TREND MICRO™
Deep Discovery™ Director
(Consolidated Mode)
Administrator’s Guide
Breakthrough Protection Against APTs and Targeted Attacks
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

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

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

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that Deep Discovery Director (Consolidated Mode) collects and provides detailed instructions on how to disable the specific features that feedback the information.


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

# Table of Contents

## Preface

Preface ............................................................................................................................. vii  
Documentation ........................................................................................................ viii  
Document Conventions ............................................................................................ ix  
About Trend Micro .................................................................................................... x  

## Chapter 1: Introduction

About Deep Discovery Director (Consolidated Mode) ........................................ 1-2  
What's New ................................................................................................................. 1-2  
Features and Benefits ............................................................................................... 1-3  

## Chapter 2: Deployment and Installation

System Requirements ................................................................................................. 2-2  
Detection Log Aggregation Requirements ............................................................. 2-3  
Installing Deep Discovery Director .......................................................................... 2-4  
Configuring Network Addresses on the Preconfiguration Console ..................... 2-6  
Logging on to the Management Console ................................................................. 2-7  

## Chapter 3: Dashboard

Dashboard Overview ................................................................................................. 3-2  
Tabs ............................................................................................................................ 3-2  
    Tab Tasks ............................................................................................................ 3-2  
Widgets ...................................................................................................................... 3-3  
    Widget Tasks ...................................................................................................... 3-3  
Deep Discovery Inspector Widgets ........................................................................ 3-7  
    Threats at a Glance ......................................................................................... 3-7  
    Top Affected Hosts ......................................................................................... 3-9  

Chapter 4: Detections

About the Detections Screen ......................................................... 4-2
  Host Severity ...................................................................................... 4-3
  Email Message Risk Levels .............................................................. 4-6
  Email Message Threat Type Classifications .................................. 4-9
  Protocols That Support Advanced Analysis Using Correlation Data ............................................................................. 4-11

Affected Hosts ...................................................................................... 4-12
  Display Options and Search Filters ................................................ 4-13
  Viewing Affected Hosts ................................................................. 4-15
  Viewing Affected Hosts - Host Details ............................................ 4-19
  Viewing Affected Hosts - Detection Details ................................... 4-23
  Affected Hosts Advanced Search Filter ........................................ 4-33

Network Detections .................................................................................. 4-47
  Display Options and Search Filters ................................................ 4-47
  Viewing Network Detections ............................................................ 4-49
  Viewing Network Detections - Detection Details ......................... 4-53
  Network Detections Advanced Search Filter ................................ 4-64

Email Messages ............................................................................................. 4-73
  Display Options and Search Filters ................................................ 4-73
  Viewing Email Messages ............................................................... 4-75
  Email Messages - Detection Details ............................................. 4-76
  Email Messages Advanced Search Filter ....................................... 4-81

Correlated Events .......................................................................................... 4-87
  Display Options and Search Filters ................................................ 4-87
  Viewing Correlated Events ............................................................. 4-90
  Viewing Correlated Events - Correlation Data ............................ 4-90
  Viewing Correlated Events - Detection Details ......................... 4-100
## Chapter 5: Threat Intelligence

- **Product Intelligence** .......................................................... 5-2
  - Synchronized Suspicious Objects .................................. 5-2
  - C&C Callback Addresses ............................................. 5-8
- **Custom Intelligence** .......................................................... 5-11
  - YARA Rules ............................................................. 5-12
  - STIX ............................................................................. 5-17
  - User-Defined Suspicious Objects .............................. 5-19
  - Exceptions ............................................................... 5-25
- **Feed Management** .......................................................... 5-29
  - Adding an Intelligence Feed .................................. 5-29
  - Editing an Intelligence Feed .................................... 5-31
  - Deleting Intelligence Feeds ...................................... 5-31
- **Sharing Settings** ............................................................. 5-31
  - TAXII ................................................................. 5-32
  - Web Service ............................................................ 5-33
  - Auxiliary Products/Services ...................................... 5-34

## Chapter 6: Appliances

- **Directory** .......................................................................... 6-2
  - Directory Tasks .......................................................... 6-2
  - Other Directory Tasks .................................................. 6-4
- **Plans** .................................................................................. 6-8
  - Plan Tasks ........................................................................ 6-10
  - Appliance Statuses ..................................................... 6-10
  - Other Plan Tasks .......................................................... 6-12
- **Repository** ......................................................................... 6-29
  - Hotfixes / Critical Patches / Firmware ........................ 6-29
  - Virtual Analyzer Images ............................................. 6-30
  - Upload Center ............................................................... 6-32
- **Logs** .................................................................................. 6-33
  - Email Message Tracking ............................................. 6-34
MTA ............................................................................................................................ 6-38

Chapter 7: Alerts

About Alerts ............................................................................................................ 7-2
Triggered Alerts ..................................................................................................... 7-2
Built-in Rules ........................................................................................................ 7-3
  Editing a Built-in Rule ....................................................................................... 7-4
Custom Rules ........................................................................................................ 7-6
  Adding a Custom Rule ...................................................................................... 7-7
  Other Custom Rules Tasks ............................................................................... 7-8

Chapter 8: Administration

Updates .................................................................................................................... 8-2
  Components ..................................................................................................... 8-2
  Hotfixes / Patches ......................................................................................... 8-3
  Firmware ........................................................................................................ 8-6
Integrated Products/Services ............................................................................. 8-7
  Microsoft Active Directory .......................................................................... 8-7
  Syslog ............................................................................................................. 8-9
System Settings ................................................................................................... 8-11
  Network ........................................................................................................ 8-11
  Proxy ............................................................................................................. 8-13
  SMTP ............................................................................................................. 8-14
  Bandwidth ..................................................................................................... 8-15
  Time ............................................................................................................... 8-16
  Certificate ..................................................................................................... 8-17
  Session Timeout ............................................................................................ 8-19
Account Management ........................................................................................... 8-19
  Accounts ....................................................................................................... 8-19
  Roles .............................................................................................................. 8-24
System Logs ......................................................................................................... 8-28
  Querying System Logs ................................................................................... 8-30
System Maintenance ............................................................................................ 8-32
  System Status ............................................................................................... 8-32
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>8-32</td>
</tr>
<tr>
<td>Back Up</td>
<td>8-34</td>
</tr>
<tr>
<td>Restore</td>
<td>8-37</td>
</tr>
<tr>
<td>Power Off / Restart</td>
<td>8-42</td>
</tr>
<tr>
<td>License</td>
<td>8-42</td>
</tr>
</tbody>
</table>

### Chapter 9: Technical Support

- Troubleshooting Resources: 9-2
  - Using the Support Portal: 9-2
  - Threat Encyclopedia: 9-2
- Contacting Trend Micro: 9-3
  - Speeding Up the Support Call: 9-4
- Sending Suspicious Content to Trend Micro: 9-4
  - Email Reputation Services: 9-4
  - File Reputation Services: 9-5
  - Web Reputation Services: 9-5
- Other Resources: 9-5
  - Download Center: 9-5
  - Documentation Feedback: 9-6
Preface

Welcome to the Trend Micro Deep Discovery Director (Consolidated Mode) *Administrator's Guide*. This guide contains information about product settings.
The documentation set for Deep Discovery Director (Consolidated Mode) includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator's Guide</td>
<td>The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Director (Consolidated Mode), and explanations on Deep Discovery Director (Consolidated Mode) concepts and features.</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 Director (Consolidated Mode).</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 Director (Consolidated Mode) management console. The Online Help contains explanations of Deep Discovery Director (Consolidated Mode) components and features, as well as procedures needed to configure Deep Discovery Director (Consolidated Mode).</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: http://docs.trendmicro.com/en-us/home.aspx
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><strong>Navigation &gt; Path</strong></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><img src="image" alt="Note" /></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><img src="image" alt="Tip" /></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><img src="image" alt="Important" /></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td><img src="image" alt="WARNING!" /></td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>
About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.
Chapter 1

Introduction

This chapter introduces Trend Micro™ Deep Discovery™ Director (Consolidated Mode) 3.5 and the new features in this release.
About Deep Discovery Director (Consolidated Mode)

Trend Micro Deep Discovery Director 3.5 is an on-premises management solution that enables the following:

- Centralized deployment of hotfixes
- Centralized deployment of critical patches
- Centralized deployment of firmware
- Centralized deployment of Virtual Analyzer images
- Configuration replication
- Log aggregation

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

Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, Deep Discovery Inspector, and Deep Discovery Director - Network Analytics.

What's New

**TABLE 1-1. What’s New in Deep Discovery Director (Consolidated Mode) 3.5**

<table>
<thead>
<tr>
<th>FEATURE/ENHANCEMENT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Discovery Email Inspector log aggregation</td>
<td>Deep Discovery Director (Consolidated Mode) now aggregates Deep Discovery Email Inspector detection, email message tracking and MTA logs. Using the same intuitive multi-level format that Deep Discovery Email Inspector users are accustomed to, the Deep Discovery Director (Consolidated Mode) management console provides real-time threat visibility and analysis.</td>
</tr>
</tbody>
</table>
Deep Discovery Email Inspector widgets

The enhanced Dashboard now provides Deep Discovery Email Inspector widgets that allow administrators to view email message detection and security related information.

Email Messages screen

The enhanced Detections screen now provides access email message detections.

Logs screen

The enhanced Appliances screen is now home to the new Logs screen where users can find Deep Discovery appliance related logs such as Email Message Tracking and MTA logs.

Email security alerts

Deep Discovery Director (Consolidated Mode) now provides built-in email security specific alerts as well as the option to create custom email security alerts.

Enhanced role-based access control

In addition to controlling which management console screens and features, and which appliances a role can see and manage, roles can now be customized to control which email message detections they can see by using domains.

Features and Benefits

Deep Discovery Director (Consolidated Mode) includes the following features:

