer

Activation Codes

Use a valid Activation Code to enable Deep Discovery Inspector. Deep Discovery Inspector will not be operable until activation is complete.

An Activation Code has 37 characters (including the hyphens) and appears as follows:
If you received a Registration Key instead of an Activation Code, use it to register Deep Discovery Inspector at:

https://olr.trendmicro.com/registration/

A Registration Key has 22 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxx-xxxx-xxxx

After registration, 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 30-day grace period takes effect after the license expires. 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 6-24. License Expiry Reminders**

<table>
<thead>
<tr>
<th>Version</th>
<th>Reminder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trial</td>
<td>Displays when the license expires</td>
</tr>
</tbody>
</table>
The consequences of not upgrading to a fully licensed version are as follows:

**TABLE 6-25. Results of an Expired Deep Discovery Inspector License**

<table>
<thead>
<tr>
<th>Licence Type and Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trial (Expired)</td>
<td>Deep Discovery Inspector disables component updates, scanning, and log transmission to Threat Management Support Portal.</td>
</tr>
<tr>
<td>Fully Licensed (Expired)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Activating or Renewing a Product License**

**Procedure**

1. Go to *Administration* > *License*.
   The *New Activation Code* screen displays.
3. Type the new Activation Code and click *Save*.
   The *Trend Micro License Agreement* displays.
4. Read the license agreement and click *Agree*.
   After Deep Discovery Inspector is activated, the *Setup Guide* is displayed.
5. Follow the steps in the *Setup Guide*. 
6. On the License screen, click **Update Information** to refresh the screen.

The new license details are displayed.

7. (Optional) Detailed license information is also available on the Customer Licensing Portal website. To view, click **View license details online**.


---

**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 **Administration > Help > About**.
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 7-8*
Frequently Asked Questions (FAQs)

Find answers to frequently asked questions in the following topics.

- FAQs - Activation on page 7-2
- FAQs - Configuration on page 7-2
- FAQs - Detections on page 7-4
- FAQs - Documentation on page 7-4
- FAQs - Installation on page 7-4
- FAQs - Upgrade on page 7-5
- FAQs - Virtual Analyzer Image on page 7-6
- FAQs - Widgets on page 7-7

FAQs - Activation

Do I need to activate Deep Discovery Inspector after installation?

Yes. Use a valid Activation Code to enable Deep Discovery Inspector features.

FAQs - Configuration

I typed the wrong password three times when logging on to the Preconfiguration Console. Then, I could no longer log on to the Preconfiguration Console. What should I do?

If you typed the wrong password three consecutive times, Deep Discovery Inspector will lock for 30 seconds before you can try to log on again. Wait for 30 seconds and try again.

How many seconds of inactivity does the Preconfiguration Console accept before logging off?

After 15 minutes of inactivity, Deep Discovery Inspector logs out of the inactive session.
Can I register Deep Discovery Inspector to more than one Control Manager server?

No, you cannot register Deep Discovery Inspector to more than one Control Manager server. For details on registering to a Control Manager server, see Registering to Control Manager in the Deep Discovery Inspector Administrator's Guide.

Will changing the Deep Discovery Inspector IP address prevent it from communicating with the Control Manager server?

Yes, changing the Deep Discovery Inspector IP address through the Preconfiguration Console or management console will cause temporary disconnection (30 seconds). During the time the Management Communication Protocol (MCP) agent disconnects from Control Manager, the MCP agent logs off from Control Manager and then logs on to provide Control Manager with the updated information.

Is there anything that I need to configure in the firewall settings?

If you use Deep Discovery Inspector only for monitoring the network, you do not need to configure the firewall settings. However, if Deep Discovery Inspector connects to the Internet for any of the following, configure the firewall to allow Ports 80, 22 or 443 traffic from Deep Discovery Inspector:

- Threat Management Services Portal
- Reputation Services

I am unable to register to Threat Management Services Portal, what can I do?

Make sure that:

- The Threat Management Services Portal logon details are correct.
- The firewall settings are configured to allow port 22 or 443 traffic.
- The proxy settings are correct.

If the problem persists, consult your support provider.

What can I do when the email notification sent from Deep Discovery Inspector is blocked by our security product as a phishing URL?

This may be due to your network’s security policies. Add Deep Discovery Inspector to your network security product’s Allow List.
FAQs - Detections

Why are there no more Virtual Analyzer detections on the widget or the Log Query screen after Deep Discovery Analyzer or Deep Discovery Advisor reinstalls?

After Deep Discovery Analyzer or Deep Discovery Advisor reinstalls, the API key changes. Change the API key on the Deep Discovery Inspector management console from Administration > Virtual Analyzer > Setup.

FAQs - Documentation

What documentation is available with this version of Deep Discovery Inspector?

This version of Deep Discovery Inspector includes the following documentation:

• Quick Start Card
• Administrator's Guide
• Installation and Deployment Guide
• User's Guide
• Syslog Content Mapping Guide
• Readme
• Online Help

FAQs - Installation

Does Deep Discovery Inspector installation disrupt network traffic?

No. 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.

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 upgrade Deep Discovery Inspector 3.6, 3.7, and 3.8 to Deep Discovery Inspector 3.8 SP1?

