Deep Discovery Inspector
Service Pack 2
Installation and Deployment Guide
Breakthrough Protection Against APTs and Targeted Attacks
Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at 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:


© 2016 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.: APEM37276/151217

Release Date: January 2016

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>v</td>
</tr>
<tr>
<td>Documentation</td>
<td>vi</td>
</tr>
<tr>
<td>Audience</td>
<td>vii</td>
</tr>
<tr>
<td>Document Conventions</td>
<td>vii</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>1-5</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: About Your System

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Contents</td>
<td>2-2</td>
</tr>
<tr>
<td>The Deep Discovery Inspector Appliance</td>
<td>2-3</td>
</tr>
<tr>
<td>Front Panel</td>
<td>2-3</td>
</tr>
<tr>
<td>Back Panel</td>
<td>2-5</td>
</tr>
<tr>
<td>NIC Indicators</td>
<td>2-9</td>
</tr>
<tr>
<td>Power Indicators</td>
<td>2-14</td>
</tr>
<tr>
<td>Setting Up the Hardware</td>
<td>2-15</td>
</tr>
<tr>
<td>Ports Used by Deep Discovery Inspector</td>
<td>2-16</td>
</tr>
<tr>
<td>Product Specifications</td>
<td>2-21</td>
</tr>
<tr>
<td>Product Specifications - 510/1100 Appliance</td>
<td>2-21</td>
</tr>
<tr>
<td>Product Specifications - 4100 Appliance</td>
<td>2-22</td>
</tr>
</tbody>
</table>
Chapter 3: Deployment

Deployment Overview .................................................................................................. 3-2
Deployment Planning .................................................................................................. 3-2
  Single Port Monitoring .......................................................................................... 3-3
  Multiple Port Monitoring ...................................................................................... 3-5
  Network Tap Monitoring ....................................................................................... 3-5
  Redundant Networks ............................................................................................. 3-7
  VLAN-based Port Monitoring .............................................................................. 3-7
  Remote Port or VLAN Mirroring .......................................................................... 3-8
  Proxy Monitoring .................................................................................................. 3-9
  Mirroring Trunk Links ......................................................................................... 3-10
Installation Requirements ......................................................................................... 3-10
System Requirements .............................................................................................. 3-11

Chapter 4: Installation

Configuring Options .................................................................................................... 4-2
  Setting Security Options for Internet Explorer .................................................. 4-2
  Setting JavaScript Options for Chrome .............................................................. 4-2
  Setting JavaScript Options for Firefox .............................................................. 4-3
  Setting JavaScript Options for Internet Explorer .............................................. 4-3
  Setting Options for Virtual Appliance in ESXi 5.x, or 6.x .............................. 4-4
Deep Discovery Inspector Installation ......................................................................... 4-5
  Installing Deep Discovery Inspector on a Hardware Appliance .................... 4-5
  Installing Deep Discovery Inspector on a Virtual Appliance ......................... 4-12

Chapter 5: Preconfiguration

Preconfiguration Console ............................................................................................ 5-2
  Preconfiguration Console Access ........................................................................ 5-2
Preconfiguration Console Main Menu ...................................................................... 5-6
  Viewing Appliance Information and Status ....................................................... 5-7
  Modifying Device Settings ............................................................................... 5-9
  Modifying Interface Settings ............................................................................. 5-11
Chapter 6: System Tasks

System Tasks Overview ................................................................. 6-2
  Importing the Configuration File ................................................ 6-2
  Exporting the Configuration File .................................................. 6-5
  Importing an HTTPS Certificate .................................................... 6-7
  Performing a Diagnostic Test ....................................................... 6-9
  Performing a Ping Test ............................................................... 6-10
  Restarting Deep Discovery Inspector .......................................... 6-10
  Changing the Root Password ..................................................... 6-12
  Logging Off ................................................................................ 6-13

Chapter 7: Appliance Rescue

About Appliance Rescue ............................................................... 7-2
  Before Rescuing an Appliance ..................................................... 7-2
  Rescuing an Appliance .............................................................. 7-4
  Detaching an iDRAC Virtual Media Device ................................. 7-10

Restoring to Factory Mode .......................................................... 7-10

Chapter 8: Create a New Virtual Appliance

Creating a Virtual Machine in VMware ESXi ................................. 8-2
  Configuring the VMware ESXi Server Network ............................ 8-3
  Enabling Promiscuous Mode in VMware ESXi ............................. 8-9

Installing Deep Discovery Inspector in VMware ESXi ....................... 8-12

Chapter 9: Troubleshoot

Frequently Asked Questions (FAQs) ............................................... 9-2
  FAQs - Activation ...................................................................... 9-2
  FAQs - Configuration ............................................................... 9-2
  FAQs - Detections ..................................................................... 9-4
  FAQs - Documentation ............................................................ 9-4
  FAQs - Installation ................................................................. 9-4
  FAQs - Upgrade ....................................................................... 9-5
  FAQs - Virtual Analyzer Image .................................................... 9-6
  FAQs - Widgets ....................................................................... 9-7
Troubleshooting ......................................................................................................................... 9-7
  Slow Management Console Response .............................................................. 9-8
  Detections .......................................................................................................................... 9-9
  Messages and Alerts ............................................................................................... 9-14
  Virtual Analyzer ........................................................................................................ 9-15
  Virtual Analyzer Images ............................................................................................ 9-16
  Diagnostics ...................................................................................................................... 9-21

Chapter 10: Technical Support

Troubleshooting Resources .......................................................... 10-2
  Contacting Trend Micro ................................................................. 10-3
  Sending Suspicious Content to Trend Micro ...................................... 10-4
  Other Resources ................................................................................................. 10-5

Appendices

Appendix A: Get Started

  Management Console .................................................................... A-2
  Get Started Tasks ........................................................................ A-9
This Installation and Deployment Guide provides information about planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console.

Learn more about the following topics:

• Documentation on page vi
• Audience on page vii
• Document Conventions on page vii
# 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>Installation and Deployment Guide</td>
<td>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>Syslog Content Mapping Guide</td>
<td>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>
<tr>
<td>Readme</td>
<td>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.</td>
</tr>
<tr>
<td>Online Help</td>
<td>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.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>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: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>
View and download product documentation from the Trend Micro Online Help Center:


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>UPPER CASE</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><em>Italics</em></td>
<td>References to other documents</td>
</tr>
<tr>
<td>Monospace</td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td>CONVENTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Navigation &gt; Path</td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
<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 1-5*
• *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 offers a range of product enhancements that improve usability and detection information.

Table 1-1. Deep Discovery Inspector 3.8 SP2 New Features

<table>
<thead>
<tr>
<th>Key Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Description</td>
<td>The new Threat Description field provides additional information about threats, including the Common Threat Family name, protocol and direction.</td>
</tr>
<tr>
<td>Additional detection details</td>
<td>Deep Discovery Inspector provides additional detection details, including the CVE-ID, HTTP referer, and Targeted Attack campaign name.</td>
</tr>
<tr>
<td>FQDN / IP address support</td>
<td>Deep Discovery Inspector supports using the FQDN or IP address for incoming and outgoing network address references, including links in reports and notifications.</td>
</tr>
</tbody>
</table>
Introduction

<table>
<thead>
<tr>
<th><strong>Key Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>New ActiveUpdate components</td>
<td>Deep Discovery Inspector integrates the following new ActiveUpdate components:</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro Intelligence Agent v.2</td>
</tr>
<tr>
<td></td>
<td>• Advanced Persistent Threat Information Pattern</td>
</tr>
<tr>
<td></td>
<td>• C&amp;C Information Pattern v.2</td>
</tr>
<tr>
<td></td>
<td>• Common Vulnerability and Exposure Information Pattern</td>
</tr>
<tr>
<td></td>
<td>• Common Threat Family Information Pattern</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Trusted Certificate Authorities</td>
</tr>
<tr>
<td>KVM virtual appliance support</td>
<td>Deep Discovery Inspector supports operation on KVM virtual appliances.</td>
</tr>
<tr>
<td>Microsoft Edge support</td>
<td>Deep Discovery Inspector supports management console access via Microsoft Edge.</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 1-5*

• *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>
</tbody>
</table>
| High capacity platforms                 | Deep Discovery Inspector features a high-performance architecture that meets the demanding and diverse capacity requirements of large organizations.  
                                        | Deep Discovery Inspector features are useful for a company of any size, and are vital to larger organizations needing to reduce the risk of targeted attacks. |

APT Attack Sequence

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

In targeted attacks, the APT life cycle follows a continuous process of six key phases.
Table 1-3. 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>
<thead>
<tr>
<th><strong>Category</strong></th>
<th><strong>Level</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical</strong></td>
<td>10</td>
<td>Host shows evidence of compromise including but not limited to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data exfiltration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple compromised hosts/servers</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Host exhibits an indication of compromise from APTs including but not limited to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Connection to an IP address associated with a known APT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access to a URL associated with a known APT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A downloaded file associated with a known APT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Evidence of lateral movement</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Host may exhibit the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A high severity network event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Connection to a C&amp;C Server detected by Web Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A downloaded file rated as high risk by Virtual Analyzer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>LEVEL</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Major    | 7     | Host may exhibit the following:  
- Inbound malware downloads; no evidence of user infection  
- An inbound Exploit detection |
|          | 6     | Host may exhibit the following:  
- Connection to a dangerous site detected by Web Reputation Services |
|          | 5     | Host may exhibit the following:  
- A downloaded medium- or low-risk potentially malicious file with no evidence of user infection |
|          | 4     | Host may exhibit the following:  
- A medium severity network event  
- A downloaded file rated as medium risk by Virtual Analyzer |
| Minor    | 3     | Host may exhibit the following:  
- Repeated unsuccessful logon attempts or abnormal patterns of usage  
- A downloaded or propagated packed executable or suspicious file  
- Evidence of running IRC, TOR, or outbound tunneling software |
|          | 2     | Host may exhibit the following:  
- A low severity network event  
- Evidence of receiving an email message that contains a dangerous URL  
- A downloaded file rated as low risk by Virtual Analyzer |
<table>
<thead>
<tr>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivial</td>
<td>1</td>
<td>Host may exhibit the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An informational severity network event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Connection to a site rated as untested or to a new domain detected by Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Evidence of a running disruptive application such as P2P</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 that manages and analyzes objects submitted by integrated products and administrators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

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

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

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.
Chapter 2

About Your System

Learn about the Deep Discovery Inspector appliance in the following topics:

- Package Contents on page 2-2
- The Deep Discovery Inspector Appliance on page 2-3
- Setting Up the Hardware on page 2-15
- Ports Used by Deep Discovery Inspector on page 2-16
- Product Specifications on page 2-21
Package Contents

Examine the Deep Discover Inspector appliance package contents and hardware to correctly configure the appliance in your network.

The following illustration shows the items that are included in the Deep Discovery Inspector appliance package.