<table>
<thead>
<tr>
<th>FEATURE/BENEFIT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced threat analysis</td>
<td>Deep Discovery Director (Consolidated Mode) integrates with Deep Discovery Director - Network Analytics to provide advanced threat analysis using correlation data.</td>
</tr>
<tr>
<td>Deep Discovery Inspector log aggregation</td>
<td>Deep Discovery Director (Consolidated Mode) aggregates Deep Discovery Inspector detection logs. Using the same intuitive multi-level format, the Deep Discovery Director (Consolidated Mode) management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.</td>
</tr>
<tr>
<td>FEATURE/BENEFIT</td>
<td>DETAILS</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Product intelligence</td>
<td>Deep Discovery Director (Consolidated Mode) consolidates suspicious objects and C&amp;C callback addresses from registered Deep Discovery appliances.</td>
</tr>
<tr>
<td>Custom intelligence</td>
<td>Deep Discovery Director (Consolidated Mode) can distribute YARA rules to registered appliances and import threat intelligence using the Structured Threat Information eXpression (STIX) format. You can also add user-defined suspicious objects that have not yet detected on your network, as well as exceptions that you consider harmless.</td>
</tr>
<tr>
<td>Feed Management</td>
<td>Deep Discovery Director (Consolidated Mode) allows you to subscribe to and monitor intelligence feeds for threat information that can be used to complement your product and custom intelligence.</td>
</tr>
<tr>
<td>Threat intelligence sharing</td>
<td>Deep Discovery Director (Consolidated Mode) can share threat intelligence data with other products or services through TAXII and HTTP or HTTPS web service.</td>
</tr>
<tr>
<td>Auxiliary products/services</td>
<td>To help provide effective detection and blocking at the perimeter, Deep Discovery Director (Consolidated Mode) can distribute threat intelligence data to auxiliary products and services.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>The <strong>Dashboard</strong> screen and Deep Discovery appliance widgets allow administrators to view network integrity, system threat data, and email message detection and security information.</td>
</tr>
<tr>
<td>Detections</td>
<td>The <strong>Detections</strong> screen provides access to real-time information about various detection categories.</td>
</tr>
<tr>
<td>Syslog</td>
<td>The <strong>Syslog</strong> screen allows Deep Discovery Director (Consolidated Mode) to send suspicious objects lists and detection and appliance related logs to up to three <strong>Syslog</strong> servers.</td>
</tr>
<tr>
<td>System alerts</td>
<td>Administrators can view the details of triggered alerts directly on the management console. Custom rules can be created to be alerted of specific threats.</td>
</tr>
<tr>
<td><strong>Feature/Benefit</strong></td>
<td><strong>Details</strong></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Role-based access control</td>
<td>Built-in roles allow administrators to control which management console screens and features can be accessed. Custom roles can be created to control which appliances a role can see and manage, and which email message detections a role can see.</td>
</tr>
<tr>
<td>Storage configuration</td>
<td>Administrators can add extra available disk space to Deep Discovery Director (Consolidated Mode) partitions to increase the number of logs or repository files that can be stored.</td>
</tr>
<tr>
<td>Directory</td>
<td>The <strong>Directory</strong> displays information about Deep Discovery appliances that are registered to Deep Discovery Director (Consolidated Mode).</td>
</tr>
<tr>
<td>Plans</td>
<td>Plans define the scope and schedule of deployments to target appliances.</td>
</tr>
<tr>
<td>Repository</td>
<td>The <strong>Repository</strong> screen displays all update, upgrade, and <strong>Virtual Analyzer</strong> image files hosted by the server. Upload and delete files from here.</td>
</tr>
<tr>
<td>Component updates</td>
<td>Deep Discovery Director (Consolidated Mode) uses components to display related information about detections.</td>
</tr>
<tr>
<td>Updates</td>
<td>The <strong>Updates</strong> screen enables you to install hotfixes, patches and firmware upgrades to Deep Discovery Director (Consolidated Mode). After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.</td>
</tr>
<tr>
<td>Microsoft Active Directory Integration</td>
<td>Deep Discovery Director (Consolidated Mode) allows <strong>Active Directory</strong> accounts to access the management console.</td>
</tr>
<tr>
<td>System Logs</td>
<td>Deep Discovery Director (Consolidated Mode) maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.</td>
</tr>
</tbody>
</table>
Chapter 2

Deployment and Installation

This chapter contains information about the requirements and procedures for deploying and installing Deep Discovery Director (Consolidated Mode).
## System Requirements

### Table 2-1. System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum Specifications</th>
</tr>
</thead>
</table>
| **Hardware** | • Network interface card: 1 with E1000 or VMXNET 3 adapter  
• **Important**  
  • Deep Discovery Director (Consolidated Mode) does not support the VMXNET 2 (Enhanced) adapter type.  
  • For port binding, specify the same adapter type to use for all network interface cards.  
  • SCSI Controller: LSI Logic Parallel  
  • CPU: 1.8GHz (at least 4 cores)  
  • Memory: 8GB  
  • Hard disk: 135GB (thin provisioned)  
• **Note**  
  The CPU, memory, and hard disk requirements increase with the number of Deep Discovery appliances Deep Discovery Director (Consolidated Mode) is expected to aggregate detection and appliance logs from.  
  For details, see *Detection Log Aggregation Requirements on page 2-3.*  |
| **Software** | • Hypervisor: VMware vSphere ESXi 5.5/6.0/6.5 or Microsoft Hyper-V in Windows Server 2012 R2/2016  
• Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)  |
| **Ports**    | • TCP 443 (Deep Discovery Director connection)  
• UDP 123 (default NTP server connection)  |
Detection Log Aggregation Requirements

The CPU, memory, and hard disk requirements increase with the number of Deep Discovery appliances Deep Discovery Director (Consolidated Mode) is expected to aggregate detection and appliance logs from.

**Table 2-2. Detection Log Aggregation Requirements**

<table>
<thead>
<tr>
<th>Number of Deep Discovery Appliances</th>
<th>Detection Log Count in Days</th>
<th>CPU (Cores)</th>
<th>Memory (GB)</th>
<th>Hard Disk (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td>4</td>
<td>8</td>
<td>135</td>
</tr>
<tr>
<td>5</td>
<td>90</td>
<td>4</td>
<td>8</td>
<td>225</td>
</tr>
<tr>
<td>5</td>
<td>180</td>
<td>4</td>
<td>8</td>
<td>315</td>
</tr>
<tr>
<td>15</td>
<td>180</td>
<td>8</td>
<td>16</td>
<td>665</td>
</tr>
<tr>
<td>Number of Deep Discovery Appliances</td>
<td>Detection Log Count in Days</td>
<td>CPU (Cores)</td>
<td>Memory (GB)</td>
<td>Hard Disk (GB)</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>25</td>
<td>180</td>
<td>8</td>
<td>16</td>
<td>1010</td>
</tr>
</tbody>
</table>

## Installing Deep Discovery Director

### Procedure

1. Create a custom virtual machine with the following minimum specifications:
   - Virtual machine hardware version: 8
   - Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)
   - CPU: 1 virtual socket with 4 cores
   - Memory: 8GB
   - Network interface card: 1 with E1000 or VMXNET 3 adapter

   **Important**
   - Deep Discovery Director (Consolidated Mode) does not support the VMXNET 2 (Enhanced) adapter type.
   - For port binding, specify the same adapter type to use for all network interface cards.

   - SCSI Controller: LSI Logic Parallel
   - Hard disk: 135GB (thin provisioned)

2. Open the virtual machine console, and then power on the virtual machine.

3. Connect the CD/DVD device of the virtual machine to the Deep Discovery Director (Consolidated Mode) ISO image file, and then boot the virtual machine from the CD/DVD drive.
The Deep Discovery Director (Consolidated Mode) Installation screen appears.

4. Select **Install software**.

The Deep Discovery Director (Consolidated Mode) Components screen appears.

5. Select one of the following installation options:

   - **Install all components**
   - **Install all components without log receiving capability**

---

**Important**

This option is permanent and installs Deep Discovery Director (Consolidated Mode) without the capability to receive logs from Deep Discovery appliances. Deep Discovery Director (Consolidated Mode) must be reinstalled to change this option.

---

The **License Agreement** screen appears.

6. Click **Accept**.

The **Disk Selection** screen appears.

7. Click **Continue**.

The **Hardware Profile** screen appears.

8. Click **Continue**.

The **Disk Space Configuration** screen appears.

9. (Optional) Modify the disk space configuration, and then click **Continue**.

The **Repartition Disks** confirmation message appears.

10. Click **Continue**.

The installation starts.
Configuring Network Addresses on the Preconfiguration Console

Procedure

1. Open the Deep Discovery Director (Consolidated Mode) virtual machine console.

2. Log on to the preconfiguration console using the following default credentials:
   - User name: admin
   - Password: admin

   The Main Menu screen appears.

3. Select Configure network settings and then press ENTER.

   The Configure Network Settings screen appears.

4. Configure the following required settings:
   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - DNS server 1

   Note

   Only IPv4 settings can be configured on the preconfiguration console. To configure IPv6 and port binding, use the Network screen on the management console.

   For details, see Network on page 8-11.

5. Press TAB to navigate to Save, and then press ENTER.

   The Main Menu screen appears after the settings are successfully saved.
Logging on to the Management Console

Procedure

1. Open a browser window and connect to the server address provided on the preconfiguration console.

   The management console logon screen appears.

2. Type the following default credentials:
   - User name: admin
   - Password: admin

3. Click Log on.

   The management console appears.
Chapter 3

Dashboard

Learn about information that displays on the Dashboard screen in the following topics:

- Dashboard Overview on page 3-2
- Tabs on page 3-2
- Widgets on page 3-3
- Deep Discovery Inspector Widgets on page 3-7
- Deep Discovery Email Inspector Widgets on page 3-10
Dashboard Overview

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

Customize the Deep Discovery Director (Consolidated Mode) dashboard with available widgets to provide timely and accurate system status and threat information about your network.

The dashboard includes the following user interface elements:

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

Tabs

Tabs provide a container for widgets.

The dashboard supports up to 30 tabs. Each tab on the dashboard can contain up to 8 widgets.

Tab Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a tab</td>
<td>Click the plus icon at the top of the dashboard.</td>
</tr>
<tr>
<td>Rename a tab</td>
<td>1. Select the tab you wish to rename.</td>
</tr>
<tr>
<td></td>
<td>2. Click the menu icon beside the tab title and then select <strong>Rename</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Type a name with a maximum of 64 characters.</td>
</tr>
<tr>
<td>Move a tab</td>
<td>Drag a tab's title to change the tab's position.</td>
</tr>
</tbody>
</table>
Widgets

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

Widgets can be customized to provide a clear snapshot of network health and vulnerabilities.

Widget Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add widgets to the dashboard</td>
<td>To add widgets to the dashboard, do any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select the tab you wish to add widgets to, click the menu icon</td>
</tr>
<tr>
<td></td>
<td>beside the tab title, and then select Add Widgets.</td>
</tr>
<tr>
<td></td>
<td>• Select the tab you wish to add widgets to, click the gear icon</td>
</tr>
<tr>
<td></td>
<td>in the top-right corner of the screen, and then select Add</td>
</tr>
<tr>
<td></td>
<td>Widgets.</td>
</tr>
<tr>
<td></td>
<td>• On newly created tabs, click Add a widget.</td>
</tr>
<tr>
<td></td>
<td>The Add Widgets screen displays.</td>
</tr>
<tr>
<td></td>
<td>For details, see Adding Widgets to the Dashboard on page 3-4.</td>
</tr>
<tr>
<td>Create a new widget</td>
<td>Create a new, customized widget to track and monitor information</td>
</tr>
<tr>
<td></td>
<td>of interest to you.</td>
</tr>
<tr>
<td></td>
<td>For details, see Creating a Widget on page 3-5.</td>
</tr>
<tr>
<td>TASK</td>
<td>STEPS</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Refresh a widget</td>
<td>Click the menu icon in the top-right corner of the widget, and then select the refresh icon.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Widget views refresh automatically. Different widgets can have different refresh times.</td>
</tr>
<tr>
<td>Edit a widget</td>
<td>Click the menu icon in the top-right corner of the widget, and then select the edit icon. The <strong>Edit Widget</strong> dialog displays.</td>
</tr>
<tr>
<td></td>
<td>For more details, see <strong>Editing a Widget on page 3-6</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Different types of widgets have different settings to configure.</td>
</tr>
<tr>
<td>Delete a widget</td>
<td>Click the menu icon in the top-right corner of the widget, and then select the delete icon.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Widgets can also be deleted from the <strong>Add Widgets</strong> screen. Deleting a widget from the <strong>Add Widgets</strong> screen affects all instances that are already on the dashboard, and the deleted widgets cannot be restored.</td>
</tr>
<tr>
<td>Move a widget</td>
<td>Drag a widget's title change the widget's position.</td>
</tr>
<tr>
<td>Resize a widget</td>
<td>Drag the resize icon in the bottom-right corner of the widget to resize the widget.</td>
</tr>
</tbody>
</table>

**Adding Widgets to the Dashboard**

**Procedure**

1. Go to the **Dashboard** screen and do any of the following:
• Select the tab you wish to add widgets to, click the menu icon beside the tab title, and then select Add Widgets.

• Select the tab you wish to add widgets to, click the gear icon in the top-right corner of the screen, and then select Add Widgets.

• On newly created tabs, click Add a widget.

The Add Widgets screen displays.

2. To find a widget to add, do any of the following:

• To reduce the number of widgets displayed, select a category from the drop-down list.

• To search for a widget, type the widget name or partial widget name in the search text box at the top of the screen.

   **Tip**

   You can also create custom widgets to add to the dashboard. For details, see *Creating a Widget on page 3-5*.