Yes. Upgrade by updating the firmware from Deep Discovery Inspector 3.6, 3.7, or 3.8 to Deep Discovery Inspector 3.8 SP1. Next, migrate all configuration settings (if migration was enabled).

**Important**

Clear the browser cache after performing the upgrade. For details, see *Clearing the Browser Cache* in the *Deep Discovery Inspector Administrator's Guide*.

Can I roll back to a previous version after upgrading to Deep Discovery Inspector 3.8 SP1?

No. The rollback function is not supported.

How often should I update Deep Discovery Inspector?

Trend Micro typically releases virus pattern files on a daily basis and recommends updating both the server and clients daily. Preserve the default schedule setting at Administration > Updates > Component Updates > Scheduled to update every two hours.

**By default, where does Deep Discovery Inspector download updated components from?**

By default, Deep Discovery Inspector receives updated components from the Trend Micro ActiveUpdate server. If you want to receive updates from other sources, configure an update source for both scheduled and manual updates.

**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.

Can I upgrade Threat Discovery Appliance 2.6 or Deep Discovery 3.0 to Deep Discovery Inspector 3.8 SP1?

No. You will need to obtain a new license for Deep Discovery Inspector and do a fresh installation.

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 with the image on VirtualBox. Does this affect Virtual Analyzer?

The Found New Hardware wizard automatically runs whenever a Virtual Analyzer 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 by VirtualBox. Attempting to import an image converted by another hypervisor may cause the import to fail.

The OVA is too large to be uploaded into Deep Discovery Inspector. What do I do now?

Make sure that the .ova image is between 1 GB and 20 GB.

The custom Virtual Analyzer import fails. What do I do now?

1. Decompress the .ova image.
2. In the .vbox file, verify the following:
   • The Chipset type is ICH9.
   • The value of "AttachedDevice type" is "HardDisk".
   • The location of "HardDisk" includes only alpha-numeric characters (a-z, A-Z, 0-9). Do not use spaces or special characters.
   • The value of "AttachedDevice port" is "0".
   • The value of "AttachedDevice device" is "0".
   • The license has not been edited.

---

**Note**
If the license is edited when exporting the custom virtual machine, the Virtual Analyzer import will be disrupted.

Virtual Analyzer displays the blue “Cannot find Operating System” screen when powered on using VirtualBox. What do I do now?

Verify the following settings:
   • The Chipset type is **ICH9**
   • IP APIC is enabled
   • TV-x/AMD-V is enabled

**FAQs - Widgets**

Why are widget heights inconsistent, even though Auto-fit is enabled in the Tab Settings?

The Auto-fit function depends on the layout option selected and how many widgets are added. Auto-fit is enabled only when the selected widgets can be arranged one widget per field.
Troubleshooting

This section describes common troubleshooting options available in Deep Discovery Inspector.

- *Slow Management Console Response on page 7-8*
- *Detections on page 7-9*
- *Messages and Alerts on page 7-14*
- *Virtual Analyzer on page 7-15*
- *VirtualBox on page 7-16*
- *Diagnostics on page 7-21*

**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://<DDI IP address>/html/troubleshooting.htm.

2. Under **Real-time Status**, select **System Process (ATOP)**.
The **System Process** screen appears.

![System Process Screen](Image)

**Figure 7-1. System Process (ATOP)**

3. Click **Suspend** and verify system resources real-time.

**Table 7-1. System Resources**

<table>
<thead>
<tr>
<th>Item</th>
<th>Line</th>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>CPU</td>
<td>Idle</td>
<td>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.</td>
</tr>
<tr>
<td>MEM</td>
<td>MEM</td>
<td>Free, cache</td>
<td>The &quot;Free&quot; field indicates available memory. A low number means that there is not enough available memory to complete certain actions.</td>
</tr>
<tr>
<td>Disk</td>
<td>DSK</td>
<td>Busy</td>
<td>A high number indicates that the disk is busy.</td>
</tr>
</tbody>
</table>

**Detections**

- No Detections on Detections Tab on page 7-10
- "Unregistered Service" Server Displays in All Detections Query on page 7-11
No Detections on Detections Tab

No detections appear on the management console Detections tab.

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 Administration > System Settings > Network > Appliance IP Address Settings.

   ![Network Interface Ports Table]

   **Figure 7-2. Appliance IP Address Settings**

   b. Under Network Interface Ports, click the Start button of the data port in use.

   c. Wait 10 seconds and click Stop.

   d. Click View.
The **Packet Capture Information** screen appears.

![Packet Capture Information Screen](image)

**Figure 7-3. Packet Capture Information**

i. In the **Capfile information** section, verify that the data rate matches the real-time traffic rate.

ii. 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.
Make sure that the server has been added to the Registered Services list. For details, see *Adding Registered Services* in the *Deep Discovery Inspector Administrator's Guide*.

**FIGURE 7-4. All Detections Query**

**Procedure**

1. Add the server to the **Registered Services** list.
   
   a. Go to **Administration > Network Groups and Assets > Registered Services**.
The **Registered Services** screen appears.

![Registered Services Screen](image)

**FIGURE 7-5. Registered Services**

b. Under **Add Registered Services**, select service type, specify server name and IP address, and click **Add**.

2. Configure **Registered Domains**.
   
a. Go to **Administration > Network Groups and Assets > Registered Domains**.
   
b. Under **Add Registered Domains**, add your domain.