![Package Contents Image]

**FIGURE 2-1. Package Contents**

**TABLE 2-1. Deep Discovery Inspector Package Contents**

<table>
<thead>
<tr>
<th>#</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Slide and rail sets (2)</td>
<td>Secure the appliance (fixed mount) or use to secure and allow the appliance to slide in and out of a four-post rack (sliding mount).</td>
</tr>
</tbody>
</table>

**Note**

The rail is assembled with the slide when the package is shipped. Remove the rail from the slide before mounting the appliance.
<table>
<thead>
<tr>
<th>#</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Trend Micro Solutions DVD for Deep Discovery Inspector (1)</td>
<td>The Solutions DVD contains patches, hot fix installers, tools, and the PDF documentation set, including the following:</td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Inspector Quick Start Card</td>
<td>• Trend Micro Deep Discovery Inspector Administrator's Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trend Micro Deep Discovery Inspector Installation and Deployment Guide</td>
</tr>
<tr>
<td></td>
<td></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>
<tr>
<td>3</td>
<td>Power cords (2)</td>
<td>Supply power to the appliance (length is 79 in/200 cm)</td>
</tr>
<tr>
<td>4</td>
<td>Deep Discovery Inspector (1)</td>
<td>The appliance</td>
</tr>
</tbody>
</table>

### The Deep Discovery Inspector Appliance

#### Front Panel

#### Front Panel - 510/1100 Appliance

![Figure 2-2. Deep Discovery Inspector 510/1100 Front Panel](image-url)
TABLE 2-2. 510/1100 Front Panel Features

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power-on indicator</td>
<td>• Lights when the system power is on</td>
</tr>
<tr>
<td></td>
<td>Power button</td>
<td>• Controls the power supply output to the appliance</td>
</tr>
<tr>
<td>2</td>
<td>Appliance ID button</td>
<td>Not supported by Deep Discovery Inspector</td>
</tr>
<tr>
<td>3</td>
<td>Video connector</td>
<td>Connects a VGA display to the appliance</td>
</tr>
<tr>
<td>4</td>
<td>LCD menu buttons</td>
<td>Enable control panel LCD menu navigation</td>
</tr>
<tr>
<td>5</td>
<td>LCD panel</td>
<td>Displays system ID, status information, and system error messages</td>
</tr>
<tr>
<td>6</td>
<td>USB management port</td>
<td>USB 2.0-compliant</td>
</tr>
<tr>
<td>7</td>
<td>Optical drive</td>
<td>DVD +/- RW drive</td>
</tr>
<tr>
<td>8</td>
<td>Hard drives (2)</td>
<td>3.5-inch, hot-swappable</td>
</tr>
<tr>
<td>9</td>
<td>USB 2.0 connector</td>
<td>• Connects USB devices (for example, keyboard or mouse) to the appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• USB 2.0-compliant</td>
</tr>
</tbody>
</table>

Front Panel - 4100 Appliance

Figure 2-3. Deep Discovery Inspector 4100 Front Panel
## Table 2-3. 4100 Front Panel Features

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1  | Power-on indicator / Power button                   | • Lights when the system power is on  
• Controls the power supply output to the appliance |
| 2  | Appliance ID button / appliance status indicator    | Not supported by Deep Discovery Inspector                                    |
| 3  | Video connector                                     | Connects a VGA display to the appliance                                       |
| 4  | LCD menu buttons                                    | Enable control panel LCD menu navigation                                     |
| 5  | LCD panel                                           | Displays system ID, status information, and system error messages            |
| 6  | Hard drives (4)                                     | 2.5-inch, hot-swappable hard drive                                           |
| 7  | USB management port                                 | • Connects to a management network for communication and interaction with other products and services  
• USB 2.0-compliant. |
| 8  | USB 2.0 connector                                   | • Connects USB devices (for example, keyboard or mouse) to the appliance  
• USB 2.0-compliant. |
| 9  | Optical drive                                       | DVD +/- RW drive                                                            |

### Back Panel
Back Panel - 510/1100 Appliance

**Figure 2-4. Deep Discovery Inspector 510/1100 Back Panel**

**Table 2-4. 510/1100 Back Panel Features**

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>USB 3.0 connector</td>
<td>• Connects USB devices (for example, keyboard or mouse) to the appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• USB 3.0-compliant.</td>
</tr>
<tr>
<td>11</td>
<td>RS-232 serial connector</td>
<td>Connects to the serial port of a computer with an RS-232 type connection to perform preconfiguration</td>
</tr>
<tr>
<td>12</td>
<td>Management port</td>
<td>Connects to a management network for communication and interaction with other products and services</td>
</tr>
<tr>
<td>13</td>
<td>iDRAC port</td>
<td>Connects to a dedicated management port on the iDRAC card</td>
</tr>
<tr>
<td>14</td>
<td>Data port 1</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>15</td>
<td>Data port 2</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>16</td>
<td>Data port 3</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>17</td>
<td>Data port 4</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>18</td>
<td>Data port 5</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>#</td>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>19</td>
<td>Power supply connectors (2)</td>
<td>Two 750-watt hot-plug power supply units:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Main power supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Backup power supply</td>
</tr>
</tbody>
</table>

**Note**

"Hot-plug" refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk.

Use the power cord included in the package (for details, see *Package Contents on page 2-2*).

| 20 | Video connector                             | Connects a VGA display to the appliance                                     |
| 21 | Appliance ID button / appliance status indicator | Not supported by Deep Discovery Inspector                                    |
| 22 | USB 2.0 connector                           | • Connects USB devices (for example, keyboard or mouse) to the appliance |
|    |                                             | • USB 2.0-compliant.                                                        |

**Back Panel - 4100 Appliance**

![Figure 2-5. Deep Discovery Inspector 4100 Back Panel](image-url)
<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>USB 3.0 connectors (2)</td>
<td>• Connects USB devices (for example, keyboard or mouse) to the appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• USB 3.0-compliant.</td>
</tr>
<tr>
<td>11</td>
<td>RS-232 serial connector</td>
<td>Connects to the serial port of a computer with an RS-232 type connection to perform preconfiguration</td>
</tr>
<tr>
<td>12</td>
<td>Management port</td>
<td>Connects to a management network for communication and interaction with other products and services</td>
</tr>
<tr>
<td>13</td>
<td>iDRAC port</td>
<td>Connects to a dedicated management port on an iDRAC card</td>
</tr>
<tr>
<td>14</td>
<td>Data port 1</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>15</td>
<td>Data port 2</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>16</td>
<td>Data port 3</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>17</td>
<td>Data port 4</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>18</td>
<td>Data port 5</td>
<td>Integrated 10/100/1000 Mbps NIC connector</td>
</tr>
<tr>
<td>19</td>
<td>Data port 6</td>
<td>10 Gbps NIC connector</td>
</tr>
<tr>
<td>20</td>
<td>Data port 7</td>
<td>10 Gbps NIC connector</td>
</tr>
<tr>
<td>21</td>
<td>Data port 8</td>
<td>10 Gbps NIC connector</td>
</tr>
<tr>
<td>22</td>
<td>Data port 9</td>
<td>10 Gbps NIC connector</td>
</tr>
<tr>
<td>#</td>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>23</td>
<td>Power supply connectors (2)</td>
<td>Two 750-watt hot-plug power supply units:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Main power supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Backup power supply</td>
</tr>
<tr>
<td></td>
<td><img src="note.png" alt="Note" /></td>
<td>&quot;Hot-plug&quot; refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the power cord included in the package (for details, see Package Contents on page 2-2).</td>
</tr>
<tr>
<td>24</td>
<td>Appliance ID button / appliance status indicator</td>
<td>Not supported by Deep Discovery Inspector</td>
</tr>
<tr>
<td>25</td>
<td>Video connector</td>
<td>Connects a VGA display to the appliance</td>
</tr>
</tbody>
</table>

### NIC Indicators

**NIC Indicators - 510/1100**

Deep Discovery Inspector has five user-configurable copper-based Ethernet NIC ports. All accept integrated 10/100/1000 Mbps connectors.

Each port has an indicator showing the current state of the port.
### Table 2-6. NIC Indicator Key: Deep Discovery Inspector 510/1100

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connection status: Port connected/not connected to a valid network</td>
</tr>
<tr>
<td></td>
<td>Data activity status: Network data transmission/reception</td>
</tr>
<tr>
<td>2</td>
<td>Data transmission speed</td>
</tr>
</tbody>
</table>

### Table 2-7. NIC Indicators: Deep Discovery Inspector 510/1100

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>INDICATOR PATTERN</th>
<th>CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Off</td>
<td>No NIC network connection</td>
</tr>
<tr>
<td></td>
<td>Green on</td>
<td>NIC connection to a valid network</td>
</tr>
<tr>
<td></td>
<td>Green flashing</td>
<td>Network data is being sent or received</td>
</tr>
<tr>
<td>2</td>
<td>Yellow</td>
<td>10 Mbps</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>Orange flashing</td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the Identify Adapter button in Intel PROSet to control blinking. For more information, see Intel PROSet Help.</td>
</tr>
</tbody>
</table>

### Table 2-8. NIC Ports and Indicators: Deep Discovery Inspector 510/1100

<table>
<thead>
<tr>
<th>DATA PORT</th>
<th>PORT STYLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data port 1</td>
<td>![Image of data port 1]</td>
</tr>
</tbody>
</table>
**Data Port**

<table>
<thead>
<tr>
<th>Data port 2</th>
<th>Data port 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data port 4</td>
<td>Data port 5</td>
</tr>
</tbody>
</table>

**Port Style**

### NIC Indicators - 4100

The Deep Discovery Inspector 4100 appliance provides the following nine user-configurable, copper-based Ethernet ports:

- Integrated 10/100/100 Mbps (5)
- 10 Gbps (4)

### NIC Indicators - 4100 1 Gbps

Each port has an indicator showing the current state of the port.

**Table 2-9. Indicator Key: Deep Discovery Inspector 4100 1 Gbps**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connection status: Port connected/not connected to a valid network</td>
</tr>
<tr>
<td></td>
<td>Data activity status: Network data is being sent or received</td>
</tr>
<tr>
<td>2</td>
<td>Data transmission speed</td>
</tr>
</tbody>
</table>
TABLE 2-10. NIC Indicators: Deep Discovery Inspector 4100 1 Gbps

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>INDICATOR PATTERN</th>
<th>CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Off</td>
<td>No NIC network connection</td>
</tr>
<tr>
<td></td>
<td>Green on</td>
<td>NIC connection to a valid network</td>
</tr>
<tr>
<td></td>
<td>Green flashing</td>
<td>Network data transmission/reception</td>
</tr>
<tr>
<td>2</td>
<td>Yellow</td>
<td>10 Mbps</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>Orange flashing</td>
<td>Identity</td>
</tr>
</tbody>
</table>

Use the Identify Adapter button in Intel PROSet to control blinking. For more information, see Intel PROSet Help.