3. Select the widgets to add to the dashboard. Each tab on the dashboard can contain up to 8 widgets.

4. Click Add.

   The selected widgets are added to the dashboard.

---

**Creating a Widget**

**Procedure**

1. Go to the Dashboard screen and select any tab.

2. Click the gear icon in the top-right corner of the screen, and then select Create New Widget.

   The Create New Widget screen displays.
3. Configure the following:
   a. Type a unique name for this widget.
   b. Select the filter to use for this widget. Only **Network Detections** and **Email Messages** saved searches can be selected. For details, see *Network Detections Advanced Search Filter on page 4-64* and *Email Messages Advanced Search Filter on page 4-81*.
   c. Type a description for this widget.
   d. Select the chart type and configure the data to display.

---

**Note**

- Different chart types have different settings to configure.
- Regardless of the selected time period, example charts are generated using data from only the last 24 hours.

---

4. Click **Save**.

   The widget is created and added to the **Add Widgets** screen.

---

**Editing a Widget**

---

**Procedure**

1. Go to the **Dashboard** screen and select the tab that contains the widget you want to edit.

2. Click the menu icon in the top-right corner of the widget, and then select the edit icon.

   The **Edit Widget** dialog displays.

3. Configure the widget.
Note

- Different types of widgets have different settings to configure.
- No example charts are displayed in the dialog.

4. Click OK.

Deep Discovery Inspector Widgets

Deep Discovery Director (Consolidated Mode) includes the following Deep Discovery Inspector widgets:

**TABLE 3-1. Deep Discovery Inspector Widgets**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats at a Glance</td>
<td>This widget displays actionable information about six key metrics and links to the corresponding detection logs.</td>
</tr>
<tr>
<td>Top Affected Hosts</td>
<td>This widget displays hosts with the highest severity rating by severity in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.</td>
</tr>
<tr>
<td>Scanned Traffic by Protocol Type</td>
<td>This widget displays total traffic volume by protocol, in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.</td>
</tr>
<tr>
<td>Threat Geographic Map - C&amp;C Communications</td>
<td>This widget displays a graphical representation of the affected hosts with C&amp;C communication detections on a virtual world map within the last 1 hour/24 hours/7 days/14 days/30 days/90 days.</td>
</tr>
</tbody>
</table>

Threats at a Glance

This widget displays actionable information about six key metrics and links to the corresponding detection logs.
## Table 3-2. Threats at a Glance

<table>
<thead>
<tr>
<th>Metric</th>
<th>Source</th>
<th>Description</th>
<th>Counted or Associated Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted attack detections</td>
<td>Affected Hosts</td>
<td>• Counts Affected Hosts&lt;br&gt;• Associated with the <strong>Targeted Attack detections</strong> preset search</td>
<td>Click a value to drill down to the <strong>Affected Hosts</strong> screen.</td>
</tr>
<tr>
<td>C&amp;C communication detections</td>
<td>Affected Hosts</td>
<td>• Counts Affected Hosts&lt;br&gt;• Associated with the <strong>C&amp;C Communication detections</strong> preset search</td>
<td>Click a value to drill down to the <strong>Affected Hosts</strong> screen.</td>
</tr>
<tr>
<td>Lateral movement detections</td>
<td>Affected Hosts</td>
<td>• Counts Affected Hosts&lt;br&gt;• Associated with the <strong>Lateral Movement detections</strong> preset search</td>
<td>Click a value to drill down to the <strong>Affected Hosts</strong> screen.</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Network Detections</td>
<td>• Counts detections&lt;br&gt;• Associated with the <strong>Ransomware</strong> preset search</td>
<td>Click on a value to drill down to the <strong>Network Detections</strong> screen.</td>
</tr>
<tr>
<td>Potential threats</td>
<td>Network Detections</td>
<td>• Counts detections&lt;br&gt;• Associated with the <strong>Potential Threats</strong> preset search</td>
<td>Click on a value to drill down to the <strong>Network Detections</strong> screen.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td><strong>Source</strong></td>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| Email threats    | Network Detections | • Counts detections  
• Associated with the Email Threats preset search  
Click on a value to drill down to the Network Detections screen. |

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

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

**Top Affected Hosts**

This widget displays hosts with the highest severity rating by severity in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

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

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

**Scanned Traffic by Protocol Type**

This widget displays total traffic volume by protocol, in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

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

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

**Threat Geographic Map - C&C Communications**

This widget displays a graphical representation of the affected hosts with C&C communication detections on a virtual world map within the last 1 hour/24 hours/7 days/14 days/30 days/90 days.
The Threat Geographic Map - C&C Communications displays regions with affected hosts as a solid red circle.

The default time period is Last 24 hours.

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

Deep Discovery Email Inspector Widgets

Deep Discovery Director (Consolidated Mode) includes the following Deep Discovery Email Inspector widgets:

**TABLE 3-3. Deep Discovery Email Inspector Widgets**

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Message Detection Summary</td>
<td>This widget displays the number of detections for different threat types.</td>
</tr>
<tr>
<td>Email Message Advanced Threat Indicators</td>
<td>This widget displays the type, amount, and risk level of advanced threat indicators detected in all email messages.</td>
</tr>
<tr>
<td>Email Message Attack Sources</td>
<td>This widget shows an interactive map representing all source MTAs that routed suspicious email traffic.</td>
</tr>
</tbody>
</table>

Email Message Detection Summary

This widget displays the number of detections for different threat types.

The graph is based on the selected period. The Y-axis represents the detection count. The X-axis represents the period. Mouse-over the points on the graph to view the period and number of detections.

Click a detection category in the legend to hide or show the related data on the graph.

The default time period is Last 24 hours.
Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

**Email Message Advanced Threat Indicators**

This widget displays the type, amount, and risk level of advanced threat indicators detected in all email messages.

The table shows detections based on the selected time period. Click a number under **High**, **Medium**, **Low**, or **Total** to learn more about the detections.

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

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.

---

**Note**

In the **Edit Widget** dialog, select **Unavailable** from the **Display data** drop-down list to display detections with **Unavailable** risk level.

---

**Email Message Attack Sources**

This widget shows an interactive map representing all source MTAs that routed suspicious email traffic.

An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), Deep Discovery Email Inspector identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

Mouse-over any point on the map to learn about the events that came from the attack source location.

Click any highlighted region on the map to learn more about attacks originating from that region.
The default time period is **Last 24 hours**.

Click the menu icon in the top-right corner of the widget, and then select the edit icon to configure the widget.
Chapter 4

Detections

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

- *About the Detections Screen on page 4-2*
- *Affected Hosts on page 4-12*
- *Network Detections on page 4-47*
- *Email Messages on page 4-73*
- *Ignore Rules on page 4-110*
About the Detections Screen

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

**TABLE 4-1. Detections**

<table>
<thead>
<tr>
<th>DETECTION CATEGORIES</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected Hosts</td>
<td>Hosts that have been involved in one or more phases of a targeted attack.</td>
</tr>
<tr>
<td></td>
<td>For details, see <a href="#">Affected Hosts on page 4-12</a>.</td>
</tr>
<tr>
<td></td>
<td>For details about the Host Severity scale, see <a href="#">Host Severity on page 4-3</a>.</td>
</tr>
<tr>
<td>Network Detections</td>
<td>Hosts with detections from all event logs, including global intelligence,</td>
</tr>
<tr>
<td></td>
<td>user-defined lists, and other sources.</td>
</tr>
<tr>
<td></td>
<td>For details, see <a href="#">Network Detections on page 4-47</a>.</td>
</tr>
<tr>
<td>Email Messages</td>
<td>Email messages that contain malicious or suspicious content, embedded links,</td>
</tr>
<tr>
<td></td>
<td>attachments, or social engineering attack related characteristics.</td>
</tr>
<tr>
<td></td>
<td>For details, see <a href="#">Email Messages on page 4-73</a>.</td>
</tr>
<tr>
<td></td>
<td>For details about email message risk levels, see <a href="#">Email Message Risk Levels on page 4-6</a>.</td>
</tr>
<tr>
<td></td>
<td>For details about email message threat type classifications, see <a href="#">Email Message Threat Type Classifications on page 4-9</a>.</td>
</tr>
</tbody>
</table>
### 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 4-2. Host Severity Scale**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Critical     | 10    | Host shows evidence of compromise including but not limited to the following:  
• Data exfiltration  
• Multiple compromised hosts/servers |
|              | 9     | Host exhibits an indication of compromise from APTs including but not limited to the following:  
• Connection to an IP address associated with a known APT  
• Access to a URL associated with a known APT  
• A downloaded file associated with a known APT  
• Evidence of lateral movement |
|              | 8     | Host may exhibit the following:  
• A high severity network event  
• Connection to a C&C Server detected by Web Reputation Services  
• A downloaded file rated as high risk by Virtual Analyzer |
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</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 |

Host is targeted by a known malicious behavior or attack and exhibits behavior that **likely** indicates host is compromised.

Host exhibits anomalous or suspicious behavior that may be benign or indicate a threat.
Table 1: Email Message Risk Levels

<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 Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Evidence of a running disruptive application such as P2P</td>
</tr>
</tbody>
</table>

Email Message Risk Levels

Deep Discovery Email Inspector assesses email message risk using multi-layered threat analysis. Upon receiving an email message, Deep Discovery Email Inspector email scanners check the email message for known threats in the Trend Micro Smart Protection Network and Trend Micro Advanced Threat Scanning Engine. If the email message has unknown or suspicious characteristics, the email scanners send file attachments and embedded URLs to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious file and URL behavior to identify potential threats. Deep Discovery Email Inspector assigns a risk level to the email message based on the highest risk assigned between the Deep Discovery Email Inspector scanners and Virtual Analyzer.

The following table explains the email message risk levels after investigation. View the table to understand why an email message was classified as high, medium, or low risk.
### TABLE 4-3. Email Message Risk Definitions

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| High       | A high-risk email message contains:  
  - Attachments with unknown threats detected as high risk by Virtual Analyzer  
  - Attachments detected as high risk based on YARA rules  
  - Attachments detected as high risk based on suspicious file matching  
  - Attachments detected by Predictive Machine Learning and Email Malware Threat Scan  
  - Business Email Compromise  
  - Links detected as high risk by Virtual Analyzer  
  - Links detected as high risk based on suspicious URL matching |
| Medium     | A medium-risk email message contains:  
  - Known malware  
  - Known phishing threats  
  - Known dangerous links  
  - Attachments detected as medium risk based on YARA rules  
  - Links detected as medium risk based on suspicious URL matching |
<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Low        | A low-risk email message contains:  
• Known highly suspicious or suspicious links (Aggressive mode)  
• Links detected as low risk by Virtual Analyzer  
• Attachments detected as low risk by Virtual Analyzer  
• Attachments detected as low risk based on YARA rules  
• Links detected as low risk based on suspicious URL matching  
• Social engineering attacks  
• Business Email Compromise (BEC) scams |
| No risk    | A no-risk email message:  
• Contains no suspicious attachments or links  
• Contains known highly suspicious or suspicious links (Standard mode)  
• Matches policy exception criteria |
### Risk Level Description

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Unrated    | An unrated email message falls under any of the following categories:  
  - Bypassed scanning: Contains an attachment with a compression layer greater than 20 (the file has been compressed over twenty times)  
  - Unscannable archive: Contains a password-protected archive that could not be extracted and scanned using the password list or heuristically obtained passwords  
  - Unscannable message or attachment: Matches any of the following criteria:  
    - Malformed email format  
    - A system timeout occurred when Virtual Analyzer attempted to analyze the message  
    - A system timeout occurred when Virtual Analyzer attempted to analyze some of the attachments or links and no other risks were detected  
    - Virtual Analyzer was unable to analyze all of the attachments or links and no other risks were detected |
| Unavailable | Deep Discovery Email Inspector does not assign a risk level to a spam/graymail message or an email message with content violation. |