---

**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 Administrator'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 entities to the Allow List. For details, see *Creating a Custom Allow List* in the *Deep Discovery Inspector Administrator's Guide*.

**Messages and Alerts**

- "Database is Corrupt" Alert Displays on page 7-14
- Rescue Operation Error Message on page 7-14

"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 *Storage Maintenance* in the *Deep Discovery Inspector Administrator's Guide*.

**Note**

After a manual repair, all current data will be lost.

---

**FIGURE 7-6. Database status alert**

**Rescue Operation Error Message**

A Deep Discovery Inspector rescue operation returns an error message with random text.

Remove any USB storage devices connected to Deep Discovery Inspector and try again.
Virtual Analyzer

- **Cannot Upload OVA on page 7-15**
- **No Virtual Analyzer Response to File Submissions on page 7-15**

**Cannot Upload OVA**

The OVA is too large and cannot upload into Deep Discovery Inspector.

The OVA image must be between 1 GB and 20 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 either an external or internal Analyzer.

For details, see Enabling Virtual Analyzer in the Deep Discovery Inspector Administrator's Guide.

b. If the Virtual Analyzer status is "Enabled", reboot 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.

---

**VirtualBox**

- VirtualBox Installation CD/DVD Won't Start on page 7-16
- "Found New Hardware" Wizard in VirtualBox on page 7-18
- Virtual Analyzer Blue Screen in VirtualBox on page 7-18

**VirtualBox Installation CD/DVD Won't Start**

The VirtualBox installation CD/DVD does not automatically start.

Verify items by importing Virtual Analyzer images to VirtualBox.

---

**Procedure**

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer 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 in VirtualBox

During Virtual Analyzer image creation, the Found New Hardware wizard appears along with the image on VirtualBox.

The Found New Hardware wizard automatically runs whenever a Virtual Analyzer 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 by VirtualBox. Attempting to import an image converted by another hypervisor may cause the import to fail.

Virtual Analyzer Blue Screen in VirtualBox

During Virtual Analyzer image creation, Virtual Analyzer displays a blue "Cannot find Operating System" screen when powered on through VirtualBox.
Before importing a custom Virtual Analyzer image to Deep Discovery Inspector, first import the image to VirtualBox.

Procedure

1. On the Oracle VM VirtualBox Manager left panel, click the Virtual Analyzer image to be imported.

2. Click the **Settings** button and select **System**.

![FIGURE 7-9. Motherboard](image)

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.
Diagnostics

For any issue not mentioned, run diagnostics and provide a test result and debug log to your Trend Micro Deep Discovery Inspector support provider.

Procedure

1. To run diagnostics, open the Preconfiguration Console and do the following:
   a. Select 4) System Tasks, and press Enter.
   a. Follow the instructions in Performing a Diagnostic Test in the Deep Discovery Inspector Installation and Deployment Guide.

2. To obtain the debug log:
b. In the left panel, click the **Debug Logs** link.

c. Set the debug level to **Debug** for the related module.

---

**Important**

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. If possible, reproduce the issue.

e. Select the **Export Debug Log** check box and click **Export**.

f. Reset to the original log settings and purge the debug logs.
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*
- *Documentation Feedback on page 8-6*
Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

- Using the Support Portal on page 8-2
- Threat Encyclopedia on page 8-2

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

2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The Technical Support product page appears.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Submit a Support Case from the left navigation and add any relevant details, or submit a support case here:


   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a
comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

**Contacting Trend Micro**

In the United States, Trend Micro representatives are available by phone or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
<th>Phone: +1 (817) 569-8900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Website</th>
<th><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Email address</th>
<th><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></th>
</tr>
</thead>
</table>

- Worldwide support offices:
  

- Trend Micro product documentation:
  
  http://docs.trendmicro.com
Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

- File Reputation Services on page 8-4
- Web Reputation Services on page 8-5
- Email Reputation Services on page 8-5

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:


Record the case number for tracking purposes.
Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:


Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

• Download Center on page 8-5
• TrendLabs on page 8-6

Download Center

Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/
If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

**TrendLabs**

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:


**Documentation Feedback**

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

Appendix A

Create a Custom Virtual Analyzer Image

Learn how to prepare a custom sandbox image from scratch in the following topics:

• VMware to VirtualBox Conversion on page A-2
• Manually Creating a Custom Image Overview on page A-50
VMware to VirtualBox Conversion

Learn how to convert an existing VMware virtual machine image into a VirtualBox image and import it into any supported Trend Micro product.

General steps:

**Procedure**

1. Install required applications.
   
   See *Required Applications on page A-3* for details.

2. Modify the environment of the target VMware image.
   
   See *Modifying the Image Environment on page A-5* for details.

3. Verify and export a target VMware image.
   
   See *Verifying and Exporting VMware Images on page A-14* for details.

4. Convert an existing image to a VirtualBox format.
   
   See *Converting VMware ESXi Images on page A-20* for details.

5. Create a custom image using VirtualBox.
   
   See *Creating a Custom Virtual Analyzer Image on page A-27* for details.

6. Configure a Virtual Analyzer image in VirtualBox.
   
   See *Configuring Virtual Analyzer Images in VirtualBox on page A-40* for details.

7. Package an image as an OVA file.
   
   See *Packaging an Image as an OVA File on page A-45* for details.