TABLE 2-11. NIC Ports and Indicators: Deep Discovery Inspector 4100 1 Gbps

<table>
<thead>
<tr>
<th>DATA PORT</th>
<th>SPEED</th>
<th>PORT STYLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data port 1</td>
<td>10/100/1000 Mbps</td>
<td><img src="image" alt="Port 1/2" /></td>
</tr>
<tr>
<td>Data port 2</td>
<td>10/100/1000 Mbps</td>
<td><img src="image" alt="Port 1/2" /></td>
</tr>
<tr>
<td>Data port 3</td>
<td>10/100/1000 Mbps</td>
<td><img src="image" alt="Port 1/2" /></td>
</tr>
<tr>
<td>Data port 4</td>
<td>10/100/1000 Mbps</td>
<td><img src="image" alt="Port 1/2" /></td>
</tr>
<tr>
<td>Data port 5</td>
<td>10/100/1000 Mbps</td>
<td><img src="image" alt="Port 1/2" /></td>
</tr>
</tbody>
</table>

NIC Indicators - 4100 10 Gbps

Each port has an indicator showing the current state of the port.
### Table 2-12. NIC Indicator Key: Deep Discovery Inspector 4100 10 Gbps

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connection status: Port connected/not connected to a valid network</td>
</tr>
<tr>
<td>2</td>
<td>Data activity status: Network data is being sent or received</td>
</tr>
</tbody>
</table>

### Table 2-13. NIC Indicators: Deep Discovery Inspector 4100 10 Gbps

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Indicator Pattern</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On</td>
<td>NIC connection to a valid network</td>
</tr>
<tr>
<td>2</td>
<td>Green flashing</td>
<td>Network data transmission/reception</td>
</tr>
<tr>
<td>Both 1 and 2</td>
<td>Off</td>
<td>No NIC network connection</td>
</tr>
</tbody>
</table>

### Table 2-14. NIC Ports and Indicators: Deep Discovery Inspector 4100 10 Gbps

<table>
<thead>
<tr>
<th>Data Port</th>
<th>Speed</th>
<th>Port Style</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data port 6</td>
<td>10 Gbps</td>
<td><img src="image.png" alt="Image" /></td>
</tr>
<tr>
<td>Data port 7</td>
<td>10 Gbps</td>
<td><img src="image.png" alt="Image" /></td>
</tr>
<tr>
<td>Data port 8</td>
<td>10 Gbps</td>
<td><img src="image.png" alt="Image" /></td>
</tr>
<tr>
<td>Data port 9</td>
<td>10 Gbps</td>
<td><img src="image.png" alt="Image" /></td>
</tr>
</tbody>
</table>
Power Indicators

Figure 2-6. Power Supply Status Indicators

1: Power supply status indicator/handle

Table 2-15. Power Supply Status Indicators

<table>
<thead>
<tr>
<th>Indicator Pattern</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not lit</td>
<td>Power is not connected</td>
</tr>
<tr>
<td>Green</td>
<td>A valid power source is connected to the power supply and the power supply is operational</td>
</tr>
<tr>
<td>Flashing green</td>
<td>When hot-adding a power supply, indicates the power supply is mismatched with the other power supply (in terms of efficiency, feature set, health status, and supported voltage) Replace the power supply that has the flashing indicator with a power supply that matches the capacity of the other installed power supply.</td>
</tr>
<tr>
<td>INDICATOR PATTERN</td>
<td>CONDITION</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Flashing amber</td>
<td>Indicates a problem with the power supply</td>
</tr>
</tbody>
</table>

**Important**

When correcting a power supply mismatch, replace only the power supply with the flashing indicator. Swapping the opposite power supply to make a matched pair can result in an error condition and an unexpected system shutdown.

To change from a high output configuration to a low output configuration or vice versa, first power down the system.

AC power supplies support both 220 V and 110 V input voltages. When two identical power supplies receive different input voltages, they may output different wattages and trigger a mismatch.

If two power supplies are used, they must be of the same type and have the same maximum output power.

---

**Setting Up the Hardware**

**Procedure**

1. Mount the appliance in a standard 19-inch 4-post rack, or on a free-standing object, such as a sturdy desktop.

   **Note**

   When mounting the appliance, leave at least two inches of clearance on all sides for proper ventilation and cooling.

2. Connect the appliance to a power source.

   Deep Discovery Inspector has two power supply units. One unit acts as the main power supply and the other as a backup.
3. Connect the monitor to the VGA port at the back panel.
   
   See Back Panel on page 2-5 for a diagram.

4. Connect the keyboard and mouse to the USB ports on the back panel.

5. Connect the management port to your network.

6. Power on the appliance.
   
   The power button is found on the front panel of the appliance, behind the bezel.
   
   See Front Panel on page 2-3 for a diagram.

A screen similar to the following appears:

![Power-on self-test (POST)](image)

**Figure 2-7. Power-on self-test (POST)**

**What to do next**

If applicable, perform initial preconfiguration using the Preconfiguration Console. For details, see Preconfiguration on page 5-1.

**Ports Used by Deep Discovery Inspector**

The following table shows the ports that are used with Deep Discovery Inspector and why they are used.
### Table 2-16. Ports used by Deep Discovery Inspector

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Listening and</td>
<td>Deep Discovery Inspector uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outbound</td>
<td>• Connect to the Preconfiguration Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is registered over SSH</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Outbound</td>
<td>Deep Discovery Inspector sends notifications and scheduled reports through SMTP.</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Deep Discovery Inspector uses this port for DNS resolution.</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>Outbound</td>
<td>Deep Discovery Inspector sends requests to the DHCP server if IP addresses are assigned dynamically.</td>
</tr>
<tr>
<td>68</td>
<td>UDP</td>
<td>Listening</td>
<td>Deep Discovery Inspector receives responses from the DHCP server.</td>
</tr>
<tr>
<td><strong>PORT</strong></td>
<td><strong>PROTOCOL</strong></td>
<td><strong>FUNCTION</strong></td>
<td><strong>PURPOSE</strong></td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 80       | TCP          | Listening and outbound            | Deep Discovery Inspector connects to other computers and integrated Trend Micro products and hosted services through this port. In particular, it uses this port to:  
  • Update components by connecting to the ActiveUpdate server  
  • Verify the Deep Discovery Inspector product license through Customer Licensing Portal  
  • Query Community File Reputation Services through Smart Protection Server  
  • Query Web Reputation Services through Smart Protection Network  
  • Connect to the Community File Reputation service for file prevalence when analyzing file samples  
  • Communicate with Trend Micro Control Manager if Deep Discovery Inspector is registered over HTTP |
| 123      | UDP          | Listening and outbound            | Deep Discovery Inspector connects to the NTP server to synchronize time.                       |
| 137      | UDP          | Outbound                          | Deep Discovery Inspector uses NetBIOS to resolve IP addresses to host names.                   |
| 161      | UDP          | Listening and outbound            | Deep Discovery Inspector uses this port for SNMP agent listening and protocol translation.     |
| 162      | UDP          | Outbound                          | Deep Discovery Inspector uses this port to send SNMP trap notifications.                       |
### About Your System

#### PORT | PROTOCOL | FUNCTION | PURPOSE
---|---|---|---
443 | TCP | Listening and outbound | Deep Discovery Inspector uses this port to:

- Access the management console with a computer through HTTPS
- Register to the mitigation server
- Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is using SSL encryption
- Connect to Trend Micro Threat Connect
- Communicate with Trend Micro Control Manager

**Note**

This is the default port. It can be configured through the management console.

- Scan APK files and send detection information to the Mobile App Reputation Service
- Query Mobile App Reputation Service through Smart Protection Server
- Query the Web Reputation Services blocking reason
- Verifies the safety of files through the Certified Safe Software Service
- Share anonymous threat information with the Smart Protection Network
- Send files to Deep Discovery Analyzer for sandbox analysis
<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
</table>
| 514  | UDP      | Outbound | Deep Discovery Inspector sends logs to a syslog server over UDP.  

**Note**  
This is the default port. It can be configured through the management console, and it must match the syslog server. |
| 601  | TCP      | Outbound | Deep Discovery Inspector sends logs to a syslog server over TCP.  

**Note**  
This is the default port. It can be configured through the management console, and it must match the syslog server. |
| 4343 | TCP      | Outbound | Communicate with Smart Protection Server |
| 5274 | TCP      | Outbound | Query Web Reputation Services through Smart Protection Server |
| 8514 | UDP      | Outbound | Deep Discovery Inspector sends syslog information to Deep Discovery Advisor if Deep Discovery Inspector is integrated with Deep Discovery Advisor.  

**Note**  
This is the default port. It can be configured through the management console, and it must match the syslog settings on Deep Discovery Advisor. |
About Your System

Port Protocol Function Purpose
6514 TCP Outbound Deep Discovery Inspector sends logs to a syslog server over TCP with SSL encryption.

Note
This is the default port. It can be configured through the management console, and it must match the syslog server.

Product Specifications

Standard Deep Discovery Inspector appliances have the following specifications.

Contact Trend Micro if the appliance you are using does not meet these hardware specifications.

Note
Hardware vendors and specifications may vary for customers in China, Japan, and other regions.

Product Specifications - 510/1100 Appliance

Table 2-17. Deep Discovery Inspector 510/1100

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack size</td>
<td>1U 19-inch standard rack</td>
</tr>
<tr>
<td>Availability</td>
<td>Raid 1 configuration</td>
</tr>
<tr>
<td>Storage size</td>
<td>2 x 1 TB 3.5-inch SATA</td>
</tr>
<tr>
<td>Feature</td>
<td>Specifications</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Connectivity</td>
<td>• Management: 1 x 1 GB/100/10Base copper</td>
</tr>
<tr>
<td></td>
<td>• Data: 5 x 1 GB/100/10Base copper</td>
</tr>
<tr>
<td>Dimensions (WxDxH)</td>
<td>43.4 cm (17.09 in) x 64.2 cm (25.28 in) x 4.28 cm (1.69 in)</td>
</tr>
<tr>
<td>Maximum weight</td>
<td>19.9 kg (43.87 lb)</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>10°C to 35°C at 10% to 80% relative humidity (RH)</td>
</tr>
<tr>
<td>Power</td>
<td>550W , 100-240 VAC 50/60 HZ</td>
</tr>
</tbody>
</table>

**Product Specifications - 4100 Appliance**

**Table 2-18. Deep Discovery Inspector 4100 Appliance**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack size</td>
<td>2U 19-inch standard rack</td>
</tr>
<tr>
<td>Availability</td>
<td>Raid 10 configuration</td>
</tr>
<tr>
<td>Storage size</td>
<td>4 x 1 TB 3.5-inch SAS</td>
</tr>
<tr>
<td>Connectivity</td>
<td>• Management: 1 x 1 GB/100/10Base copper</td>
</tr>
<tr>
<td></td>
<td>• Data:</td>
</tr>
<tr>
<td></td>
<td>4 x 10 GB SPF+ Direct Attach copper</td>
</tr>
<tr>
<td></td>
<td>5 x 1 GB/100/10Base copper</td>
</tr>
<tr>
<td>Dimensions (WxDxH)</td>
<td>43.4 cm (17.09 in) x 75.58 cm (29.75 in) x 8.73 cm (3.44 in)</td>
</tr>
<tr>
<td>Maximum weight</td>
<td>31.5 kg (69.3 lb)</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>10°C to 35°C at 10% to 80% relative humidity (RH)</td>
</tr>
<tr>
<td>Power</td>
<td>750W , 100-240 VAC 50/60 HZ</td>
</tr>
</tbody>
</table>
Chapter 3

Deployment

Learn tips, suggestions, and requirements for installing Deep Discovery Inspector in the following sections:

• Deployment Overview on page 3-2
• Deployment Planning on page 3-2
• Installation Requirements on page 3-10
Deployment Overview

**Procedure**

1. Plan the deployment.
   
   See *Deployment Planning on page 3-2.*

2. Review the installation requirements.
   
   See *Installation Requirements on page 3-10.*

3. Review the system requirements.
   
   See *System Requirements on page 3-11.*

   
   See *Installation on page 4-1.*

5. Preconfigure Deep Discovery Inspector.
   
   See *Preconfiguration on page 5-1.*

Deployment Planning

Plan how to best deploy Deep Discovery Inspector by doing the following:

- Determine the segments of your network that need protection.
- Plan for network traffic, considering the location of appliances critical to your operations such as email, web, and application servers.
- Determine both the number of appliances needed to meet your security needs and their locations on the network.
- Conduct a pilot deployment on a test segment of your network.
- Redefine your deployment strategy based on the results of the pilot deployment.
• Use the following examples to plan a customized Deep Discovery Inspector deployment.