### Email Message Threat Type Classifications

The following table explains the threat types detected during scanning or analysis. View the table to understand the malicious activity affecting your network.
### TABLE 4-4. Email Message Threat Types

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted malware</td>
<td>Malware made to look like they come from someone a user expects to receive email messages from, possibly a boss or colleague</td>
</tr>
<tr>
<td>Malware</td>
<td>Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems</td>
</tr>
<tr>
<td>Malicious URL</td>
<td>A hyperlink embedded in an email message that links to a known malicious web site</td>
</tr>
<tr>
<td>Suspicious File</td>
<td>A file that exhibits malicious characteristics</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Always handle suspicious files with caution.</td>
</tr>
<tr>
<td>Suspicious URL</td>
<td>A hyperlink embedded in an email message that links to an unknown malicious website</td>
</tr>
<tr>
<td>Phishing</td>
<td>Email messages that seek to fool users into divulging private information by redirecting users to legitimate-looking web sites</td>
</tr>
</tbody>
</table>
| Spam/Graymail     | Unsolicited spam email messages, often of a commercial nature, sent indiscriminately to multiple individuals  
                     | Graymail refers to solicited bulk email messages that are not spam             |
| Content violation | Content that you deem inappropriate, such as personal communication or large attachments |
Protocols That Support Advanced Analysis Using Correlation Data

Deep Discovery Director - Network Analytics provides correlation data for the following protocols:

- HTTP
- FTP
- RDP
- SMB/SMB2
- KRB5
- SMTP

Reasons Why No Correlations Are Found

There are certain reasons why Deep Discovery Director - Network Analytics reports that no correlations are found, including the following:

- Invalid parameters found while attempting to find correlations. Try again later after errors are resolved.
- Client errors were encountered while attempting to find correlations. Try again later after errors are resolved.
- Invalid response while attempting to find correlations. Try again later after errors are resolved.
- Internal errors were encountered while attempting to find correlations. Try again later after errors are resolved.
- No correlation provided because the selected incident originated from a client in the safe server list.
- No correlation provided because the protocol for the selected event is not supported.
• Currently, no correlation has been found for the selected incident. The system is still attempting to find correlations.

• No correlations have been found for the selected incident. No further attempts to find correlations will be made.

• No correlation provided because the selected event could not be found.

Affected Hosts

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

Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows you to prioritize and quickly respond. For details about the Host Severity scale, see Host Severity on page 4-3.

Access different information about Affected Hosts on the following views:

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

   By default, Deep Discovery Director (Consolidated Mode) searches the Affected Hosts view by IP Address and Host Name.

2. Host Details view:
   • Displays host event details in chronological order
   • Provides access to Detection Details views
   • By default, Deep Discovery Director (Consolidated Mode) searches the Affected Hosts - Host Details view by Peer Host.

3. Detection Details view:
   • Displays details of each detected threat
- Provides access to different information panels, depending on search and other filter criteria and settings

## Display Options and Search Filters

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

### Table 4-5. Display Options and Search Filters: Affected Hosts

<table>
<thead>
<tr>
<th><strong>Filter Options</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detection severity</strong></td>
<td>Filter options include the following detection severity settings:</td>
</tr>
<tr>
<td>High</td>
<td>Displays high severity detections</td>
</tr>
<tr>
<td>Medium</td>
<td>Displays medium severity detections</td>
</tr>
<tr>
<td>Low</td>
<td>Displays low severity detections</td>
</tr>
<tr>
<td>Informational</td>
<td>Displays informational detections</td>
</tr>
<tr>
<td>All detection severity levels</td>
<td>Displays all detections</td>
</tr>
<tr>
<td><strong>Period</strong></td>
<td></td>
</tr>
<tr>
<td>Last 24 hours</td>
<td></td>
</tr>
<tr>
<td>Last 7 days</td>
<td></td>
</tr>
<tr>
<td>Last 14 days</td>
<td></td>
</tr>
<tr>
<td>Last 30 days</td>
<td></td>
</tr>
<tr>
<td>Last 60 days</td>
<td></td>
</tr>
<tr>
<td>Custom range</td>
<td></td>
</tr>
<tr>
<td><strong>Data source</strong></td>
<td>Select which appliances to include as data source.</td>
</tr>
<tr>
<td><strong>Customize Columns</strong></td>
<td>Display optional columns.</td>
</tr>
<tr>
<td>Filter Options</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Basic search</td>
<td>Search for an IP address or host name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Type a case-insensitive keyword in the basic search field to search a partial host match.</td>
</tr>
<tr>
<td>Saved Searches</td>
<td>Search by saved search criteria.</td>
</tr>
<tr>
<td></td>
<td>• The <em>Affected Hosts</em> view includes the following built-in saved searches:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Targeted Attack detections</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>C&amp;C Communication detections</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Lateral Movement detections</strong></td>
</tr>
<tr>
<td></td>
<td>• The <em>Host Details</em> view includes the following preset searches:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Threats</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Known Threats</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Potential Threats</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Ransomware</strong></td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Search by user-defined criteria sets.</td>
</tr>
<tr>
<td></td>
<td>Each set includes one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• Attributes</td>
</tr>
<tr>
<td></td>
<td>• Operators</td>
</tr>
<tr>
<td></td>
<td>• Associated values</td>
</tr>
<tr>
<td></td>
<td>For details, see <em>Affected Hosts Advanced Search Filter on page 4-33</em>.</td>
</tr>
</tbody>
</table>
Viewing Affected Hosts

Procedure

1. Go to Detections > Affected Hosts.

   The Affected Hosts screen appears.

2. Select the detection severity level by using the drop-down control.

3. Select a time period.

4. Select which appliances to include as data source.

5. (Optional) Click the More icon beside Advanced, select Customize columns, select the columns to hide or display, and then click Apply to return to the modified Affected Hosts screen.

<table>
<thead>
<tr>
<th>TABLE 4-6. Host Information Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLUMN NAME</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>Network Group</td>
</tr>
<tr>
<td>Host Severity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Most Notable Threat</td>
</tr>
<tr>
<td>COLUMN NAME</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Latest Detection</td>
</tr>
</tbody>
</table>

**Note**

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

### TABLE 4-7. Notable Statistics Columns

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Attack</td>
<td></td>
<td>A threat that aims to exfiltrate data from a target system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>APT Attack Sequence on page 4-18.</em></td>
</tr>
</tbody>
</table>

### TABLE 4-8. Attack Phase Columns

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence Gathering</td>
<td>X</td>
</tr>
<tr>
<td>Point of Entry</td>
<td>X</td>
</tr>
</tbody>
</table>

Attackers identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack.

The initial compromise is typically from zero-day malware delivered via social engineering (email, IM, or drive-by download). A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.
<table>
<thead>
<tr>
<th><strong>COLUMN NAME</strong></th>
<th><strong>PRESELECTED</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>C&amp;C Communication</td>
<td>X</td>
<td>C&amp;C communication is typically used throughout the attack, allowing the attacker to instruct and control the malware used, and to exploit compromised machines, move laterally within the network, and exfiltrate data.</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>X</td>
<td>Once inside the network, an attacker compromises additional machines to harvest credentials, escalate privilege levels, and maintain persistent control.</td>
</tr>
<tr>
<td>Asset/Data Discovery</td>
<td>X</td>
<td>Several techniques (such as port scanning) are used to identify the noteworthy servers and the services that house the data of interest.</td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td>X</td>
<td>Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.</td>
</tr>
<tr>
<td>Unknown Attack Phase</td>
<td>X</td>
<td>Detection is triggered by a rule that is not associated with an attack phase.</td>
</tr>
</tbody>
</table>

6. To run a basic search, type an IP address or host name in the search text box, and then press ENTER or click the magnifying glass icon.

   By default, Deep Discovery Director (Consolidated Mode) searches Affected Hosts by IP Address and Host Name.

7. To run a saved search, click the Saved Searches icon, and then select a saved search.

   Deep Discovery Director (Consolidated Mode) provides the following built-in saved searches:
TABLE 4-9. Built-in Saved Searches

<table>
<thead>
<tr>
<th>NAME</th>
<th>FILTER OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts with Targeted Attack detections</td>
<td>Notable events in targeted attack</td>
</tr>
<tr>
<td>Hosts with C&amp;C Communication detections</td>
<td>Notable events in C&amp;C communication</td>
</tr>
<tr>
<td>Hosts with Lateral Movement detections</td>
<td>Notable events in lateral movement</td>
</tr>
</tbody>
</table>

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

For details, see Affected Hosts Advanced Search Filter on page 4-33.

9. (Optional) Click the More icon beside Advanced, select Export, select a delimiter to use, and then click OK to export and download the currently filtered list of affected hosts to a CSV file with the chosen delimiter.

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 4-10. 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>
</tbody>
</table>
Point of Entry

An initial compromise typically from zero-day malware delivered via social engineering (email/IM or drive-by download)

A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.

Command & Control (C&C) Communication

Communications used throughout an attack to instruct and control the malware used

C&C communication allows the attacker to exploit compromised machines, move laterally within the network, and exfiltrate data.

Lateral Movement

An attack that compromises additional machines

Once inside the network, an attacker can harvest credentials, escalate privilege levels, and maintain persistent control beyond the initial target.

Asset/Data Discovery

Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest

Data Exfiltration

Unauthorized data transmission to external locations

Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker’s control.

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

**Viewing Affected Hosts - Host Details**

**Procedure**

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

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

Details about the host are displayed.

3. Select the detection severity level by using the drop-down control.

4. Select a time period.

5. (Optional) Click the customize columns icon beside **Advanced Search**, select one or more optional columns for display, and click **Apply** to return to the modified **Host Details** screen.

**TABLE 4-11. General Columns**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>X</td>
</tr>
<tr>
<td>Details</td>
<td>X</td>
</tr>
<tr>
<td>Data Source</td>
<td>X</td>
</tr>
<tr>
<td>Source Host</td>
<td></td>
</tr>
<tr>
<td>Destination Host</td>
<td></td>
</tr>
<tr>
<td>Interested Host</td>
<td></td>
</tr>
<tr>
<td>Interested Network Group</td>
<td></td>
</tr>
<tr>
<td>Peer Host</td>
<td>X</td>
</tr>
<tr>
<td>Peer Network Group</td>
<td></td>
</tr>
<tr>
<td>Peer IP Country</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

The default **Timestamp**, **Details**, and **Threat Description** columns cannot be removed.
To run a basic search, type an IP address or host name in the search text box, and then press ENTER or click the magnifying glass icon.

By default, Deep Discovery Director (Consolidated Mode) searches **Affected Hosts - Host Details** by **Peer Host**.
7. To run a saved search, click the **Saved Searches** icon, and then select a saved search.

Deep Discovery Director (Consolidated Mode) provides the following built-in saved searches:

**TABLE 4-14. Built-in Saved Searches**

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

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

For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-39*.

9. Click **Export** to export the currently filtered list of host details.

The **Export** dialog appears.

10. Confirm the filters and select a delimiter to use.
11. Click **OK** to export and download the currently filtered list of host details to a CSV file with the chosen delimiter.

---

### Viewing Affected Hosts - Detection Details

**Procedure**

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

   Detection details about the event are displayed.

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

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

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

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

     **Important**

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

     The password for the zip archive is "virus".

3. In the **File Analysis Result** section, you may do the following:
• **Click View Virtual Analyzer Report** to view the Virtual Analyzer report.

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

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

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

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

---

**Important**

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

The password for the zip archive is "virus".

---

4. In the **Suspicious Object and Related File Analysis Result** section, view suspicious object and related analyzed file information.