8. Import an OVA file.
   
   See *Importing an OVA File on page A-49* for details.
If you encounter any issues, see *Troubleshooting Common Issues on page A-49* for details.

**Required Applications**

The Virtual Analyzer image requires the following necessary applications for threat analysis:

**TABLE A-1. Required Applications**

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ensure that you are properly licensed to virtualize the software then ensure macros are enabled. See <a href="https://support.office.com">https://support.office.com</a> for details.</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Adobe Reader | **Tip**
  Trend Micro recommends installing the version of Adobe Reader that is licensed and is most widely used in your organization.
  To download the most current version of Adobe Reader, go to [http://www.adobe.com/downloads/](http://www.adobe.com/downloads/).

If the image has Adobe Reader installed, see [Preparing Adobe Reader on page A-5](#). If you do not install Adobe Reader, Virtual Analyzer does the following:

- Automatically installs Adobe Reader 8, 9, and 11 on all images
- Uses all three versions during analysis

**WARNING!**
This consumes additional computing resources.

- If the image operating system is Windows XP or Windows Server 2003, install .NET Framework 3.5 (or later).

With these software applications, the custom Virtual Analyzer image returns acceptable detection rates. There is no need to install additional software applications, including VBoxTool, unless advised by a Trend Micro security expert.

**Important**

To prevent the anti-VM functions of some malware, do not install VMware tools on the image.
Preparing Adobe Reader

If Adobe Reader is currently installed on the virtual machine, perform the following steps:

**Procedure**

1. Disable automatic updates to avoid threat simulation issues.
   

2. Install the necessary Adobe Reader language packs so that file samples authored in languages other than those supported in your native Adobe Reader can be processed.

   For example, if you use the English version of Adobe Reader and you expect to analyze objects authored in East Asian languages, install the Asian and Extended Language Pack.

3. Before exporting the image, start Adobe Reader.

   If necessary, read and accept the licensing agreement.

Modifying the Image Environment

Modify a custom Virtual Analyzer image environment to run Virtual Analyzer Sensors, a module used for simulating threats.

Follow the steps for your operating system:

- *Modifying the Image Environment (Windows XP or Windows Server 2003) on page A-6*

- *Modifying the Image Environment (Windows 7/8/8.1 or Windows Server 2008/2008 R2) on page A-8*
Modifying the Image Environment (Windows XP or Windows Server 2003)

Procedure

1. Open a command prompt (cmd.exe) using an account with administrator privileges.

2. Set the logon password for the “Administrator” account to “1111”.
   
   Type `net user "Administrator" 1111`.

3. Configure automatic log on from the “Administrator” account.
   
   Each time the image starts, the logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system.
   
   a. Type the following commands:
      
      • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`
      
      • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f`
      
      • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f`

   b. Restart the image.
No logon prompt is displayed and the “Administrator” account is automatically used to log on.

![Figure A-1. Windows XP Administrator Account](image)

4. View all user accounts.
   Type `net user`

5. Delete non-built-in user accounts one at a time.
   Type `net user "<username>" /delete`.

   For example:
   Type `netsh firewall set opmode mode=DISABLE`.

   **Note**
   Windows Firewall slows down the installation of Virtual Analyzer.

   For details, see *Uninstalling VMware Tools in Windows on page A-12*.

8. Restart the image.

---

**Modifying the Image Environment (Windows 7/8/8.1 or Windows Server 2008/2008 R2)**

**Procedure**

1. Open a command prompt (cmd.exe) using an account with administrator privileges.

2. Enable the “Administrator” account.
   Type `net user "Administrator" /active:yes`.

3. Set the logon password for the “Administrator” account to “1111”.
   Type `net user "Administrator" 1111`.

4. Configure automatic log on from the administrator account.
   Each time the image starts, the logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system.
   a. Type the following commands:
Create a Custom Virtual Analyzer Image

- REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f
- REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f
- REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f

**Note**
In Windows Server 2008/2008 R2, launch the Local Security Policy snap-in (secpol.msc) to disable the **Password must meet complexity requirements** Local Security Setting.

![Local Security Settings](image)

**Figure A-2. Disable Password must meet complexity requirements**

b. Restart the image.
No logon prompt is displayed and the “Administrator” account is automatically used to log on.

**Figure A-3. Windows 7 Administrator Account**

5. View all user accounts.
   
   Type `net user`.

6. Delete non-built-in user accounts one at a time.
   
   Type `net user "<username>" /delete`. 
Create a Custom Virtual Analyzer Image

For example:

```
net user "test" /delete
```

7. Go to Control Panel > AutoPlay.

![Image of AutoPlay settings]

**Figure A-4. AutoPlay**

8. Select Install or run program from your media for Software and games, and then click Save.

   - In Windows 8/8.1, go to Control Panel, type Windows Firewall into the search box, and then click Turn Windows Firewall on or off.
   - In Windows 7 or Windows Server 2008/2008 R2, type `netsh firewall set opmode mode=DISABLE` into the command prompt.

---

**Note**

Windows Firewall slows down the installation of Virtual Analyzer.


For details, see *Uninstalling VMware Tools in Windows* on page A-12.
11. Restart the image.

Uninstalling VMware Tools in Windows

VMware Tools will try to connect to a VMware ESXi host, which might prevent an image from being imported into VirtualBox. Uninstall VMware Tools to help prevent such error.