Single Port Monitoring

The Deep Discovery Inspector data port connects to the mirror port of the core switch, which mirrors the traffic through the port to the firewall.

(Optional) Configure the mirror port to mirror inbound/outbound traffic from single or multiple source ports.

Note
Mirrored traffic should not exceed the capacity of the network interface card.
Figure 3-1. Single Port Monitoring
Multiple Port Monitoring

Deep Discovery Inspector can monitor different network segments using different data ports. Deep Discovery Inspector data ports are connected to the mirror ports of access or distribution switches.

**Figure 3-2. Multiple Port Monitoring**

Network Tap Monitoring

Network taps monitor the data flowing across the network from interconnected switches, routers, and clients. Multiple Deep Discovery Inspector appliances can be connected to a network tap.
Note

If using network taps, make sure that they copy DHCP traffic to Deep Discovery Inspector instead of filtering DHCP traffic.

FIGURE 3-3. Network Tap Monitoring - Single Deep Discovery Inspector
Redundant Networks

Many enterprise environments use redundant networks to provide high availability. When available, an asymmetric route connects Deep Discovery Inspector to redundant switches.

**Figure 3-4. Redundant Network Monitoring**

VLAN-based Port Monitoring

VLAN-based port mirroring allows users to choose to monitor traffic on all ports belonging to a particular VLAN. In this scenario, connect Deep Discovery Inspector to a switch if the mirror configuration is VLAN-based.
Remote Port or VLAN Mirroring

Use remote mirroring in the following conditions:

- Monitoring switches
- Local switches do not have enough physical ports
- Port speed on local switches do not match (GB versus MB)

**Figure 3-5. Remote Port or VLAN Mirroring**

**Note**

In this diagram, the dotted line displays the remote mirror, and the solid line displays the direct mirror.
Proxy Monitoring

When configuring Deep Discovery Inspector in proxy environments outside the proxy server, enable XFF on the proxy server.

To avoid false alarms when configuring Deep Discovery Inspector in proxy environments inside or outside the proxy server, add HTTP Proxy as a registered service on Deep Discovery Inspector.

![Figure 3-6. Proxy Monitoring](image)
Mirroring Trunk Links

When multiple VLANs encapsulate the same physical link, mirror the source port from a trunk link. Make sure that the switch mirrors the correct VLAN tag to Deep Discovery Inspector for both directions.

![Diagram of Mirroring Trunk Links](image)

**Figure 3-7. Mirroring Trunk Links**

### Installation Requirements

Ensure the following before installing Deep Discovery Inspector.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match port speeds</td>
<td>The destination port speed should be the same as the source port speed to ensure equal port mirroring. If the destination port is unable to handle the faster speed of the source port, the destination port may drop some data.</td>
</tr>
</tbody>
</table>
Configure Virtual Analyzer data ports

When enabling an internal Virtual Analyzer, select one of the following network options and make sure the data ports are configured as follows:

- **Isolated Network**
  Virtual Analyzer does not exchange data with the Internet.

- **Specified Network**
  Virtual Analyzer uses an additional specified data port to exchange data with the Internet.

- **Management Network**
  Virtual Analyzer uses a management port to exchange data with the Internet.

For details, see *Internal Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

Monitor all data

Deep Discovery Inspector monitors all inbound and outbound network traffic.

**Note**

For better performance when installing Deep Discovery Inspector, Trend Micro recommends using a plug-in NIC rather than an onboard NIC as a data port.

**Note**

To ensure Deep Discovery Inspector captures traffic from both directions, configure the mirror port, and make sure that traffic in both directions is mirrored to the port.

---

**System Requirements**

Deep Discovery Inspector requires the following:
## Table 3-1. System Requirements

<table>
<thead>
<tr>
<th>Resource</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware host appliance</td>
<td>Trend Micro provides the Deep Discovery Inspector appliance hardware. No other hardware is supported.</td>
</tr>
<tr>
<td>VMware ESXi virtual host appliance</td>
<td>Deep Discovery Inspector supports installation on a VMware ESXi 5.x or 6.x virtual appliance. Trend Micro recommends the following minimum specifications:</td>
</tr>
<tr>
<td></td>
<td>• Virtual disk: 100 GB</td>
</tr>
<tr>
<td></td>
<td>• Virtual CPU cores: 5</td>
</tr>
<tr>
<td></td>
<td>• Virtual memory: 8 GB</td>
</tr>
<tr>
<td></td>
<td>• Virtual NICs: 2</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Trend Micro recommends using the VMXNET 3 network adapter on ESXi 5.5 or later.</td>
</tr>
<tr>
<td>CentOS KVM virtual host appliance</td>
<td>Deep Discovery Inspector supports installation on a CentOS KVM 7.0 or later virtual appliance. Trend Micro recommends the following minimum specifications:</td>
</tr>
<tr>
<td></td>
<td>• Virtual disk: 100 GB</td>
</tr>
<tr>
<td></td>
<td>• Virtual CPU cores: 6</td>
</tr>
<tr>
<td></td>
<td>• Virtual memory: 8 GB</td>
</tr>
<tr>
<td></td>
<td>• Virtual NICs: 2</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Trend Micro recommends using the E1000 network adapter.</td>
</tr>
</tbody>
</table>
### Deployment

<table>
<thead>
<tr>
<th>Resource</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preconfiguration Console</td>
<td>The Deep Discovery Inspector Preconfiguration Console is a</td>
</tr>
<tr>
<td></td>
<td>terminal communications program used to configure the network</td>
</tr>
<tr>
<td></td>
<td>and system settings that are required to access the Deep Discovery</td>
</tr>
<tr>
<td></td>
<td>Inspector management console.</td>
</tr>
<tr>
<td></td>
<td>For details, see <em>Preconfiguration Console on page 5-2</em></td>
</tr>
<tr>
<td></td>
<td>Access to the Preconfiguration Console requires the following:</td>
</tr>
<tr>
<td></td>
<td>• VGA connections:</td>
</tr>
<tr>
<td></td>
<td>• Monitor with a VGA port</td>
</tr>
<tr>
<td></td>
<td>• USB keyboard</td>
</tr>
<tr>
<td></td>
<td>• VGA cable</td>
</tr>
<tr>
<td></td>
<td>• Serial connections:</td>
</tr>
<tr>
<td></td>
<td>• Computer with a serial port</td>
</tr>
<tr>
<td></td>
<td>• RS-232 serial cable</td>
</tr>
<tr>
<td></td>
<td>• Serial communication application (HyperTerminal)</td>
</tr>
<tr>
<td>Management console</td>
<td>Deep Discovery Inspector provides a built-in online management console</td>
</tr>
<tr>
<td></td>
<td>for viewing system status, configuring and viewing threat detections and</td>
</tr>
<tr>
<td></td>
<td>logs, running reports, administering Deep Discovery Inspector, updating</td>
</tr>
<tr>
<td></td>
<td>components, and obtaining help.</td>
</tr>
<tr>
<td></td>
<td>For details, see <em>Management Console</em> in the *Deep Discovery Inspector</td>
</tr>
<tr>
<td></td>
<td>Administrator's Guide*.</td>
</tr>
<tr>
<td></td>
<td>The Deep Discovery Inspector management console supports the following</td>
</tr>
<tr>
<td></td>
<td>web browsers:</td>
</tr>
<tr>
<td></td>
<td>• Google™ Chrome™ 46.0 or later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft™ Internet Explorer™ 10.0 or 11.0</td>
</tr>
<tr>
<td></td>
<td>• Mozilla™ FireFox™ 41.0 or later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft™ Edge</td>
</tr>
<tr>
<td></td>
<td>Adobe™ Flash™ player 8.0 or later</td>
</tr>
<tr>
<td></td>
<td>Recommended resolution rate: 1280x800</td>
</tr>
<tr>
<td>RESOURCE</td>
<td>REQUIREMENT</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Operating system installation media (disk or disk image) for Virtual Analyzer images</td>
<td>Windows operating systems and other Microsoft products are available separately from Microsoft and Microsoft channel partners.</td>
</tr>
</tbody>
</table>

**Important**

Trend Micro does not provide any Microsoft Windows operating systems or Microsoft Office products required for installation on Virtual Analyzer images or sandbox instances you create in Deep Discovery Inspector. You must provide the operating system and Microsoft Office installation media and appropriate licensing rights necessary for you to create any sandboxes.
Chapter 4

Installation

Learn the steps for installing Deep Discovery Inspector as a hardware or virtual appliance in the following sections:

• *Configuring Options on page 4-2*
• *Deep Discovery Inspector Installation on page 4-5*
Configuring Options

Set the following options to enable Deep Discovery Inspector management console navigation.

- Setting Security Options for Internet Explorer on page 4-2
- Setting JavaScript Options for Chrome on page 4-2
- Setting JavaScript Options for Firefox on page 4-3
- Setting JavaScript Options for Internet Explorer on page 4-3
- Setting Options for Virtual Appliance in ESXi 5.x, or 6.x on page 4-4

Setting Security Options for Internet Explorer

Note
For all Internet Explorer versions, make sure that the following options are enabled.

Procedure
1. On the browser, go to the Tools > Internet Options > Security tab.
2. Select the Internet zone and click Custom level....
3. Enable Allow META REFRESH found under Miscellaneous settings.
4. Repeat steps 1-3 for Local intranet and Trusted sites zones.
5. Verify that browser zoom is set to 100%.

Setting JavaScript Options for Chrome

Procedure
1. On the browser, go to Settings.
2. Click **Show advanced settings**....
3. Under **Privacy**, click **Content settings**....
4. Under **JavaScript**, click **Allow all sites to run JavaScript** (recommended).
5. Click **Done**.