---

**Affected Hosts - Detection Details**

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

- **Affected Hosts - Detection Details - Connection Details on page 4-25**
- **Affected Hosts - Detection Details - File Analysis Result on page 4-29**
- **Affected Hosts - Detection Details - Suspicious Object and Related File Analysis Result on page 4-32**
Affected Hosts - Detection Details - Connection Details

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

- *Affected Hosts - Detection Details - Detection Information on page 4-25*
- *Affected Hosts - Detection Details - Connection Summary on page 4-27*
- *Affected Hosts - Detection Details - Protocol Information on page 4-28*
- *Affected Hosts - Detection Details - File Information on page 4-29*
- *Affected Hosts - Detection Details - Additional Information on page 4-29*

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

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

If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file. In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

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

---

**Important**

- Suspicious files and pcap files must always be handled with caution. Extract the detected file and pcap file at your own risk. Trend Micro recommends analyzing the files in an isolated environment.
- The password for the zip archive is "virus".

---

**Affected Hosts - Detection Details - Detection Information**

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

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

---

**Tip**

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

---

• Detection severity
• Detection type
• Event class
• Notable Object
• Protocol
• Reference
• Targeted attack campaign
• Targeted attack related
• Threat
• Threat description
• Timestamp
• URL category
• Virtual Analyzer risk level

---

**Note**

Additional information may appear for specific correlated incidents.
### TABLE 4-15. Detection Types

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

**Affected Hosts - Detection Details - Connection Summary**

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

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

Affected Hosts - Detection Details - Protocol Information

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

• BOT command
• BOT URL
• Domain name
• Host name
• HTTP referer
• ICMP code
• ICMP type
• IRC channel name
• IRC nick name
• Message ID
• Protocol
• Queried domain
• Recipients
• Sender
• Subject
• Target share
• Transport Layer Security (TLS)
• URL
• User agent
• User name

Affected Hosts - Detection Details - File Information

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

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

Affected Hosts - Detection Details - Additional Information

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

• Attempted to disrupt connection
• Detected by
• Mitigation
• VLAN ID

Affected Hosts - Detection Details - File Analysis Result

The **File Analysis Result** section of the **Affected Hosts - Detection Details** screen contains the following information:
Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.

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

---

**Tip**

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

---

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

---

**Important**

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

The password for the zip archive is "virus".

---

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

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

---

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

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

- Child files
  - File name
  - File size (bytes)
• File type
• File SHA-1
• File name
• File size
• File type
• File MD5
• File SHA-1
• File SHA-256
• Threat
• Virtual Analyzer risk level

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

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

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

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

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

• Affected Hosts - Detection Details - Suspicious Object Information on page 4-32
• Affected Hosts - Detection Details - Related Analyzed File Information on page 4-32

Affected Hosts - Detection Details - Suspicious Object Information

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

• Related analyzed file
• Suspicious object
• Type
• Virtual Analyzer risk level

Affected Hosts - Detection Details - Related Analyzed File Information

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

• Child files
  • File name
  • File size (bytes)
  • File type
  • File SHA-1
• File name
• File size
• File type
• File MD5
• File SHA-1
• File SHA-256
• Threat
• Virtual Analyzer risk level

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

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

**Affected Hosts Advanced Search Filter**

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

• **Affected Hosts**

For details, see *About Affected Hosts Advanced Search Filter on page 4-34.*
• Affected Hosts - Host Details

For details, see About Affected Hosts - Host Details Advanced Search Filter on page 4-39.

About Affected Hosts Advanced Search Filter

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

**TABLE 4-16. Search Filter Criteria: Affected Hosts**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain/Starts with/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP Address</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>MAC Address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Notable Events</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Targeted Attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
</tbody>
</table>

For details, see the following:

• Adding an Affected Hosts Advanced Search Filter on page 4-35
• Editing an Affected Hosts Saved Search on page 4-36
• Importing Affected Hosts Saved Searches on page 4-38
Adding an Affected Hosts Advanced Search Filter

Procedure

1. To create an Affected Hosts advanced search filter, go to Detections > Affected Hosts, and then click Advanced.

2. Select an attribute and an associated operator.

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

   **Tip**
   Type a keyword to search a partial match.

   For details, see About Affected Hosts Advanced Search Filter on page 4-34.

   **Note**
   You can add multiple criteria entries by pressing ENTER after typing a value.

4. (Optional) Click AND or OR to include other criteria sets in the search filter.

5. Click Apply.

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

6. To save the search, do the following:
   a. Click the Save icon and select Save as.

      The Save As dialog appears.

   b. Type a name and an optional description, and then click Save.

      The name of the new saved search is added to the list of saved searches.
A saved search includes any search filter you create and the current customized column settings.

7. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

**Editing an Affected Hosts Saved Search**

**Procedure**

1. To edit an **Affected Hosts** saved search, go to **Detections > Affected Hosts**, and then click the **Saved Searches** icon.

2. Select a saved search to edit.

3. To edit the saved search, do one of the following:
   - Click the edit icon on the right side of the screen.
   - Click **Advanced**

4. Select an attribute and an associated operator.

5. Do one of the following to provide an action:
   - Type a value in the text box.
   - Select a value from the drop-down list.

**Tip**

Type a keyword to search a partial match.

For details, see *About Affected Hosts Advanced Search Filter on page 4-34*.

**Note**

You can add multiple criteria entries by pressing ENTER after typing a value.
6. (Optional) Click **AND** or **OR** to include other criteria sets in the search filter.

7. Click **Apply**.

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

8. To save the edited saved search, click the **Save** icon and do one of the following:
   - To save the edited saved search with the same name, select **Save**.
   - To save the edited saved search with a new name, select **Save as** and do the following:
     a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

---

**Note**

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

---

9. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

---

### Deleting an Affected Hosts Saved Searches

**Procedure**

1. To delete a **Affected Hosts** saved search, go to **Detections > Affected Hosts** and click the **Saved Searches** icon.

2. Click the delete icon beside the saved search to be deleted.

---

**Note**

Built-in filters cannot be deleted.
Importing Affected Hosts Saved Searches

Procedure

1. To import one or more Affected Hosts saved searches, go to Detections > Affected Hosts, and then click the Saved searches icon.

2. Click Import at the top of the Saved searches drop-down menu.
   
The Import to Saved Searches dialog appears.

3. Click Select to locate the file containing the saved searches.
   
The file is uploaded and validated.

4. Click Import.

   Note
   Importing overwrites existing saved searches with the same names.

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

Exporting Affected Hosts Saved Searches

Procedure

1. To export one or more Affected Hosts saved searches, go to Detections > Affected Hosts, and then click the Saved searches icon.

2. Click Export at the top of the Saved searches drop-down menu.
   
The Export Saved Searches dialog appears.

3. Select each saved search that you want to export or select the check box at the top of the column to export all saved searches. By default, all saved searches are selected for export.
Note

Built-in filters cannot be exported.

4. Click **Export**.

The saved searches file download begins.

**About Affected Hosts - Host Details Advanced Search Filter**

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

**TABLE 4-17. Search Filter Criteria: Affected Hosts - Host Details**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain/</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Starts with/Equals</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Contains/Does not contain/</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>MAC Address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>Contains/Does not contain/</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td>IP Country</td>
<td>In/Not in</td>
<td>Select one or more peer IP</td>
</tr>
<tr>
<td></td>
<td>countries</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td>Has user account/No user account</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Protocol</td>
<td>In/Not in</td>
<td>Select one or more protocols</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Over SSL/TLS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not over SSL/TLS</td>
</tr>
<tr>
<td>Direction</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External</td>
</tr>
<tr>
<td>Threat/Detection/Reference</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Correlation Rule ID (ICID)</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Type</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruptive Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Correlated Incident</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intelligence Gathering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Point of Entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset/Data Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Exfiltration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown Attack Phase</td>
</tr>
<tr>
<td>URL Category</td>
<td>In/Not in</td>
<td>Select one or more URL categories</td>
</tr>
<tr>
<td>C&amp;C List Source</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Global Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User-defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Relevance Rule</td>
</tr>
<tr>
<td>C&amp;C Callback Address</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>C&amp;C Risk Level</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td>Virtual Analyzer Result</td>
<td>Has analysis results/No analysis results</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PCAP File</td>
<td>Has PCAP file/No PCAP file</td>
<td></td>
</tr>
<tr>
<td>Is Targeted Attack Related</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No</td>
</tr>
<tr>
<td>File Detection Type</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Known Malware</td>
</tr>
<tr>
<td>File Name</td>
<td>Has file name/No file name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td>File SHA-1</td>
<td>Has file SHA-1/No file SHA-1/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equal</td>
<td></td>
</tr>
<tr>
<td>File SHA-256</td>
<td>Has file SHA-256/No file SHA-256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equal</td>
<td></td>
</tr>
<tr>
<td>IP Address/Domain/URL</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td>Suspicious Object/Deny List Entity</td>
<td>Contains/Does not contain/等于</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>Stars with/Equals</td>
<td></td>
</tr>
<tr>
<td>Sender (Email)</td>
<td>Has sender/No sender</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
### Adding an Affected Hosts - Host Details Advanced Search Filter

#### Procedure

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

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

   Details about the host are displayed.

3. Click **Advanced**.

4. Select an attribute and an associated operator.

5. Do one of the following to provide an action:
   - Type a value in the text box.

---

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient (Email)</td>
<td>Has recipient/No recipient</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td></td>
</tr>
<tr>
<td>Message ID (Email)</td>
<td>Has message ID/No message ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td></td>
</tr>
<tr>
<td>Subject (Email)</td>
<td>Has subject/No subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td></td>
</tr>
</tbody>
</table>

For details, see the following:

- *Adding an Affected Hosts - Host Details Advanced Search Filter on page 4-43*
- *Editing an Affected Hosts - Host Details Saved Search on page 4-45*
• Select a value from the drop-down list.

---

**Tip**

Type a keyword to search a partial match.

For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-39.*

---

**Note**

You can add multiple criteria entries by pressing ENTER after typing a value.

---

6. (Optional) Click **AND** or **OR** to include other criteria sets in the search filter.

7. Click **Apply**.

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

8. To save the search, do the following:
   
a. Click the **Save** icon and select **Save as**.

The *Save As* dialog appears.

b. Type a name and an optional description, and then click **Save**.

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

---

**Note**

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

---

9. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.
Editing an Affected Hosts - Host Details Saved Search

Procedure

1. Go to Detections > Affected Hosts.

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

   Details about the host are displayed.

3. Click the Saved Searches icon.

4. Select a saved search to edit.

5. To edit the saved search, do one of the following:
   - Click the edit icon on the right side of the screen.
   - Click Advanced

6. Select an attribute and an associated operator.

7. Do one of the following to provide an action:
   - Type a value in the text box.
   - Select a value from the drop-down list.

   Tip

   Type a keyword to search a partial match.

   For details, see About Affected Hosts - Host Details Advanced Search Filter on page 4-39.

---

Note

You can add multiple criteria entries by pressing ENTER after typing a value.

8. (Optional) Click AND or OR to include other criteria sets in the search filter.
9. Click **Apply**.

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

10. To save the edited saved search, click the **Save** icon and do one of the following:
    - To save the edited saved search with the same name, select **Save**.
    - To save the edited saved search with a new name, select **Save as** and do the following:
      a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

---

**Note**

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

---

11. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

---

**Deleting an Affected Hosts - Host Details Saved Search**

**Procedure**

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

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

   Details about the host are displayed.

3. Click the **Saved Searches** icon.
4. Click the delete icon beside the saved search to be deleted.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in filters cannot be deleted.</td>
</tr>
</tbody>
</table>

**Network Detections**

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

By default, Deep Discovery Director (Consolidated Mode) searches **Network Detections** by **Source Host**, **Destination Host** and **Interested Host**.