Procedure

1. Click Start > Control Panel.
   
The Control Panel screen appears.

2. Depending on your operating system, perform one of the following steps:
   - Windows XP or Windows Server 2003: Click Add or Remove Programs.
A list of installed software appears.

**Figure A-5. Add or Remove Programs (Windows XP)**

4. Click **Yes** to uninstall the VMware Tools.

5. When prompted, click **Yes** to restart Windows.

VMware Tools is uninstalled.

**Verifying and Exporting VMware Images**

Before exporting an existing image from a VMware ESXi or Workstation hypervisor, you must verify or modify some settings. After verification, the current image can be exported in order to prepare it for VirtualBox format conversion.

Follow the steps for your environment:

- *Verifying and Exporting a VMware ESXi Image on page A-15*
Verifying and Exporting a VMware ESXi Image

Procedure

1. Shut down the image on the ESXi host.

2. Right-click the Virtual Analyzer image in the left pane, and select **Edit Settings**.

   The **Virtual Machine Properties** screen appears.

3. In the **Virtual Machine Properties** screen, verify the following:

   - Hardware **CD/DVD drive 1**: Device Type is configured as **Client Device**.
   - Hardware **Floppy drive 1**: Device Type is configured as **Client Device**.

---

*Figure A-7. Edit Settings*
4. Select the Virtual Analyzer image in the left pane, and go to File > Export > Export OVF Template.
Create a Custom Virtual Analyzer Image

5. In the Export OVF Template screen, configure the following:
   - **Name**: Type a name for this Virtual Analyzer image.
     (Optional) Click the folder icon to change the path of the OVF template files.
   - **Format**: Select Folder of files (OVF).

   **Note**
   Verify that Include image files attached to floppy and CD/DVD devices in the OVF package is deselected.

6. Click **OK** to export the image.
Verifying and Exporting from VMware Workstation

Procedure

1. Shut down the image on the VMware Workstation.
2. Right-click the Virtual Analyzer image in the left pane, and select Settings. The Virtual Machine Settings screen appears.

**Figure A-10. Virtual Machine Settings**

3. In the Virtual Machine Settings screen, verify the following:

   - Device **CD/DVD (IDE)**: Connection is configured as **Use physical drive**.
   - Device **Floppy**: Connection is configured as **Use physical drive**.
4. In the Virtual Machine Settings screen, click the Options tab and click General in the left pane. Locate the Virtual Machine Disk (*.vmdk) in the Working directory in the right panel.
Converting VMware ESXi Images

The Virtual Machine Disk (*.vmdk) of a VMware ESXi image cannot be added to VirtualBox directly. Use one of the following tools to convert the image format:

- Using QEMU on page A-21
- Using VMware vCenter Converter Standalone on page A-21
Using QEMU

See [http://wiki.qemu.org/Main_Page](http://wiki.qemu.org/Main_Page) for more information about QEMU.

**Procedure**

1. Download the latest version of QEMU from [http://qemu.weilnetz.de/w64/](http://qemu.weilnetz.de/w64/).
2. Install QEMU with the default settings.
3. After installing QEMU, open a command prompt (cmd.exe) using an account with administrator privileges.
4. Convert the Virtual Machine Disk (*.vmdk) from VMware to VirtualBox.

   Type `qemu-img.exe convert [-f fmt] [-O output_fmt] filename output_filename`.

   For example:

   ```
   "C:\Program Files\qemu\qemu-img.exe" convert -f vmdk -O vmdk C:\ESX_xpsp3en_offices_noab.vmdk C:\ESX_xpsp3en_offices_noab_converted.vmdk
   ```

   After conversion, the *.vmdk file can be used to create a new Virtual Analyzer image using VirtualBox.

Using VMware vCenter Converter Standalone

**Procedure**

1. Download VMware vCenter Converter Standalone from [https://my.vmware.com/web/vmware/info/slug/infrastructure_operations_management/vmware_vcenter_converter_standalone/5_5#product_downloads](https://my.vmware.com/web/vmware/info/slug/infrastructure_operations_management/vmware_vcenter_converter_standalone/5_5#product_downloads).

**Note**

VMware vCenter Converter Standalone 5.0 does not support vCenter Server and ESXi versions later than 5.0. Download and install a version later than 5.0.1.
2. After installation, open VMware vCenter Converter Standalone and click **Convert machine** at the top left of the screen.

![VMware vCenter Converter Standalone](image)

**Figure A-13. VMware vCenter Converter Standalone**

The **Conversion** screen appears.

3. In the **Source System** section of the **Conversion** screen, configure the following:
   
a. **Select source type**: Select **VMware Infrastructure virtual machine**.
   
b. **Server**: Type the ESXi server IP address.
   
c. **User name, Password**: Type the credentials that provide administrator access to the VMware server.

4. Click **Next**.
The **Source Machine** section appears.

![Source Machine Image](image)

**Figure A-14. Conversion > Source Machine**

5. In the **Source Machine** section, select the virtual machine that you want to convert and click **Next**.
The **Destination System** section appears.