---

### Setting JavaScript Options for Firefox

**Procedure**

1. For Firefox versions lower than 23, do the following.
   a. On the browser, go to the **Options > Content** tab.
   b. Verify that **Enable JavaScript** is selected.
   c. Click **OK**.

2. For Firefox version 23 or higher, do the following.
   a. In the address bar, type `about:config` and press Enter.
   b. Click **I’ll be careful, I promise!**.
   c. Verify that the **Value** of **Preference Name javascript.enabled** is set to **true**.

---

### Setting JavaScript Options for Internet Explorer

**Procedure**

1. On the browser, go to the **Tools > Internet Options > Security** tab.

2. Select the **Internet** zone and click **Custom level**....

3. Under **Scripting**, enable **Active scripting**.
4. Click OK.

Setting Options for Virtual Appliance in ESXi 5.x, or 6.x

Procedure

1. On the **vSphere Client** > **Inventory** screen, right-click the appliance name and select **Edit Settings**....

   The settings screen appears.

2. On the **Settings** screen, click the **Options** tab and select **VMware Tools**.

3. Disable the **Synchronize guest time with host** option.

![Virtual Appliance Options](image)

**Figure 4-1. Virtual Appliance Options**
Deep Discovery Inspector Installation

Deep Discovery Inspector is available as a hardware or virtual appliance.

| Hardware appliance | • Trend Micro provides a bare metal server with Deep Discovery Inspector pre-installed.  
|                    | • Trend Micro provides Deep Discovery Inspector packaged as an ISO file on an installation DVD.  
|                    | Install the Deep Discovery Inspector software on a bare metal server that meets the requirements listed in *Installation Requirements on page 3-10*. |
| Virtual appliance  | Install the Deep Discovery Inspector software as a virtual appliance on a bare metal server that meets the requirements listed in *Installation Requirements on page 3-10*.  
|                    | Connect the virtual CD/DVD drive to the installation DVD or the ISO file. |

Installing Deep Discovery Inspector on a Hardware Appliance

**WARNING!**

Back up any pre-existing data on the target hard disk before installing Deep Discovery Inspector. The installation process formats and repartitions the hard disk and removes all existing data.

**Procedure**

1. Using a VGA cable, connect the monitor VGA port to the Deep Discovery Inspector appliance VGA port.

2. Insert the Deep Discovery Inspector installation DVD into the CD/DVD drive.

3. Power on the appliance.
The **BIOS** screen appears.

**Figure 4-2. BIOS**


The **Boot Manager** screen appears.

**Figure 4-3. Boot Manager**
5. Select **BIOS Boot Menu** and press ENTER.

The **BIOS Boot Manager** screen appears.

![BIOS Boot Manager Menu](image)

**Figure 4-4. BIOS Boot Manager Menu**

---

**Note**

When installing Deep Discovery Inspector through a serial connection, press ESC and simultaneously press **SHIFT** and 1 to enter the BIOS Boot Manager.

---

6. Select **TSSTcorp DVD-ROM SN-108BB** and press ENTER.

The **Installation DVD** screen appears.
7. Press ENTER.
   • When installing Deep Discovery Inspector through a serial connection, type `serial` and press ENTER.

The **System Information** screen appears.

---

**Figure 4-5. Deep Discovery Inspector Installation DVD**

---

8. Perform the following tasks:
a. (Optional) To show system information, type 0 and press ENTER.

b. (Optional) Perform a system requirements check.
   - To skip the system requirements check, type 2 and press ENTER.
   - By default, the installer checks system requirements before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.
   - Skip the system requirements check to test the product in a controlled environment before installing it on the network.

c. Start the installation.

   To start installing Deep Discovery Inspector, type 1 and press ENTER.

d. Obtain installation logs.

   To obtain installation logs (used for troubleshooting installation problems), type 3 and press ENTER.

The **Management Port Selection** screen appears.

![Management Port Selection](image)

**FIGURE 4-7. Management Port Selection**
9. Perform the following tasks:
   
a. Verify that the network port status and the actual port status match.
   
   If a status conflict exists, select **Re-detect** and press **ENTER**.
   
b. Select an active link card.
   
   To determine which active link card is connected to the management domain, perform the steps listed on the **Management Port Selection** screen.
   
c. Select an active link card and press **ENTER**.

   Installation continues and completes.

   ![Export Installation Logs]

   **FIGURE 4-8. Export Installation Logs**

10. **Note**

    If you enabled installation log export on the **System Information** screen, a list of storage devices is displayed on the **Export Installation Logs** screen.
To save the exported installation logs, perform the following tasks:

a. Select a storage device and press ENTER.

b. When the installation log file name appears, press ENTER.

Trend Micro recommends saving exported installation logs to sda11.

---

**Note**

Record the file name for future reference.

The file name is in the following format:

*install.log.YYYY-MM-DD-hh-mm-ss*

c. If the preferred device is not listed, verify that it is connected to the appliance by doing the following:

i. Go to **Re-detect**.

ii. Press ENTER to refresh the list.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

11. (Optional) Remove the DVD to prevent reinstallation.


For details, see *Preconfiguration Console on page 5-2.*

---

**Note**

Preconfiguration tasks are identical for both hardware and virtual appliances.
Installing Deep Discovery Inspector on a Virtual Appliance

**WARNING!**
Back up any existing data on the target hard disk before installing Deep Discovery Inspector. The installation process formats and repartitions the hard disk and removes all existing data.

**Important**
You must separately license VMware ESXi and such use is subject to the terms and conditions of the VMware license agreement for that product.

**Procedure**

1. Create a CentOS KVM or VMware ESXi virtual appliance.
   
   For details, see *Create a New Virtual Appliance on page 8-1.*
   
   When installing Deep Discovery Inspector on a VMware ESXi server, disable the snapshot feature for the virtual appliance to preserve hard disk space.

2. Start the virtual machine.

3. Perform the following tasks:
   
   a. Insert the Deep Discovery Inspector installation DVD into the physical CD/DVD drive of the hypervisor server.
   
   b. Connect the virtual CD/DVD drive of the virtual appliance to the physical CD/DVD drive of the hypervisor server.
   
   c. Connect the virtual CD/DVD drive of the virtual appliance to the ISO file.

4. Restart the virtual appliance.

   - On the VMware vSphere Client, go to **Inventory** > **Virtual Machine** > **Guest** > **Send** and press **CTRL+ALT+DEL**.
• On the CentOS KVM server, use an available management tool. For details, see http://www.linux-kvm.org/page/Management_Tools.

The **Installation DVD** screen appears.

---

![Installation DVD Screen](image)

**Figure 4-9. Deep Discovery Inspector Installation DVD**

5. Press ENTER. When installing Deep Discovery Inspector through a serial connection, type **serial** and press ENTER.

The **System Information** screen appears.
6. Perform the following tasks:

a. (Optional) To show system information, type 0 and press ENTER.

b. (Optional) Perform a system requirements check.

To skip the system requirements check, type 2 and press ENTER.

By default, the installer performs a system requirements check before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.

Skip the system requirements check to test the product in a controlled environment before installing it on the network.

c. Start the installation.

To start installing Deep Discovery Inspector, type 1 and press ENTER.

d. Obtain installation logs.

To obtain installation logs (used for troubleshooting installation problems), type 3 and press ENTER.

The Management Port Selection screen appears.
7. Perform the following tasks:

a. Verify that the network port status and the actual port status match.
   
   If a status conflict exists, select **Re-detect** and press ENTER.

b. To determine which active link card is connected to the management domain, perform the steps listed on the **Management Port Selection** screen.

c. Select an active link card and press ENTER.

Installation continues and completes.
8. **Note**

If you enabled installation log export on the **System Information** screen, a list of storage devices is displayed on the **Export Installation Logs** screen.

To save the exported installation logs, perform the following tasks:

a. Select a storage device and press ENTER.

b. When the installation log file name appears, press ENTER.

**Tip**

Trend Micro recommends saving exported installation logs to *sda11*.

**Note**

Record the file name for future reference.

The file name is in the following format:

`install.log.YYYY-MM-DD-hh-mm-ss`
c. If the preferred device is not listed, verify that it is connected to the appliance by doing the following:
   i. Navigate to Re-detect.
   ii. Press ENTER to refresh the list.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

9. (Optional) Remove the DVD to prevent reinstallation.

    For details, see Preconfiguration Console on page 5-2.

---

**Note**

Preconfiguration tasks are identical for both hardware and virtual appliances.
Chapter 5

Preconfiguration

Learn how to use the Preconfiguration Console to configure initial Deep Discovery Inspector settings in the following sections:

• Preconfiguration Console Access on page 5-2
• Preconfiguration Console Main Menu on page 5-6
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.

The Preconfiguration Console also supports recovery operations if the management console is not available.

Use the Preconfiguration Console to do the following:

• Configure initial settings (product IP address and host name)
• Import/export appliance configurations
• Import HTTPS certificates
• Perform a diagnostic test
• Ping the network to verify configuration
• Restart the appliance
• View system logs
• Change the root password

Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

Preconfiguration Console Access

The Deep Discovery Inspector Preconfiguration Console is accessible from a hardware or virtual appliance.

Access the Preconfiguration Console as follows:

• Accessing the Preconfiguration Console with a VGA Port on page 5-3
Tip
Trend Micro recommends accessing the Preconfiguration Console using a monitor with a VGA port.

- Accessing the Preconfiguration Console with a Serial Port on page 5-4

Accessing the Preconfiguration Console with a VGA Port

Procedure
1. Using a VGA cable, connect the monitor VGA port to the appliance VGA port.
2. When the Preconfiguration Console screen opens, type the default password admin and press Enter twice.

Note
To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.
**Accessing the Preconfiguration Console with a Serial Port**

**Procedure**

1. Using an RS-232 serial cable, connect the serial port of the Deep Discovery Inspector appliance to the serial port on a computer.

2. On the computer, open a serial communication application (HyperTerminal).

3. Type the following values if you are accessing the Preconfiguration Console for the first time:
   - Bits per second: **115200**
   - Data bits: **8**
   - Parity: **None**
   - Stop bits: **1**
   - Flow control: **None**
Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

4. When the Preconfiguration Console screen appears, type the default password `admin` and press Enter twice.
Preconfiguration Console Main Menu

The Preconfiguration Console main menu displays the following menu items:

**TABLE 5-1. Main Menu Items**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) <strong>Device Information and Status</strong></td>
<td>View information about Deep Discovery Inspector and monitor memory usage.</td>
</tr>
<tr>
<td>2) <strong>Device Settings</strong></td>
<td>Modify the Deep Discovery Inspector IP address, subnet mask, network default gateway address, and DNS servers.</td>
</tr>
<tr>
<td>3) <strong>Interface Settings</strong></td>
<td>View the network speed and duplex mode for the management port, automatically detected by Deep Discovery Inspector.</td>
</tr>
<tr>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4) System Tasks</td>
<td>Configure the following:</td>
</tr>
<tr>
<td></td>
<td>• Perform a diagnostic test, or restart the product.</td>
</tr>
<tr>
<td></td>
<td>• Import or export the configuration file and import the HTTPS certificate.</td>
</tr>
<tr>
<td></td>
<td>• Ping a server in the same subnet.</td>
</tr>
<tr>
<td>5) Change Password</td>
<td>Change the root password.</td>
</tr>
<tr>
<td>6) Log Off with Saving</td>
<td>Log off from the Preconfiguration Console after saving changes.</td>
</tr>
<tr>
<td>7) Log Off without Saving</td>
<td>Log off from the Preconfiguration Console without saving changes.</td>
</tr>
</tbody>
</table>

To access a menu item, type the number for the menu item and then press Enter.