**Display Options and Search Filters**

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

**Table 4-18. Display Options and Search Filters: Network Detections**

<table>
<thead>
<tr>
<th><strong>FILTER OPTIONS</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection severity</td>
<td>Filter options include the following detection severity settings:</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>All detection severity levels</td>
</tr>
<tr>
<td>FILTER OPTIONS</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>Period</strong></td>
<td><strong>Last 24 hours</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Last 7 days</strong></td>
</tr>
<tr>
<td></td>
<td><strong>last 14 days</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Last 30 days</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Last 60 days</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Custom range</strong></td>
</tr>
<tr>
<td>Data source</td>
<td>Select which appliances to include as data source.</td>
</tr>
<tr>
<td>Customize Columns</td>
<td>Display optional columns.</td>
</tr>
<tr>
<td>Basic search</td>
<td>Search for an IP address or host name.</td>
</tr>
</tbody>
</table>

**Note**

Type a case-insensitive keyword in the basic search field to search a partial host match.
## Viewing Network Detections

### Procedure

1. Go to **Detections > Network Detections**.

   The **Network Detections** screen appears.
2. Select the detection severity level by using the drop-down control.

3. Select a time period.

4. Select which appliances to include as data source.

5. (Optional) Click the More icon beside Advanced, select Customize columns, select the columns to hide or display, and then click Apply to return to the modified Network Detections screen.

**TABLE 4-19. General Columns**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>X</td>
</tr>
<tr>
<td>Data Source</td>
<td>X</td>
</tr>
<tr>
<td>Details</td>
<td>X</td>
</tr>
<tr>
<td>Source Host</td>
<td>X</td>
</tr>
<tr>
<td>Destination Host</td>
<td>X</td>
</tr>
<tr>
<td>Interested Host</td>
<td>X</td>
</tr>
<tr>
<td>Interested Network Group</td>
<td></td>
</tr>
<tr>
<td>Peer Host</td>
<td></td>
</tr>
<tr>
<td>Peer Network Group</td>
<td></td>
</tr>
<tr>
<td>Peer IP Country</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

The default Timestamp column cannot be removed.

**TABLE 4-20. Email Columns**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-21. Detection Information Columns

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>PRESELECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td></td>
</tr>
<tr>
<td>Email Subject</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Threat Description</td>
<td>X</td>
</tr>
<tr>
<td>Detection Name</td>
<td>X</td>
</tr>
<tr>
<td>Threat (Virtual Analyzer)</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>Detection Type</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>X</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td></td>
</tr>
<tr>
<td>Detection Severity</td>
<td>X</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>X</td>
</tr>
<tr>
<td>URL Category</td>
<td></td>
</tr>
<tr>
<td>Direction</td>
<td></td>
</tr>
<tr>
<td>Notable Object</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note**

The default Threat Description column cannot be removed.

6. To run a basic search, type an IP address or host name in the search text box, and then press ENTER or click the magnifying glass icon.

By default, Deep Discovery Director (Consolidated Mode) searches Network Detections by Source Host, Destination Host, and Interested Host.
7. To run a saved search, click the **Saved Searches** icon, and then select a saved search.

Deep Discovery Director (Consolidated Mode) provides the following built-in saved searches:

**TABLE 4-22. Built-in Saved Searches**

<table>
<thead>
<tr>
<th>NAME</th>
<th>FILTER OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td>Known Threats</td>
<td>File Detection Types: Known Malware</td>
</tr>
<tr>
<td>Potential Threats</td>
<td>• Virtual Analyzer Result: Has analysis results</td>
</tr>
<tr>
<td></td>
<td>• File Detection type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td>Email Threats</td>
<td>Protocol options include the following:</td>
</tr>
<tr>
<td></td>
<td>• IMAP4</td>
</tr>
<tr>
<td></td>
<td>• POP3</td>
</tr>
<tr>
<td></td>
<td>• SMTP</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Detection name options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Ransomware-related detections</td>
</tr>
<tr>
<td>NAME</td>
<td>FILTER OPTIONS</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Detections with Correlation Data</td>
<td>Note: Deep Discovery Inspector must be integrated with Network Analytics servers to display correlation data.</td>
</tr>
</tbody>
</table>

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

   For details, see *Network Detections Advanced Search Filter on page 4-64*.

9. (Optional) Click the **More** icon beside **Advanced**, select **Export**, select a delimiter to use, and then click **OK** to export and download the currently filtered list of network detections to a CSV file with the chosen delimiter.

---

**Viewing Network Detections - Detection Details**

**Procedure**

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

   Detection details about the event are displayed.

2. In the **Connection Details** section, you may do the following:
   - Click **View in Threat Connect** to connect with **Threat Connect**, where you can search for current information about the threat.
   - Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.
   - If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File** to download a password protected ZIP archive containing the pcap file.
In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

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

---

**Important**

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

The password for the zip archive is "virus".

---

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

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

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

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

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

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

---

**Important**

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

The password for the zip archive is "virus".

---

4. **In the Suspicious Object and Related File Analysis Result** section, view suspicious object and related analyzed file information.
Network Detections - Detection Details

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

- Network Detections - Detection Details - Connection Details on page 4-55
- Network Detections - Detection Details - File Analysis Result on page 4-60
- Network Detections - Detection Details - Suspicious Object and Related File Analysis Result on page 4-62

Network Detections - Detection Details - Connection Details

The Connection Details section of the Network Detections - Detection Details screen can contain the following information:

- Network Detections - Detection Details - Detection Information on page 4-56
- Network Detections - Detection Details - Connection Summary on page 4-58
- Network Detections - Detection Details - Protocol Information on page 4-58
- Network Detections - Detection Details - File Information on page 4-59
- Network Detections - Detection Details - Additional Information on page 4-60

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

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

If a packet capture has been enabled and the detection matched a packet capture rule, click Download and then select PCAP File to download a password protected ZIP archive containing the pcap file. In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

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

- Suspicious files and pcap files must always be handled with caution. Extract the detected file and pcap file at your own risk. Trend Micro recommends analyzing the files in an isolated environment.
- The password for the zip archive is "virus".

Network Detections - Detection Details - Detection Information

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

- Activity detected
- Attack phase
- Correlation Rule ID (ICID)
- Detection name
- Detection rule ID
- Detection severity
- Event class
- Notable Object
- Protocol
- Reference
- Targeted attack campaign
- Targeted attack related
- Threat
- Threat description
- Detection type
- Timestamp
- URL category
• Virtual Analyzer risk level

**Note**
Additional information may appear for specific correlated incidents.

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

Network Detections - Detection Details - Connection Summary

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

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

Network Detections - Detection Details - Protocol Information

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

- BOT command
- BOT URL
- Domain name
- Host name
• HTTP referer
• ICMP code
• ICMP type
• IRC channel name
• IRC nick name
• Message ID
• Protocol
• Queried domain
• Recipients
• Sender
• Subject
• Target share
• Transport Layer Security (TLS)
• URL
• User agent
• User name

**Network Detections - Detection Details - File Information**

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

• File name
• File SHA-1
• File SHA-256
• File size
Network Detections - Detection Details - Additional Information

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

- Attempted to disrupt connection
- Detected by
- Mitigation
- VLAN ID

Network Detections - Detection Details - File Analysis Result

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

- Network Detections - Detection Details - File Analysis Result - File Information on page 4-61
- Network Detections - Detection Details - File Analysis Result - Notable Characteristics on page 4-61

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

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

---

Tip

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

---

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

---

Important

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

The password for the zip archive is "virus",
Click **Download** and then select **Detected File** to download a password protected ZIP archive containing the detected file.

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

**Network Detections - Detection Details - File Analysis Result - File Information**

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

- Child files
  - File name
  - File size (bytes)
  - File type
  - File SHA-1
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- Threat
- Virtual Analyzer risk level

**Network Detections - Detection Details - File Analysis Result - Notable Characteristics**

Information provided in the **File Analysis Result - Notable Characteristics** section of the **Detection Details** window may include characteristics that are commonly associated with malware. Characteristics are grouped into the following categories:
• Anti-security, self-preservation
• Autostart or other system reconfiguration
• Deception, social engineering
• File drop, download, sharing, or replication
• Hijack, redirection, or data theft
• Malformation or other known malware traits
• Process, service, or memory object change
• Rootkit, cloaking
• Suspicious network or messaging activity
• Other notable characteristic

Network Detections - Detection Details - Suspicious Object and Related File Analysis Result

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

• Network Detections - Detection Details - Suspicious Object Information on page 4-62
• Network Detections - Detection Details - Related Analyzed File Information on page 4-63

Network Detections - Detection Details - Suspicious Object Information

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

• Related analyzed file
• Virtual Analyzer risk level
• Suspicious object
• Type
Network Detections - Detection Details - Related Analyzed File Information

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

- Child files
  - File name
  - File size (bytes)
  - File type
  - File SHA-1
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- Threat
- Virtual Analyzer risk level

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

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

Network Detections Advanced Search Filter

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

For details, see the following:
• Adding a Network Detections Advanced Search Filter on page 4-69
• Editing a Network Detections Saved Search on page 4-70
• Importing Network Detections Saved Searches on page 4-72

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

TABLE 4-24. Search Criteria: Network Detections

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Contains/Does not contain/Starts with/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Interested Host</td>
<td>Contains/Does not contain/Starts with/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Peer Host</td>
<td>Contains/Does not contain/Starts with/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>IP Address</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Interested IP Address</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>Peer IP Country</td>
<td>In/Not in</td>
<td>Select one or more peer IP countries</td>
</tr>
<tr>
<td>MAC Address</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Network Group</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>User Account</td>
<td>Has user account/No user account</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Protocol</td>
<td>In/Not in</td>
<td>Select one or more protocols</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Over SSL/TLS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not over SSL/TLS</td>
</tr>
<tr>
<td>Direction</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External</td>
</tr>
<tr>
<td>Threat/ Detection/ Reference</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Rule ID</td>
<td>In/Not in</td>
<td>Type a range</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Correlation Rule ID (ICID)</td>
<td>In/Not in</td>
<td>Type a value</td>
</tr>
<tr>
<td>Detection Type</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Suspicious Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Exploit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Grayware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruptive Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Correlated Incident</td>
</tr>
<tr>
<td>Attack Phase</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intelligence Gathering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Point of Entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C&amp;C Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral Movement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset/Data Discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Exfiltration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown Attack Phase</td>
</tr>
<tr>
<td>URL Category</td>
<td>In/Not in</td>
<td>Select one or more URL categories</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>C&amp;C List Source</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Global Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Analyzer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User-defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Relevance Rule</td>
</tr>
<tr>
<td>C&amp;C Callback Address</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>C&amp;C Risk Level</td>
<td>In/Not in</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td>Virtual Analyzer Result</td>
<td>Has analysis results/No analysis results</td>
<td></td>
</tr>
<tr>
<td>PCAP File</td>
<td>Has PCAP file/No PCAP file</td>
<td></td>
</tr>
<tr>
<td>Is Targeted Attack Related</td>
<td>Equals</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No</td>
</tr>
<tr>
<td>File Detection Type</td>
<td>In</td>
<td>Select one or more of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Highly Suspicious File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Heuristic Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Known Malware</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>File Name</td>
<td>Has file name/No file name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain/ Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>File SHA-1</td>
<td>Has file SHA-1/No file SHA-1/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>File SHA-256</td>
<td>Has file SHA-256/No file SHA-256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Domain/URL</td>
<td>Contains/Does not contain/ Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Suspicious Object/Deny List Entity/ User-Defined SO</td>
<td>Contains/Does not contain/ Starts with/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Sender (Email)</td>
<td>Has sender/No sender</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Recipient (Email)</td>
<td>Has recipient/No recipient</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Message ID (Email)</td>
<td>Has message ID/No message ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Subject (Email)</td>
<td>Has subject/No subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
Adding a Network Detections Advanced Search Filter

Procedure

1. To create an **Network Detections** advanced search filter, go to **Detections > Network Detections**, and then click **Advanced**.