**Figure A-15. Conversion > Destination System**

6. In the **Destination System** section, configure the following options and then click Next.

   a. **Select destination type**: Choose **VMware Workstation or other VMware virtual machine**.

   b. **Select VMware product**: Choose **VMware Workstation 6.5.x**.

   c. **Name, Location**: Accept the default Virtual Machine name and location or click **Browse** to select a different file.
The **Options** section appears.

![Options section](image)

**Figure A-16. Conversion > Options**

7. In the **Options** section, verify the image description for additional settings and then click **Next**.

Ensure **Install VMware Tools** is set to **No**.

The **Summary** section appears.
**Figure A-17. Conversion > Summary**

8. Verify the image information, and then click **Finish**.
VMware vCenter Converter Standalone starts to convert the Virtual Machine Disk (*.vmdk).

![Image Conversion Progress](image)

**Figure A-18**. Image Conversion Progress

Creating a Custom Virtual Analyzer Image

After preparing the Virtual Machine Disk (*.vmdk), use VirtualBox to create a new VM as your custom Virtual Analyzer image.

In this section, learn how to create a custom Virtual Analyzer image using VirtualBox.

- *Downloading and Installing VirtualBox on page A-28*
- *Using VirtualBox to Create Custom Images on page A-29*
Downloading and Installing VirtualBox

Procedure

1. Download the latest version of VirtualBox from https://www.virtualbox.org/wiki/Downloads.

   Note
   The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

2. Configure the language settings in one of the following ways:
   - Install VirtualBox with English as default.
   - Configure after installation by navigating to File > Preferences > Language, and then selecting English.
Procedure

1. Open VirtualBox.
The **VirtualBox Manager** screen opens.

**FIGURE A-20. VirtualBox Manager**

2. **Click New.**
The **Create Virtual Machine** screen opens.

![Create Virtual Machine](image)

**Figure A-21. Create Virtual Machine**

3. At the **Name and operating system** screen, configure the following and then click **Next**.
   
   a. **Name**: Type a permanent name for the virtual machine.
   
   b. **Type**: Select **Microsoft Windows** as the operating system.
   

---

**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 for installation on virtual appliances you create within the product. You must provide the operating system media and appropriate licensing rights.

The **Memory size** screen appears.

**FIGURE A-22. Memory Size**

4. Specify the amount of memory as follows, and then click **Next**.
   - Windows XP or Windows Server 2003: **512 MB**
Create a Custom Virtual Analyzer Image

The **Hard drive** screen appears.

![Hard drive screen](image)

**Figure A-23. Hard Drive**

5. Select **Do not add a virtual hard drive** and then click **Create**.

The following message appears:

![VirtualBox - Warning](image)

6. Click **Continue**.
VirtualBox Manager creates the virtual machine. The new virtual machine appears in the left pane.

![Newly-created Virtual Machine](image)

**Figure A-24. Newly-created Virtual Machine**

7. In the **VirtualBox Manager** screen, click the **Settings** icon.
The VirtualBox settings display.

**FIGURE A-25. VirtualBox Settings**

8. In **Settings**, click **System**.
The system options display.

![System Options](image)

**Figure A-26. System Options**

9. On the **Motherboard** tab, configure the following:
   a. Chipset: ICH9
   b. Pointing Device: USB Tablet
   c. Extended Features: Enable IO APIC

10. On the **Processor** tab, select **Enable PAE/NX**.

11. On the **Acceleration** tab, select **Enable VT-x/AMD-V** and **Enable Nested Paging**.

12. In **Settings**, click **Storage** to configure the storage controller.
Create a Custom Virtual Analyzer Image

A screen similar to the following appears:

![VirtualBox Settings](sandbox-wimp.png)

a. (Optional) If **Controller: SATA** is under **Storage Tree**, click **Controller: SATA**, and then click ![Remove](remove.png) to remove the default controller.

b. Click **Controller: IDE**, and then click ![Add](add.png).

The following prompt appears:

![VirtualBox Question](question.png)

**FIGURE A-27. Choose Existing Disk**

c. Click **Choose existing disk**, and then navigate to the saved *.vmdk* file that was converted from VMware.

d. Under **Attributes**, keep all default settings.

e. Under **Storage Tree**, select **Controller: IDE**, and then click the optical drive icon to verify that **CD/DVD Drive** is **IDE Secondary Master**.
13. In **Settings**, click **Audio** and deselect the **Enable Audio** checkbox.
14. In **Settings**, click **USB** and select **Enable USB Controller**.

---

**Important**

Do not select **Enable USB 2.0 (EHCI) Controller**.

---

![Enable USB Controller](image-url)

**Figure A-30. Enable USB Controller**

15. In **Settings**, click **Shared Folders** and verify that there are no shared folders.
16. Click OK.

The Settings screen closes and displays the main VirtualBox Manager screen.

17. On the main VirtualBox Manager screen, click to power on the image.

**Configuring Virtual Analyzer Images in VirtualBox**

Reconfigure newly created custom Virtual Analyzer images that were converted from a Virtual Machine Disk (*.vmdk) to ensure that the image runs successfully.

Follow the steps for your operating system:

- *Configuring Virtual Analyzer Images (Windows XP or Windows Server 2003) on page A-41*

Configuring Virtual Analyzer Images (Windows XP or Windows Server 2003)

Procedure

1. On the guest operating system, click **Start**, right-click **My Computer**, and then click **Manage**.

   The **Computer Management** screen appears.