**Viewing Appliance Information and Status**

Use the **Device Information & Status** screen to view the product name, version, and memory usage.

**Note**

View memory usage information on the Deep Discovery Inspector management console. Go to Dashboard > System Status.

For details, see System Status in the Deep Discovery Inspector Administrator's Guide.

**Procedure**

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type 4 to select **Device Information & Status** and press Enter.
**Note**

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

The **Device Information and Status** screen appears.

![Device Information and Status](image)

**FIGURE 5-4. Device Information and Status**

3. Press Enter to return to the main menu.
Modifying Device Settings

Use the **Device Settings** screen to configure the management IP address settings.

**Note**

These tasks can also be performed on the management console.

**Procedure**

1. Log on to the Preconfiguration Console.
   
   The **Main Menu** appears.

2. To select **Device Settings**, type `2` and press ENTER.
To enter data when using a serial communication application (for example, HyperTerminal), disable the scroll lock function on your keyboard.

The **Device Settings** screen appears.

3. In the **Type** field, use the space bar to select one of the following properties:
   - **dynamic**
   - **static**

4. Configure the following IPv4 address settings:
   a. In the **IP address** field, type an IPv4 address.
      Type a **Subnet mask**.
   b. Type a **Gateway** IP address.
   c. Type a **Primary** and **Secondary DNS server** IP address.

5. (Optional) Configure the following IPv6 address settings:
   a. In the **Enable** field, select **yes**.
   b. In the **IP address** field, type an IPv6 address.
      Type a **Subnet prefix**.
   c. Type a **Gateway** IP address.
   d. Type a **DNS server** IP address.

6. (Optional) Type a VLAN ID.

   **Note**
   The VLAN ID is used when a trunk connection is required between the Deep Discovery Inspector management port and a switch. The VLAN ID is used as a VLAN tag in 802.1Q Ethernet frame.

7. Go to **Return to main menu** and press ENTER.
8. To save the settings, type 6 and press ENTER.

Modifying Interface Settings

By default, Deep Discovery Inspector automatically detects the network speed and duplex mode for the management port. These settings may be manually configured.

Tip
To maximize throughput, Trend Micro recommends full-duplex mode. Half-duplex is acceptable, but network throughput may be limited by transmission delays.

Note
Deep Discovery Inspector data ports can be managed from the management console. Go to Administration > System Settings > Network. For details, see Network in the Deep Discovery Inspector Administrator’s Guide.
Procedure

1. Log on to the Preconfiguration Console.
   The Main Menu appears.

2. Type 3 to select Interface Settings and press ENTER.

   Note
   To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

   The Interface Settings screen appears.

3. To change the interface settings, perform the following tasks:
   a. Type 1 and press ENTER.
   b. In the Speed and Duplex fields, use the space bar to change the network speed and duplex mode.
   c. Navigate to Return to main menu and press ENTER.

4. Type 2 and press ENTER to return to the main menu.

5. Type 6 and press ENTER to save the settings.
Chapter 6

System Tasks

Learn how to perform system tasks on the Preconfiguration Console in the following topics:

- Importing the Configuration File on page 6-2
- Exporting the Configuration File on page 6-5
- Importing an HTTPS Certificate on page 6-7
- Performing a Diagnostic Test on page 6-9
- Performing a Ping Test on page 6-10
- Restarting Deep Discovery Inspector on page 6-10
- Changing the Root Password on page 6-12
- Logging Off on page 6-13
System Tasks Overview

Use the **System Tasks** screen to perform the following system tasks.

---

**Tip**

You can also import and export a configuration file from the management console.

---

**Importing the Configuration File**

If Deep Discovery Inspector encounters errors with the current settings, restore the configuration and database from a backup file.

---

**WARNING!**

Export the current configuration settings before importing the backup configuration file. For details, see *Exporting the Configuration File on page 6-5.*
**Note**

The following steps are for HyperTerminal only. Other serial communication applications can be used, but the steps may be different.

---

**Procedure**

1. Log on to the Preconfiguration Console.

   The **Main Menu** appears.

2. Type **4** and press Enter.

   The **System Tasks** screen appears.

3. Type **1** and press Enter.

   The **Import configuration file** screen appears.

4. On the HyperTerminal console, go to **Transfer > Send File** to send the configuration file to Deep Discovery Inspector before importing.
5. Browse to the configuration file to be imported.

6. Change the protocol to **Kermit** and click **Send**.
Deep Discovery Inspector imports and applies the settings from the configuration file.

### Exporting the Configuration File

Back up the configuration files regularly.

**Note**

The following steps are for HyperTerminal only. Other serial communication applications can be used, but the steps may be different.

**Procedure**

1. Log on to the Preconfiguration Console.
   
   The **Main Menu** appears.

2. Type 4 and press Enter.
   
   The **System Tasks** screen appears.

3. Type 2 and press Enter.
   
   The **Export configuration file** screen appears.
4. On the HyperTerminal console, go to **Transfer > Receive File**.

![Image of HyperTerminal console showing Transfer > Receive File]

**Figure 6-5. Receive File Options**

The **Receive File** window opens.

![Image of Receive File window]

**Figure 6-6. Receive File**

5. Browse to the configuration file to be exported.

6. Change the protocol to **Kermit**, and then click **Receive**.
Deep Discovery Inspector exports the configuration settings to a `config.dat` file.

![Kermit File Receive for Serial Connection](image)

**FIGURE 6-7. Kermit File Receive for Serial Connection**

7. Rename the exported configuration files for proper version control.

---

**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.

Deep Discovery Inspector supports the following HTTPS formats:

- X509 PEM

---

**Note**

For details on generating an HTTPS certificate, see *Generating an HTTPS Certificate* in the *Deep Discovery Inspector Administrator’s Guide*.

---

**Note**

The following steps are for HyperTerminal only. Other serial communication applications can be used, but the steps may be different.
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. Log on to the Preconfiguration Console.
   The **Main Menu** appears.

3. Type **4** and press Enter.
   The **System Tasks** screen appears.

4. Type **3** and press ENTER.
   The **Import HTTPS certificate** screen appears.

   ![Kermit file receive for Serial Connection](image)

   **Figure 6-8. Import HTTPS Certificate**

5. From the HyperTerminal menu, click **Transfer > Send File**.

6. Browse to the HTTPS certificate file to be imported.

7. Change the **Protocol** to **Kermit** and click **Send**.
Performing a Diagnostic Test

Run a diagnostic test on Deep Discovery Inspector to capture and view a log of hardware and software status and events.

Procedure

1. Log on to the Preconfiguration Console.

   The Main Menu appears.

2. Type 4 and press Enter.

   The System Tasks screen appears.

3. Type 4 and press Enter.

   The Diagnostic Test screen appears.

4. On the HyperTerminal console, go to Transfer > Capture Text.

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

5. Browse to the folder and specify a file name for the log.

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

6. Click Start.

   This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

7. Under Run diagnostic test now?, go to OK and press Enter.
While the diagnostic test runs, Deep Discovery Inspector displays log entries on the console.

After the diagnostic test finishes, Deep Discovery Inspector generates a summary log report, and automatically restarts.

8. After Deep Discovery Inspector restarts, open the log summary report to view the results.

Performing a Ping Test

Use a Ping test to verify network configuration.

Procedure

1. Log on to the Preconfiguration Console.
   
   The Main Menu appears.
   
2. Type 4 and press Enter.
   
   The System Tasks screen appears.
   
3. Type 6 and press Enter.
   
   The Ping Test screen appears.
   
4. Input the server IP address and press Ping.
   
   Ping test results appear on the screen.
   
5. Press Esc to return to the main menu.

Restarting Deep Discovery Inspector

To restart Deep Discovery Inspector, access the Preconfiguration Console using a serial communication application (for example, HyperTerminal). Using Deep Discovery Inspector to access the Preconfiguration Console allows you to restart the appliance remotely.
When Deep Discovery Inspector starts, it verifies the integrity of its configuration files. The management console password may reset if the configuration file containing password information is corrupted. If management console logon is unsuccessful when using the preferred password, log on using the default password admin.

---

**Procedure**

1. Log on to the Preconfiguration Console.
   
   The **Main Menu** appears.

2. Type 4 and press Enter.
   
   The **System Tasks** screen appears.

3. Type 5 and press Enter.
   
   The **Restart System** screen appears.


---

![Restart System](image)

**Figure 6-9. Restart System**
Deep Discovery Inspector restarts.

---

**Changing the Root Password**

![Change Password](image)

**Figure 6-10. Change Password**

**Procedure**

1. Log on to the Preconfiguration Console.
   
   The **Main Menu** appears.

2. Type 5 and press Enter.
   
   The **Change Password** screen appears.

3. Type the old and new passwords.

4. Confirm the new password.
5. Go to **Return to main menu** and press Enter to return to the main menu and save the settings.

---

**Logging Off**

Log off from the Preconfiguration Console with or without saving.

---

**Procedure**

1. After changing the configuration settings, return to the main menu.

2. Select one of the following logoff options:
   - To save the changes, type **6** and press ENTER.
   - To exit without saving the changes, type **7** and press ENTER.

3. Navigate to **OK** and press ENTER.
Chapter 7

Appliance Rescue

If Deep Discovery Inspector files become corrupted, learn how to rescue the Deep Discovery Inspector appliance in the following topics:

- *About Appliance Rescue on page 7-2*
- *Before Rescuing an Appliance on page 7-2*
- *Rescuing an Appliance on page 7-4*
- *Detaching an iDRAC Virtual Media Device on page 7-10*
About Appliance Rescue

To rescue the Deep Discovery Inspector appliance, do one of the following:

- Reinstall Deep Discovery Inspector and revert to saved or default settings.
  
  Data will not be saved but some configurations can be restored.

- Run the Deep Discovery Inspector rescue program from the Solutions DVD.
  
  Data, including logs, will be saved and configurations can be restored or reset to default.

Rescuing the appliance is not the same as applying a system update:

- **Rescuing**: Application files are replaced. Logs and configurations can be restored or reset to default.

- **Applying a system update**: Updates existing Deep Discovery Inspector files to enhance features.

Before Rescuing an Appliance

---

**WARNING!**

Before starting an appliance rescue, do the following:

- Detach external USB storage devices.
- Detach iDRAC virtual media devices.