2. Select an attribute and an associated operator.

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

   **Tip**
   Type a keyword to search a partial match.
   For details, see **Network Detections Advanced Search Filter on page 4-64**.

   **Note**
   You can add multiple criteria entries by pressing ENTER after typing a value.

4. (Optional) Click **AND** or **OR** to include other criteria sets in the search filter.

5. Click **Apply**.

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

6. To save the search, do the following:
   a. Click the **Save** icon and select **Save as**.

      The **Save As** dialog appears.

   b. Type a name and an optional description, and then click **Save**.

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

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

7. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

Editing a Network Detections Saved Search

Procedure

1. To edit an Network Detections saved search, go to Detections > Network Detections, and then click the Saved Searches icon.

2. Select a saved search to edit.

3. To edit the saved search, do one of the following:
   • Click the edit icon on the right side of the screen.
   • Click Advanced

4. Select an attribute and an associated operator.

5. Do one of the following to provide an action:
   • Type a value in the text box.
   • Select a value from the drop-down list.

Tip

Type a keyword to search a partial match.

For details, see Network Detections Advanced Search Filter on page 4-64.

Note

You can add multiple criteria entries by pressing ENTER after typing a value.
6. (Optional) Click **AND** or **OR** to include other criteria sets in the search filter.

7. Click **Apply**.

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

8. To save the edited saved search, click the **Save** icon and do one of the following:
   - To save the edited saved search with the same name, select **Save**.
   - To save the edited saved search with a new name, select **Save as** and do the following:
     a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

---

**Note**

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

9. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

---

**Deleting a Network Detections Saved Search**

**Procedure**

1. To delete a **Network Detections** saved search, go to **Detections > Network Detections** and click the **Saved Searches** icon.

2. Click the delete icon beside the saved search to be deleted.

---

**Note**

Built-in filters cannot be deleted.
**Importing Network Detections Saved Searches**

**Procedure**

1. To import one or more **Network Detections** saved searches, go to **Detections > Network Detections**, and then click the **Saved searches** icon.

2. Click **Import** at the top of the **Saved searches** drop-down menu.
   - The **Import to Saved Searches** dialog appears.

3. Click **Select** to locate the file containing the saved searches.
   - The file is uploaded and validated.

4. Click **Import**.

   **Note**
   - Importing overwrites existing saved searches with the same names.

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

**Exporting Network Detections Saved Searches**

**Procedure**

1. To export one or more **Network Detections** saved searches, go to **Detections > Network Detections**, and then click the **Saved searches** icon.

2. Click **Export** at the top of the **Saved searches** drop-down menu.
   - The **Export Saved Searches** dialog appears.

3. Select each saved search that you want to export or select the check box at the top of the column to export all saved searches. By default, all saved searches are selected for export.
4. Click **Export**.

   The saved searches file download begins.

---

**Email Messages**

The **Email Messages** screen displays a list of email messages that have been detected to contain malicious or suspicious content, embedded links, attachments, or social engineering attack related characteristics. Deep Discovery Email Inspector assigns a risk rating to each email message based on the investigation results.

Query detected email messages to:

- Better understand the threats affecting your network and their relative risk
- Find senders and recipients of detected messages
- Understand the email subjects of detected messages
- Research attack sources that route detected messages
- Discover trends and learn about related detected messages
- See how Deep Discovery Email Inspector handled the detected message

**Display Options and Search Filters**

To customize the display, apply the following display options and search filters:
### Table 4-25. Display Options and Search Filters: Email Messages

<table>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level</td>
<td>Filter options include the following risk level settings:</td>
</tr>
<tr>
<td></td>
<td>High Displays high-risk email messages</td>
</tr>
<tr>
<td></td>
<td>Medium Displays medium-risk email messages</td>
</tr>
<tr>
<td></td>
<td>Low Displays low-risk email messages</td>
</tr>
<tr>
<td></td>
<td>Unavailable Displays spam/graymail messages and email messages with content violation</td>
</tr>
<tr>
<td></td>
<td>All Displays all email messages</td>
</tr>
<tr>
<td>Period</td>
<td>Last 24 hours</td>
</tr>
<tr>
<td></td>
<td>Last 7 days</td>
</tr>
<tr>
<td></td>
<td>last 14 days</td>
</tr>
<tr>
<td></td>
<td>Last 30 days</td>
</tr>
<tr>
<td></td>
<td>Last 60 days</td>
</tr>
<tr>
<td></td>
<td>Custom range</td>
</tr>
<tr>
<td>Monitored domain</td>
<td>Select domains from which email messages should be displayed.</td>
</tr>
<tr>
<td>Basic search</td>
<td>Type a case-insensitive keyword in the basic search field to search a partial sender, email header (from), recipient or email header (to) match.</td>
</tr>
<tr>
<td>Saved Searches</td>
<td>Search by saved search criteria.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Search by user-defined criteria sets. Each set includes one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>Attributes</td>
</tr>
<tr>
<td></td>
<td>Operators</td>
</tr>
<tr>
<td></td>
<td>Associated values</td>
</tr>
</tbody>
</table>
## Viewing Email Messages

Gain intelligence about the context of a spear-phishing attack by investigating a wide array of information facets. Review the email headers to quickly verify the email message origin and how it was routed. Investigate attacks trending on your network by correlating common characteristics (examples: email subjects that appear to be your Human Resource department or fake internal email addresses). Based on the detections, change your policy configuration and warn your users to take preventive measures against similar attacks.

### Procedure

1. Go to **Detections > Email Messages**.
   
   The **Email Messages** screen appears.

2. Select the risk level by using the drop-down control.

3. Select a time period.

4. Select domains from which email messages should be displayed.

5. (Optional) Click the **More** icon beside **Advanced**, select **Customize columns**, select the columns to hide or display, and then click **Apply** to return to the modified **Email Messages** screen.

6. To run a basic search, type a keyword in the search text box, and then press ENTER or click the magnifying glass icon.

   By default, Deep Discovery Director (Consolidated Mode) searches **Email Messages** by **Recipients, Email Header (To), Sender, Email Header (From)**.

7. To run a saved search, click the **Saved Searches** icon, and then select a saved search.

   By default, Deep Discovery Director (Consolidated Mode) provides the following built-in saved searches:

---

### Filter Options

<table>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize Columns</td>
<td>Customize the display by hiding or displaying columns.</td>
</tr>
</tbody>
</table>

---

4-75
Table 4-26. Built-in Saved Searches

<table>
<thead>
<tr>
<th>Name</th>
<th>Filter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Analyzer Result Available</td>
<td>Identified by: Virtual Analyzer</td>
</tr>
<tr>
<td>Suspicious Message Identified</td>
<td>Threat type options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Targeted malware</td>
</tr>
<tr>
<td></td>
<td>• Malware</td>
</tr>
<tr>
<td></td>
<td>• Malicious URL</td>
</tr>
<tr>
<td></td>
<td>• Suspicious File</td>
</tr>
<tr>
<td></td>
<td>• Suspicious URL</td>
</tr>
<tr>
<td></td>
<td>• Phishing</td>
</tr>
<tr>
<td>Spam/Graymail</td>
<td>Threat Type: Spam/Graymail</td>
</tr>
<tr>
<td>Content Violation</td>
<td>Threat Type: Content violation</td>
</tr>
<tr>
<td>Password-protected Attachment</td>
<td>Has password-protected attachment</td>
</tr>
</tbody>
</table>

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

For details, see Email Messages Advanced Search Filter on page 4-81.

9. (Optional) Click the More icon beside Advanced, select Export, select a delimiter to use, and then click OK to export and download the currently filtered list of email messages to a CSV file with the chosen delimiter.

Email Messages - Detection Details

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

- Email Messages - Detection Details - Overview on page 4-78
- Email Messages - Detection Details - Messages on page 4-79
Viewing Email Messages - Detection Details

Procedure

1. To view Email Messages detection details for any email message, click the icon under the Details column on the Email Messages screen. Details about the email message are displayed.

2. In the Connection Details section, you may do the following:
   - Click View Virtual Analyzer Report to view the analysis report in HTML format.
   - Click View in Threat Connect to connect with Threat Connect, where you can search for current information about the threat.
   - Click View Screenshot to safely display the email message as an image.
   - Click Download and then select Detection Details to download the detection details as CSV file.
   - Click Download and then select Detected Message to download a password protected ZIP archive containing the detected email message.
   - Click Download and then select Virtual Analyzer Report to download the Virtual Analyzer report in PDF format.
   - Click Download and then select Investigation Package to download a password protected ZIP archive containing the investigation package.
   - Click Download and then select All to download a password protected ZIP archive containing the detection details, detected message, Virtual Analyzer report, and investigation package.
Important

Suspicious files must always be handled with caution. Extract any archives at your own risk.

The password for the zip archive is "virus".

3. View details and information about the email message in the Overview, Messages, Attachments, Links, Message Characteristics, and Email Header sections.

Email Messages - Detection Details - Overview

View the message ID, recipients, last detection time, and sender and source IP addresses of the email message to understand where the message came from and other tracking information.

Get information about policy rules that the mail message violates.

Information provided in the Overview section may include the following:

- Risk level
- Timestamp
- Threat type
- Message ID
- Email subject
- Source IP
- Sender IP
- Sender
- Recipients
- Email header (from)
- Email header (to)
Email Messages - Detection Details - Messages

View the name of the scanning engine and the category for detected email messages that are considered as spam or graymail.

Information provided in the Messages section may contain the following:

- Identified by
- Category
- Threat

Email Messages - Detection Details - Attachments

Get information about any files attached to the email message, including the file name, password, file type, risk level, SHA-1 value, the scan engine that identified the threat, and the name of detected threats.

Information provided in the Attachments section may contain the following:

- File name
- Password
- File type
- Size (bytes)
- Risk level
- SHA-1
- Identified by
- Threat
Email Messages - Detection Details - Links

Get information about any embedded suspicious URLs that appeared in the email message, including the URL, site category, risk level, the scan engine that identified the threat, and the name of detected threats.

Information provided in the Links section may contain the following:

- URL
- Extraction source
- Site category
- Risk level
- Identified by
- Threat

Email Messages - Detection Details - Message Characteristics

Get information about any social engineering attack related characteristics that were detected in the email message, including the mail server reputation, gaps between transits, inconsistent recipient accounts, and forged sender addresses or unexpected relay servers, etc.

Information provided in the Message Characteristics section may contain the following:

- Detection
- Details

Email Messages - Detection Details - Email Header

View the email message header content. This information is the same as if you viewed the header in your local email client.
Email Messages Advanced Search Filter

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

For details, see the following:

- *Adding an Email Messages Advanced Search Filter on page 4-83*
- *Editing an Email Messages Saved Search on page 4-84*
- *Importing Email Messages Saved Searches on page 4-86*

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

**TABLE 4-27. Search Criteria: Email Messages**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Recipient</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Header (From)</td>
<td>Has from/No from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Header (To)</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Source IP</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>Source IP Country/Region</td>
<td>In/Not in</td>
<td>Select one or more source IP countries</td>
</tr>
<tr>
<td>Sender IP</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>OPERATOR</td>
<td>ACTION</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Sender IP Country/Region</td>
<td>In/Not in</td>
<td>Select one or more source IP countries</td>
</tr>
<tr>
<td>Message ID</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Subject</td>
<td>Has subject/No subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>URL</td>
<td>Has URL/No URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Like/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Attachment</td>
<td>Has attachment/No attachment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Password-protected Attachment</td>
<td>Yes/No</td>
<td></td>
</tr>
<tr>
<td>File SHA-1</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Threat Name</td>
<td>Contains/Does not contain/Equals/Starts with</td>
<td>Type a value</td>
</tr>
<tr>
<td>Threat Type</td>
<td>In/Not in</td>
<td>Select one or more threat types</td>
</tr>
<tr>
<td>Identified By</td>
<td>In/Not in</td>
<td>Select one or more identification sources</td>
</tr>
<tr>
<td>Policy</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Policy Rule</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>User Submitted</td>
<td>Yes/No</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>In/Not in</td>
<td>Select one or more actions</td>
</tr>
</tbody>
</table>
Adding an Email Messages Advanced Search Filter

Procedure

1. To create an Email Messages advanced search filter, go to Detections > Email Messages, and then click Advanced.

2. Select an attribute and an associated operator.

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

4. (Optional) Click AND or OR to include other criteria sets in the search filter.