   ![Computer Management](image)

   **Figure A-32. Computer Management**

2. In the **Computer Management** screen, click **Device Manager** in the left pane. Click **Network adapters** in the right pane and ensure the network adapter driver is ready.
3. Open a command prompt (cmd.exe) using an account with administrator privileges.

4. Modify the Windows Registry key to disable the Found New Hardware Wizard.
   • For Windows XP 32-bit, type:
     ```
     reg add "HKEY_LOCAL_MACHINE\Software\Policies\Microsoft \Windows\DeviceInstall\Settings" /v SuppressNewHWUI /t REG_DWORD /d 1 /f
     ```
   • For Windows XP 64-bit or Windows Server 2003, type:
     ```
     reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\PlugPlay\Parameters" /v SuppressUI /t REG_DWORD /d 1 /f
     ```
5. Restart the image, and verify that the Found New Hardware Wizard does not appear.

6. Power off the image.

Configuring Virtual Analyzer Images (Windows 7/8/8.1 or Windows Server 2008/2008 R2)

Procedure

1. On the guest operating system, click **Start**, right-click **Computer**, and then click **Manage**.
The **Computer Management** screen appears.

![Computer Management Screen](image)

**FIGURE A-35. Computer Management**

2. In the **Computer Management** screen, click **Device Manager** in the left pane. Click **Network adapters** in the right pane and ensure the network adapter driver is ready.
Create a Custom Virtual Analyzer Image

FIGURE A-36. Device Management - Network Adapter

3. Power off the image.

Packaging an Image as an OVA File

The custom Virtual Analyzer image contains many files. These files must be packaged as a single OVA file to avoid issues when importing the image into the product.

Important

To successfully complete an image import, the target OVA file size must be between 1 GB and 20 GB.

Procedure

1. Power off the image.
Before exporting the images, verify that the CD/DVD drive is empty.

2. On the VirtualBox main menu, go to **File > Export Appliance**.

   The **Export Virtual Appliance** wizard appears.

![Virtual machines to export](image)

**Figure A-37. Export Virtual Appliance Wizard**

3. Select the custom Virtual Analyzer image, and then click **Next**.
The **Storage settings** screen appears.

![Storage Settings Screen](image)

**FIGURE A-38. Storage Settings**

4. Accept the default **File** name and path or click ![Folder Icon] to select a different file.

5. For **Format**, select **OVF 1.0**.

---

**Note**

Format options include OVF 0.9, 1.0 and 2.0. Your product does not support the OVF 2.0 format.

---

6. Click **Next**.
Important

Ensure that no information is entered in the License field. Your product does not support the Software License Agreement while importing a virtual appliance.

The Export Virtual Appliance screen appears.

![Export Virtual Appliance](image)

**Figure A-39. Export Virtual Appliance - Appliance Settings**

7. Double-click the image description for additional settings, and then click Export.
VirtualBox creates the OVA file.

**Figure A-40. Disk Image Export Progress Bar**

**Importing an OVA File**

Upload an OVA file to a server (HTTP or FTP) before importing into your product. Ensure that the target computer has connectivity to this server. For HTTP servers, your product can connect through secure HTTP.

When an OVA file has been uploaded to a server, perform the following tasks:

- Import the OVA file from the product's management console.
- Configure Virtual Analyzer settings.

**Note**

For details, refer to the documentation that comes with your product.

**Troubleshooting Common Issues**

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>DESCRIPTION/WORKAROUND</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Found New Hardware Wizard</strong> opens with the image on VirtualBox.</td>
<td>The hardware wizard automatically runs whenever a VMware image is converted to a VirtualBox image. Create images using VirtualBox to avoid issues when importing images to Virtual Analyzer.</td>
</tr>
<tr>
<td>ISSUE</td>
<td>DESCRIPTION/WORKAROUND</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------</td>
</tr>
<tr>
<td>The converted <code>.vmdk</code> file displays the blue screen <code>Cannot find Operating System</code> when powered on through VirtualBox.</td>
<td>The chipset <strong>ICH9</strong> must be selected and the IP APIC must be enabled.</td>
</tr>
<tr>
<td>An OVA file experiences problems uploading into your product.</td>
<td>Verify that the OVA file was created from VirtualBox.</td>
</tr>
<tr>
<td>The OVA file is too large and cannot be uploaded.</td>
<td>The OVA file size must be between 1 GB and 20 GB. Try removing unnecessary programs and software on the image and then package the image again as an OVA file.</td>
</tr>
</tbody>
</table>

## Manually Creating a Custom Image Overview

Learn how to manually create a custom Virtual Analyzer image using VirtualBox and import it into Deep Discovery Inspector.

### Procedure

1. Download and install VirtualBox.

   **Note**
   
   The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at [http://www.gnu.org/licenses/old-licenses/gpl-2.0.html](http://www.gnu.org/licenses/old-licenses/gpl-2.0.html).

2. Prepare the operating system installer.

   For details, see *Preparing the Operating System Installer on page A-51*.

3. Manually create a custom image using VirtualBox.

   For details, see *Manually Creating Custom Images on page A-52*.

4. Install required applications.

   For details, see *Required Applications on page A-3*. 
5. Modify the environment of the target VMware image.
   For details, see *Modifying the Image Environment on page A-5*.