For details, see *Detaching an iDRAC Virtual Media Device on page 7-10.*

---

The following files are part of the rescue process:

1. *.R image file
2. Rescue.exe or Solutions DVD
3. Backup configuration file
Procedure

1. Create a backup of your settings.

   For details, see *Exporting the Configuration File on page 6-5.*

   __Note__

   If the management console is still accessible, go to **Administration > System Maintenance > Backup / Restore.** For details, see the *Deep Discovery Inspector Administrator's Guide, Backing Up Encrypted File Settings.*

2. Copy the Deep Discovery Inspector Rescue Tool (`Rescue.exe`) from the Solutions DVD or the latest image you have to the Windows computer that can be used to launch the Deep Discovery Inspector Rescue Tool.

3. Prepare the computer with the rescue tool to run the Deep Discovery Inspector Rescue Tool for uploading a Deep Discovery Inspector image file (.R).

   Configure the computer with the rescue tool as follows:
   • Connect the computer with the rescue tool to Deep Discovery Inspector through a management port.
   • Make sure that the computer running the rescue tool is on the same network segment (192.168.252.0/24) as Deep Discovery Inspector.

   __Note__

   In rescue mode, the Deep Discovery Inspector IP address is 192.168.252.1 and the subnet mask is 255.255.255.0.
Rescuing an Appliance

**WARNING!**

Before starting an appliance rescue, do the following:

- Detach external USB storage devices.
- Detach iDRAC virtual media devices.

For details, see *Detaching an iDRAC Virtual Media Device on page 7-10.*

**Procedure**

1. Reboot Deep Discovery Inspector by one of the following methods:
   - On the management console, go to Administration > System Maintenance > Power Off / Restart.
     
     For details, see the *Deep Discovery Inspector Administrator's Guide*, *Restarting Deep Discovery Inspector*.
   - On the Preconfiguration Console:
     a. Log on to the Preconfiguration Console through a monitor.
        
        For details, see *Preconfiguration Console Access on page 5-2.*

     
     **Note**
     Deep Discovery Inspector only supports rescue operations that use a monitor connected to a VGA port.

     b. Select **System Tasks** and press ENTER.
        
        The **System Tasks** screen appears.
      
      c. Select **Restart System** and press ENTER.
The **Restart System** screen appears.

![Restart System Screen](image)

**Figure 7-1. Restart System**

2. When the **Press any key to enter the menu** message appears on the boot screen, press any key immediately.

![Press any key to enter the menu](image)

**Figure 7-2. Escape Initiation**
The boot menu appears.

![Boot Menu]

**Figure 7-3. Boot Menu**

3. To enter rescue mode, use the arrow key to select *Rescue mode* and press ENTER.

---

**WARNING!**

If there is no connection to the rescue tool within 600 seconds, Deep Discovery Inspector restarts automatically.
The Deep Discovery Inspector rescue mode screen appears.

**Figure 7-4. Deep Discovery Inspector Rescue Mode**

4. On the computer with the rescue tool, double-click `Rescue.exe` to launch the rescue tool.

---

**WARNING!**

Make sure the Deep Discovery Inspector appliance is in rescue mode before using the rescue tool.
5. Browse to the latest image file: *.R.

6. Click Update.

The Deep Discovery Inspector Rescue Tool uploads the new image.

**Note**

Do not power off or reset the appliance during the update process.

7. After the file uploads successfully, click Finish.

8. On the Preconfiguration Console, when the Start rescuing Deep Discovery Inspector? message appears, type `y` and press ENTER.
9. When the **Start migrating Configuration files?** message appears, do one of the following:

   • Type **Y** to migrate configurations.
   • Type **N** to reset configurations to default.

   **Important**

   If configurations are not migrated, network settings must be configured. For details, see step 11.

10. Press ENTER to continue.

    Deep Discovery Inspector starts migrating the configuration files.

11. (Optional) If configurations were not migrated, open the Preconfiguration Console and configure the Deep Discovery Inspector network settings.

    For details, see *Modifying Device Settings on page 5-9*.

---

**What to do next**

After rescuing the appliance, clear the browser cache.
For details, see the *Deep Discovery Inspector Administrator's Guide, Clearing the Browser Cache*.

**Detaching an iDRAC Virtual Media Device**

To prevent a rescue operation failure, detach iDRAC virtual media devices before beginning the rescue operation.

---

**Note**

The Dell® Remote Access Controller or DRAC interface card provides out-of-band management functionality, and allows system administrators to remotely configure an appliance. The controller has its own processor, memory, network connection, and access to the system bus. Key features include power management, virtual media access, and remote console capabilities provided through a supported web browser or command line interface.

---

**Procedure**

1. Log on to the iDRAC virtual media device web console.
2. On the left panel, go to **Overview** > **Server** tab.
3. On the top menu, go to **Properties** > **Summary** and then in the **Virtual Console Preview** click **Launch**.
   
   A virtual console appears.
4. In the virtual console, click **Virtual Media**.
5. Select the Deep Discovery Inspector installation ISO image and click **Remove**.

---

**Restoring to Factory Mode**

Reset Deep Discovery Inspector by restoring the default settings that shipped with the product.
Procedure

1. Power on Deep Discovery Inspector with a monitor connected to a VGA port.
   When Deep Discovery Inspector is starting and before the Preconfiguration Console opens, the Press any key to enter the menu prompt appears.

2. Press any key to enter the boot system options menu.

3. Using the arrow key, select Restore to factory mode and press Enter.
   Deep Discovery Inspector restarts and the Preconfiguration Console opens.
Create a New Virtual Appliance

Learn how to create a virtual appliance using VMware ESXi in the following topics:

- Creating a Virtual Machine in VMware ESXi on page 8-2
- Configuring the VMware ESXi Server Network on page 8-3
- Enabling Promiscuous Mode in VMware ESXi on page 8-9
- Installing Deep Discovery Inspector in VMware ESXi on page 8-12

For details about the minimum virtual appliance system requirements and supported hypervisors, see System Requirements on page 3-11.
Creating a Virtual Machine in VMware ESXi

**Important**

You must separately license VMware ESXi and such use is subject to the terms and conditions of the VMware license agreement for that product.

To install Deep Discovery Inspector in a VMware server, prepare the following:

<table>
<thead>
<tr>
<th><strong>Requirement</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| VMware ESXi server | Install the Deep Discovery Inspector virtual machine and verify the following:  
  - ESXi server is version 5.x or 6.x  
  - Two or more NICs on the VMware ESXi server (one Manager Network, one or more Data Networks)  
  For details, see *Configuring the VMware ESXi Server Network on page 8-3.*  
  - **Promiscuous Mode** is enabled to pass all traffic received by the Data Network.  
  For details, see *Enabling Promiscuous Mode in VMware ESXi on page 8-9.* |
| VMware vSphere client | Synchronizes VMware vSphere Client with the ESXi server.  
VMware vSphere Client provides the following functionality:  
  - Performs deployment tasks  
  - Manages the Deep Discovery Inspector virtual machine |
| Windows computer | Install the following software on a Windows computer:  
  - VMware vSphere Client  
  - Internet Explorer, Microsoft Edge, Firefox, or Chrome (for accessing the Deep Discovery Inspector management console) |
Configuring the VMware ESXi Server Network

Use VMware vSphere Client to connect the ESXi server to a Windows computer.

Procedure

1. To open VMware vSphere Client, type the VMware ESXi server IP Address, User name, and Password, and click Login.

2. Go to the Configurations tab and click Networking. Observe the initial state.

3. Set the default VM Network as the Management Network.

4. Click Add Networking...
The **Add Network Wizard** opens.

5. In the **Add Network Wizard**, click **Connection Type**. Select **Virtual Machine**, and then click **Next**.
6. On the **Network Access** screen, do the following:
   
a. Select **Create a vSphere standard switch**.

b. Select a NIC card as the Data Network.

c. Click **Next**.
7. On the **Connection Settings** screen, do the following:
   
   a. In **Network Label**, type **Data Network**.
   
   b. In **VLAN ID (Optional)**, select **All (4095)**.
   
   c. Click **Next**.
8. On the **Summary** screen, verify that all new and modified vSphere standard switches are configured appropriately.
9. Click Finish.

10. Go to the Configurations tab and click Networking to verify that the Data Network is connected to the Monitored Network.
11. Enable **Promiscuous Mode**.

For details, see *Enabling Promiscuous Mode in VMware ESXi on page 8-9.*

12. (Optional) Create additional data networks by repeating steps 6 to 11.

---

**Enabling Promiscuous Mode in VMware ESXi**

**Procedure**

1. In the VMware vSphere Client, go to the **Configurations** tab and click **Networking**.
2. At your Data Network vSwitch, click **Properties**.
3. Click **Edit**.

4. Click the **Security** tab and set **Promiscuous Mode** as **Accept**. Click **OK**.
Create a New Virtual Appliance

Policy Exceptions

Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Reject
Installing Deep Discovery Inspector in VMware ESXi

The following procedure is for VMware.

**Procedure**

1. From the VMware ESXi menu bar, select **File > New > Virtual Machine**.
2. On the **Configuration** screen, click **Custom > Next**.
3. On the Name and Location screen, specify a name for the virtual machine and click Next.

4. On the Storage screen, select the destination storage where the virtual machine will reside and click Next.
5. On the **Virtual Machine Version** screen, select the virtual machine version and click **Next**.
6. On the **Guest Operating System** screen, perform the following steps.
   a. For **Guest Operating System**, select **Linux**.
   b. For **Version**, select **CentOS 4/5/6 (64-bit)**.
   c. Click **Next**.
7. On the **CPUs** screen, adjust the number of virtual sockets and cores per virtual socket to allocate at least 5 total cores for the virtual machine and click **Next**.
8. On the Memory screen, allocate at least 8 GB of memory for the virtual machine and click Next.
9. On the **Network** screen, configure at least two NICs for the virtual machine and click **Next**.

Set the VMware ESXi server **VM Network** as the Deep Discovery Inspector Management Network (NIC 1). Set **Data Network** as the Deep Discovery Inspector Data Network (NIC 2).

**Note**

Trend Micro recommends using the VMXNET 3 network adapter on ESXi 5.5 or later.
10. On the **SCSI Controller** screen, select the I/O adapter type appropriate for the virtual disk and click **Next**.
11. On the **Select a Disk** screen, select **Create a new virtual disk** and click **Next**.
12. On the **Create a Disk** screen, allocate at least 100 GB of hard disk space for the virtual machine and click **Next**.
13. On the **Advanced Options** screen, keep the default selections and click **Next**.
14. On the Ready to Complete screen, review the settings and click Finish.
Create New Virtual Machine

Ready to Complete

Click Finish to start a task that will create the new virtual machine.

Settings for the new virtual machine:
- Name: New Virtual Machine
- Host/Clust: localhost
- Resource Pool: Ariel
- Datastore: datastore1
- Guest OS: Other 2.6.x Linux (64-bit)
- Cpus: 4
- Memory: 8192 MB
- Nic1: 2
- NIC 1 Network: VM Network
- NIC 2 Network: VM Network
- NIC 2 Type: E1000
- SCSI Controller: LSI Logic Parallel
- Create disk: New virtual disk
- Disk capacity: 160 GB
- Disk provisioning: Thin Provision
- Datastore: datastore1
- Virtual Device Node: SCSI (0:0)
- Disk mode: Persistent

Create a Disk

Advanced Options

Ready to Complete

Choose disk

Edit the virtual machine settings before completion

Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.
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 9-2*
- *Troubleshooting on page 9-7*
Frequently Asked Questions (FAQs)

Find answers to frequently asked questions in the following topics.