6. Package an image as an OVA file.
   For details, see *Packaging an Image as an OVA File on page A-45*.

   For details, see *Importing an OVA File on page A-49*.

---

### Preparing the Operating System Installer

The custom Virtual Analyzer image must run on one of the following operating systems:

- Windows XP
- Windows 7
- Windows 8/8.1
- Windows Server 2003
- Windows Server 2008/2008 R2

---

**Tip**

Trend Micro recommends using the English version of the listed operating systems.

---

**Procedure**


2. Package the installer as an ISO file.

3. Copy the ISO file to the host computer running VirtualBox.
Manually Creating Custom Images

Procedure

1. Open VirtualBox.

Note

The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

The VirtualBox Manager screen opens.

2. Click New.
The **Create Virtual Machine** screen opens.

![Create Virtual Machine Screen](image)

**FIGURE A-42. Create Virtual Machine**

3. At the **Name and operating system** screen, configure the following and then click **Next**.
   a. **Name**: Type a permanent name for the virtual machine.
   b. **Type**: Select **Microsoft Windows** as the operating system.

---

**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 for installation on virtual appliances you create within the product. You must provide the operating system media and appropriate licensing rights.

The Memory size screen appears.

![Memory size screen](image)

**Figure A-43. Memory Size**

4. At the Memory size screen, use the slider to allocate the base memory size for the virtual machine:
   - Windows XP or Windows Server 2003: 512 MB

5. Click **Next**.
The **Hard drive** screen appears.

![Create Virtual Hard Drive Screen](image)

**Figure A-44. Create Virtual Hard Drive**

6. Select **Create a virtual hard drive now** and then click **Create**.
The **Hard drive file type** screen appears.

7. At the **Hard drive file type** screen, select VDI (VirtualBox Disk Image) or VMDK (Virtual Machine Disk) and click **Next**.
The **Storage on physical hard drive** screen appears.

![Create Virtual Hard Drive](image)

**FIGURE A-45. Storage on Physical Hard Drive Window**

8. At the **Storage on physical hard drive** screen, select **Dynamically allocated** and click **Next**.

---

**Note**

If you chose **VMDK (Virtual Machine Disk)** as the hard drive file type, in the **Storage on physical hard drive** screen do not enable **Split into files of less than 2GB**.
The **File location and size** window appears.

![File Location and Size Window](image)

**Figure A-46. File Location and Size Window**

9. (Optional) Click the folder icon to change the path of the virtual disk file.

10. Use the slider to allocate the virtual disk size for the virtual machine.

   - For Windows XP or Windows Server 2003: 15 GB
   - For Windows 7/8/8.1 or Windows Server 2008/2008 R2: 25 GB

11. Click **Create**.
VirtualBox Manager creates the virtual machine. The new virtual machine appears in the left pane.

**Figure A-47. Newly-created Virtual Machine**

12. At the VirtualBox Manager screen, click the **Settings** icon.
The VirtualBox settings appear.

![VirtualBox Settings](image)

**Figure A-48. VirtualBox Settings**

13. In **Settings**, click **System**.
The system options appear.

FIGURE A-49. System Options

14. On the Motherboard tab, configure the following:
   a. Chipset: ICH9
   b. Pointing Device: USB Tablet
   c. Extended Features: Enable IO APIC

15. On the Processor tab, select Enable PAE/NX.

16. On the Acceleration tab, select Enable VT-x/AMD-V and Enable Nested Paging.

17. In Settings, click Storage to configure the storage controller.
A screen similar to the following appears:

![Settings Screen](sandbox-wmp - Settings)

18. (Optional) If **Controller: SATA** is under **Storage Tree**, perform the following steps to remove the SATA controller and add the virtual hard drive to the IDE controller.

   a. Click **Controller: SATA**, and then click ![Remove Controller](remove) to remove the default controller.

   b. Click **Controller: IDE**, and then click ![Add Controller](add).

   The following prompt appears:

   ![VirtualBox Question](VirtualBox - Question)

   **Figure A-50. Choose Existing Disk**

   c. Click **Choose existing disk** and select the corresponding virtual hard drive file (*vdi* or *.vmdk) that was created in the previous steps.

   d. Under **Attributes**, keep all default settings.
Create a Custom Virtual Analyzer Image

e. Under Storage Tree, select Controller: IDE, and then click the optical drive icon to verify that CD/DVD Drive is IDE Secondary Master.

![Figure A-51. IDE Secondary Master](image)

19. Under Storage Tree, click Controller: IDE, and then click the optical drive icon.

20. Under Attributes, click the CD icon (to the right of CD/DVD Drive).

   A file menu appears.

21. Select Choose a virtual CD/DVD disk file... and the ISO file containing the operating system installer.

   The ISO file is available as a device.

22. In Settings, click Audio and deselect the Enable Audio checkbox.
23. In Settings, click USB and select Enable USB Controller.

**Important**
Do not select Enable USB 2.0 (EHCI) Controller.
Figure A-53. Enable USB Controller

24. In Settings, click Shared Folders and verify that there are no shared folders.

Figure A-54. Shared Folders Settings
25. Click **OK**.

   The **Settings** screen closes and the main **VirtualBox Manager** screen appears.

26. On the main **VirtualBox Manager** screen, click **Start** to power on the image.

   The installation process starts.

27. Follow the on-screen instructions to complete the installation.