- FAQs - Activation on page 9-2
- FAQs - Configuration on page 9-2
- FAQs - Detections on page 9-4
- FAQs - Documentation on page 9-4
- FAQs - Installation on page 9-4
- FAQs - Upgrade on page 9-5
- FAQs - Virtual Analyzer Image on page 9-6
- FAQs - Widgets on page 9-7

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
• 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?
Troubleshoot

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 SP2?

Yes. Upgrade by updating the firmware from Deep Discovery Inspector 3.6, 3.7, or 3.8 to Deep Discovery Inspector 3.8 SP2. 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 SP2?

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, Deep Discovery 3.0, or Deep Discovery Inspector 3.2 to Deep Discovery Inspector 3.8 SP2?**

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 when the image is tested in VirtualBox. Does this affect Virtual Analyzer?**

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another. If the **Found New Hardware** wizard appears when the image is tested in VirtualBox, it may interfere with the CD/DVD auto-run.

**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.

---

An image displays the blue “Cannot find Operating System” screen when tested in 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

The management console response is slow or times out.

This occurs when system resources are insufficient.

Procedure

1. To verify CPU, memory, and disk usage, go to https://<appliance IP address>/html/troubleshooting.htm.

2. Under Real-time Status, select System Process (ATOP).
The System Process screen appears.

**FIGURE 9-1. System Process (ATOP)**

3. Click Suspend and verify system resources real-time.

**TABLE 9-1. System Resources**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>LINE</th>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| CPU  | CPU  | Idle   | The lower the number, the busier the CPU is.  
If this number is low, view the process information and record the CPU with the highest usage. |
| MEM  | MEM  | Free, cache | The "Free" field indicates available memory. A low number means that there is not enough available memory to complete certain actions. |
| Disk | DSK  | Busy   | A high number indicates that the disk is busy. |

**Detections**

- *No Detections on Detections Tab on page 9-10*
- "Unregistered Service" Server Displays in All Detections Query on page 9-11
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.

   ![Figure 9-2. Appliance IP Address Settings](image)

   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.

**Figure 9-3. 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*.

![All Detections Query](image)

**FIGURE 9-4. All Detections Query**

**Procedure**

1. Add the server to the **Registered Services** list.
   a. Go to *Administration > Network Groups and Assets > Registered Services*. 

   ![Registered Services](image)
The **Registered Services** screen appears.

![Registered Services](image)

**FIGURE 9-5. 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 9-14
- Rescue Operation Error Message on page 9-14

**"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.

---

![Database status alert](image)

**FIGURE 9-6. 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 9-15**
- **No Virtual Analyzer Response to File Submissions on page 9-15**

**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.

---

Virtual Analyzer Images

- Installation CD/DVD Won’t Start on page 9-16
- "Found New Hardware” Wizard on page 9-18
- An Image Displays a Blue Screen on page 9-18

---

Installation CD/DVD Won't Start

The installation CD/DVD does not automatically start.

Verify items by testing the Virtual Analyzer images in VirtualBox.

---

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.

2. Click Settings and select Storage.

3. Select Controller: IDE and verify that the specified type is PIIX4.
4. Select the optical disc icon and verify that the specified CD/DVD drive is **IDE Secondary Master**.
"Found New Hardware" Wizard

During Virtual Analyzer image creation, the Found New Hardware wizard appears.

The Found New Hardware wizard automatically runs whenever an image is transferred from one machine to another.

When an image is imported, the Found New Hardware wizard may interfere with the CD/DVD auto-run. Make sure the Virtual Analyzer image is created and prepared using the correct procedure. For details, see the Virtual Analyzer Image Preparation User's Guide at http://docs.trendmicro.com/en-us-enterprise/virtual-analyzer-image-preparation.aspx.

An Image Displays a Blue Screen

An image displays the blue "Cannot find Operating System" screen when tested in VirtualBox.

Verify items by testing the Virtual Analyzer images in VirtualBox.
Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.

2. Click the **Settings** and select **System**.

![Figure 9-9. 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 Debug Logs.

c. In Debug Log Settings, 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. Click Save.

e. If possible, reproduce the issue.

f. Select one or more debug logs to export.

   - Select Export debug log to export the debug log.
   - Select Export advanced debug log to export all the advanced debug logs.
   - Select one or more dated debug logs under Export advanced debug log to export the advanced debug log for that date.

g. Click Export.

---

**Important**

To conserve system resources, only perform one export at a time.

---

h. In Debug Log Settings, click Reset to default log settings.

i. In Debug Log Maintenance, click Purge Debug Logs.
Chapter 10

Technical Support

Learn about the following topics:

- Troubleshooting Resources on page 10-2
- Contacting Trend Micro on page 10-3
- Sending Suspicious Content to Trend Micro on page 10-4
- Other Resources on page 10-5
Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

2. Select from the available products or click the appropriate button to search for solutions.
3. Use the Search Support field to search for available solutions.
4. If no solution is found, click Contact Support and select the type of support needed.

Tip

To submit a support case online, visit the following URL:


A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of “blended threats” which combine two or more technologies to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia
Technical Support

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/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or “in the wild”
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Inc., 225 E. John Carpenter Freeway, Suite 1500, Irving, Texas 75062</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Phone: +1 (817) 569-8900&lt;br&gt;Toll free: (888) 762-8736</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</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 connected hardware or devices
• Amount of memory and free hard disk space
• Operating system and service pack version
• Version of the installed agent
• Serial number or activation code
• Detailed description of install environment
• Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com

Refer to the following Knowledge Base entry to send message samples to Trend Micro:


File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

Record the case number for tracking purposes.

**Web Reputation Services**

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called “disease vector” (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

**Other Resources**

In addition to solutions and support, there are many other helpful resources available online to help you stay up to date, learn about innovations, and to be aware of the latest security trends.

**Download Center**

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://downloadcenter.trendmicro.com

If a patch has not been applied (patches are dated), open the Readme to determine whether it is relevant to your environment. The Readme also contains installation instructions.

**Documentation Feedback**

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:
http://www.trendmicro.com/download/documentation/rating.asp
Appendices
Appendix A

Get Started

Learn about the Deep Discovery Inspector management console and basic appliance settings in the following topics:
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 A-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 FQDN or IP address  
  • Network traffic |
### # UI Element Description

3. Main screen tabs

The management console includes the following tabs:
- Dashboard
- Detections
- Reports
- Administration
- Help

### Management Console Requirements

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

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google™ Chrome™</td>
<td>46.0 or later</td>
</tr>
<tr>
<td>Mozilla™ Firefox™</td>
<td>41.0 or later</td>
</tr>
<tr>
<td>Microsoft™ Internet Explorer™</td>
<td>10.0 and 11.0</td>
</tr>
<tr>
<td>Microsoft™ Edge</td>
<td></td>
</tr>
</tbody>
</table>

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

Recommended resolution: 1280x800 or higher

### Opening the Management Console

**Procedure**

1. From a network workstation, open a supported browser.
2. Set the Internet security level to Medium and enable ActiveX Binary and Script Behaviors to make sure that tool tips and reports appear.

3. Type the management console IP address:
   - If using the default Deep Discovery Inspector IP address, type the following:
     
     **Note**
     
     The URL is case sensitive.
   
   - If using a unique IP address, type that IP address.

4. Type the default user name:
   
   admin

5. Type the default password:
   
   admin

6. Click **Log on**.

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

7. Change the default password.
   
   See *Management Console Account Passwords on page A-5*.

8. Set system time.
   
   See *Configuring Time Options on page A-7*.

   
   See *Activating or Renewing a Product License on page A-8*.
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

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.

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

1. On any Deep Discovery Inspector main screen, at the top-right corner, open the drop-down menu under your account name.

2. Click Change Password.

3. Type the old password.

4. Type the new password and confirm it.

5. Click Save.

Deep Discovery Inspector automatically logs off.

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

7. 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.
**Get Started**

**Procedure**

1. On any Deep Discovery Inspector main screen, at the top-right corner, open the drop-down menu under your account name.

2. Click **Change Password**.

3. Type the old password.

4. Type the new password and confirm it.

5. Click **Save**.

   Deep Discovery Inspector automatically logs off.

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

**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**.

---

### Activating or Renewing a Product License

**Procedure**

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

2. Under **License Information**, click **New Activation Code**.
   
   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**.

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 A-10.

2. Configure Registered Domains.
   For details, see Adding Registered Domains on page A-12.

3. Configure Registered Services.
   For details, see Adding Registered Services on page A-12.

4. (Optional) Configure Proxy Settings.
   For details, see Configuring a Proxy Server on page A-14.

5. Update components.
   For details, see Performing Manual Updates on page A-15.
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.

   The Network Groups window appears.

3. Type a group name.

   ___________
   **Note**
   Provide specific groups with descriptive names for easy identification of the network to which the IP address belongs. For example: "Finance network", "IT network", or "Administration".

4. Type an IP address range in the text box (up to 1,000 IP address ranges).

   ___________
   **Note**
   The IP address range cannot contain a Class D or Class E address (224.0.0.0 - 255.255.255.255)

Deep Discovery Inspector provides a default network group containing the following IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks:

- IPv4: 10.0.0.0 - 10.255.255.255
- IPv4: 172.16.0.0 - 172.31.255.255
- IPv4: 192.168.0.0 - 192.168.255.255

---

**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`

---

**Note**
Add up to three layers of sub-groups.

---

5. Select the **Network zone**.

---

**Note**

*Trusted* indicates a secure network and *Untrusted* indicates a degree of doubt about the security of the network.

---

6. Click **Add**.

7. Click **Save**.
Adding Registered Domains

Add domains used by companies for internal purposes or those considered trustworthy. Identifying trusted domains ensures detection of unauthorized domains.

Add only trusted domains (up to 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.

![Note]
Registered domain names appear in the Defined Registered Domains section.

3. (Optional) Click Analyze to display a list of domains that can be added to the list.
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>
<thead>
<tr>
<th>SERVICE</th>
<th>NETWORK SERVER DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Provides directory services and stores user accounts and passwords. Configure the same server as the Domain Controller.</td>
</tr>
<tr>
<td>Authentication Servers - Kerberos</td>
<td>Provides Kerberos authentication</td>
</tr>
<tr>
<td>Content Management Server</td>
<td>Manages content</td>
</tr>
<tr>
<td>Database Server</td>
<td>Used as a database server</td>
</tr>
<tr>
<td>DNS</td>
<td>Used as a DNS server</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>Responds to security authentication requests and allows host access to domain resources. 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>Service</td>
<td>Network Server Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------</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**.

---

## 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 **Host 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.

---

### 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.**