5. Click Apply.

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

6. To save the search, do the following:

   a. Click the Save icon and select Save as.

      The Save As dialog appears.

   b. Type a name and an optional description, and then click Save.

      The name of the new saved search is added to the list of saved searches.
A saved search includes any search filter you create and the current customized column settings.

7. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

---

**Editing an Email Messages Saved Search**

**Procedure**

1. To edit an Email Messages saved search, go to Detections > Email Messages, and then click the Saved searches icon.

2. Select a saved search to edit.

3. To edit the saved search, do one of the following:
   - Click the edit icon on the right side of the screen.
   - Click Advanced

4. Select an attribute and an associated operator.

5. Do one of the following to provide an action:
   - Type a value in the text box.
   - Select a value from the drop-down list.

**Tip**

Type a keyword to search a partial match.

**Note**

You can add multiple criteria entries by pressing ENTER after typing a value.

6. (Optional) Click AND or OR to include other criteria sets in the search filter.
7. Click **Apply**.

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

8. To save the edited saved search, click the **Save** icon and do one of the following:
   - To save the edited saved search with the same name, select **Save**.
   - To save the edited saved search with a new name, select **Save as** and do the following:
     a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

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

9. (Optional) Click the right-arrow icon beside the saved searches drop-down list to close the advanced search feature.

### Deleting an Email Messages Saved Search

**Procedure**

1. To delete a **Email Messages** saved search, go to **Detections > Email Messages** and click the **Saved searches** icon.

2. Click the delete icon beside the saved search to be deleted.

   **Note**
   Built-in filters cannot be deleted.
Importing Email Messages Saved Searches

Procedure

1. To import one or more Email Messages saved searches, go to Detections > Email Messages, and then click the Saved searches icon.

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

   The Import to Saved Searches dialog appears.

3. Click Select to locate the file containing the saved searches.

   The file is uploaded and validated.

4. Click Import.

   Note
   Importing overwrites existing saved searches with the same names.

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

Exporting Email Messages Saved Searches

Procedure

1. To export one or more Email Messages saved searches, go to Detections > Email Messages, and then click the Saved searches icon.

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

   The Export Saved Searches dialog appears.

3. Select each saved search that you want to export or select the check box at the top of the column to export all saved searches. By default, all saved searches are selected for export.
4. Click **Export**.

The saved searches file download begins.

---

**Correlated Events**

The Correlated Events screen displays a list of events that show one or more attack patterns derived from the correlated data of multiple detections in your network.

**Display Options and Search Filters**

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

**Table 4-28. Display Options and Search Filters: Correlated Events**

<table>
<thead>
<tr>
<th><strong>FILTER OPTIONS</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Filter options include the following severity settings:</td>
</tr>
<tr>
<td>High</td>
<td>Displays high severity events</td>
</tr>
<tr>
<td>Medium</td>
<td>Displays medium severity events</td>
</tr>
<tr>
<td>Low</td>
<td>Displays low severity events</td>
</tr>
<tr>
<td>All</td>
<td>Displays all events</td>
</tr>
<tr>
<td>Filter Options</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Period</td>
<td>Last 24 hours</td>
</tr>
<tr>
<td></td>
<td>Last 7 days</td>
</tr>
<tr>
<td></td>
<td>Last 14 days</td>
</tr>
<tr>
<td></td>
<td>Last 30 days</td>
</tr>
<tr>
<td></td>
<td>Last 60 days</td>
</tr>
<tr>
<td></td>
<td>Custom range</td>
</tr>
</tbody>
</table>
### Filter Options

<table>
<thead>
<tr>
<th>Filter Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Pattern</td>
<td>Filter options include the following attack patterns:</td>
</tr>
<tr>
<td>All attack patterns</td>
<td>Displays all events</td>
</tr>
<tr>
<td>Brute Force</td>
<td>Displays events with brute force authentication attack patterns</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>CnC Callback</td>
<td>Displays events with C&amp;C callback attack patterns</td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td>Displays events with data exfiltration attack patterns</td>
</tr>
<tr>
<td>Lateral Probing</td>
<td>Displays events with lateral probing attack patterns</td>
</tr>
<tr>
<td>Malicious Download</td>
<td>Displays events with malicious download attack patterns</td>
</tr>
<tr>
<td>Phone Home</td>
<td>Displays events with phone home attack patterns</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Displays events with vulnerability exploit attack patterns</td>
</tr>
<tr>
<td>Exploit</td>
<td></td>
</tr>
<tr>
<td>Other Malicious</td>
<td>Displays events with malicious activity attack patterns</td>
</tr>
<tr>
<td>Activities</td>
<td></td>
</tr>
<tr>
<td>Undefined</td>
<td>Displays events with undefined attack patterns</td>
</tr>
<tr>
<td>Data source</td>
<td>Select which appliances to include as data source.</td>
</tr>
<tr>
<td>Basic search</td>
<td>Search for an interested IP address.</td>
</tr>
</tbody>
</table>
Viewing Correlated Events

Procedure

1. Go to Detections > Correlated Events.
   The Correlated Events screen appears.
2. Select the severity level by using the drop-down control.
3. Select the attack patterns by using the drop-down control.
4. Select a time period.
5. Select which appliances to include as data source.
6. To run a basic search, type an IP address in the search text box, and then press ENTER or click the magnifying glass icon.

Viewing Correlated Events - Correlation Data

Procedure

1. To view correlation data for any event, click the Correlation Data icon (.symbol) under the Details column on the Correlated Events screen.
   The Deep Discovery Director - Network Analytics Correlation Data screen appears.
2. Use the following sections for advanced analysis of malicious activity:
   • Summary
     Provides a high-level overview of the malicious activity, risk level, and risk analysis for this correlation data.
   • Correlation Graph
     Provides a visual representation of correlations made between the detection object selected in Deep Discovery Director and other related events as they occur over time.
• **Transaction Details**

Provides details about each transaction represented in the correlation graph. Transactions are listed from oldest correlated events at the top to the most recent correlated event at the bottom.

---

**Tip**

Information displayed in the **Deep Discovery Director - Network Analytics Correlation Data** screen is created dynamically. The number of correlations and details about interactions and malicious activity between hosts presented in the **Deep Discovery Director - Network Analytics Correlation Data** screen can change over time. You can access the correlation data for a specific detection at a later time to see if additional analysis details are available.

---

3. For details on how to use the information displayed in the **Deep Discovery Director - Network Analytics Correlation Data** screen to assist in advanced analysis, see *Analyzing Correlation Data Information on page 4-91*.

---

**Analyzing Correlation Data Information**

- *Overview of the Correlation Data Screen on page 4-91*
- *Reviewing the Correlation Data Summary on page 4-92*
- *Analysis Using the Correlation Data Graph on page 4-94*
- *Analysis Using Transaction Data on page 4-99*

**Overview of the Correlation Data Screen**

The **Correlation Data** screen consists of the following main sections:

- **Summary**
- **Correlation Data Graph**
- **Transaction Data**
Summary

The Summary section provides a high-level overview of the malicious activity, risk level, and risk analysis for the correlation data.

You can click on [Show detection history] for more summary details.

See Reviewing the Correlation Data Summary on page 4-92.

Correlation Data Graph

The Correlation Data Graph section is a visual representation of correlations made between the correlated event or suspicious object selected in Deep Discovery Director and other related events as they occur over time.

See Analysis Using the Correlation Data Graph on page 4-94.

Transaction Data

The Transaction Data section provides details about each transaction that is represented in the Correlation Data Graph section.

Transactions are listed from oldest transaction at the top to the most recent transaction at the bottom. Listed transactions might have occurred in a single day or might span several months, depending on the correlations found by Deep Discovery Director - Network Analytics.

See Analysis Using Transaction Data on page 4-99.

Reviewing the Correlation Data Summary

The Correlation Data Summary section provides a high-level overview of the malicious activity, risk level, and risk analysis of the correlation data for the correlation event or suspicious object selected from Deep Discovery Director.

Procedure

1. Review the risk and activity summary.

   The summary provides the following information:
2. **Review more detailed summary data by clicking on **Show detection history.**

The detection history provides the following information:

<table>
<thead>
<tr>
<th>Start IP address</th>
<th>Displays the IP address found in the Interested IP field of the correlated event selected in Deep Discovery Director.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The detection history for suspicious objects does not contain a start IP address entry.</td>
</tr>
</tbody>
</table>
Summary details

- Summary details shown are log event entries sent by Deep Discovery Inspector for correlated events.
- Summary sections can include log event entries such as the following:
  - Intelligence Gathering
  - Point of Entry
  - Command and Control Communications
  - Asset and Data Discovery
  - Lateral Movement
  - Data Exfiltration

3. Click on **Hide detection history** to hide the detailed summary information.

Analysis Using the Correlation Data Graph

Open the Correlation Data screen from Deep Discovery Director to see the Correlation Data Graph for the selected event.

The Correlation Data Graph is a visual representation of correlations made between the correlated event or suspicious object selected in the Deep Discovery Director and other related events as they occurred over time.

Procedure

- From the main screen, perform initial analysis:

<table>
<thead>
<tr>
<th>ELEMENT IN CORRELATION DATA GRAPH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIGURE 4-1. Playback Bar</strong></td>
</tr>
</tbody>
</table>

Click on the playback bar to view the time line for the correlated events. Deep Discovery Director - Network Analytics draws the oldest correlation event first and continues through to the latest correlation.
Correlation Line

- Each correlation graph contains one or more correlation lines that correlate malicious or suspicious activity between a source and destination.
- Each correlation can be between an internal host and external server or between two internal hosts (lateral correlations).
- For each internal host and external server, the host name is supplied if known.
  - For internal hosts, the user name for that host is supplied if known.
- The circular icon embedded in each line displays the number of transactions associated with each correlation.
- The color of each circular icon represents the protocol used in the correlation.

Legend

Provides information about protocols used in correlation data transactions and other information such as the Detected Threat correlation line color and certain icons used in the graph such as the “Priority Watch List” icon.

<table>
<thead>
<tr>
<th>Detected Threat</th>
<th>Priority Watch List</th>
<th>HTTP</th>
<th>FTP</th>
</tr>
</thead>
</table>

**Figure 4-2. Example: Legend**

Detected Threat

Represents the correlated event selected in Deep Discovery Director.

The interaction is generally between an internal host and external server and is identified by the orange line connecting the source and destination.

**Note**

Suspicious Object detections selected from Deep Discovery Director generally do not generate a Detected Threat correlation.
**Element in Correlation Data Graph**

<table>
<thead>
<tr>
<th>Activity Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies key activities for the internal host and external server participants in the graph.</td>
</tr>
<tr>
<td>- Activities vary for each specific correlation data graph.</td>
</tr>
<tr>
<td>- Can include activities similar to the following: Lateral Activity, Detected Event, C&amp;C Activity, and Malicious Download</td>
</tr>
<tr>
<td>- Actions correspond to “Reason” in Deep Discovery Inspector logs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Participant Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can determine the activities in which each internal host or external server participated.</td>
</tr>
<tr>
<td>- Participant icons indicate if an internal host or external server is a participant in a specific activity.</td>
</tr>
<tr>
<td>- Hover over a internal host or external server to see the activities in which they are participants.</td>
</tr>
<tr>
<td>- Also determine which internal hosts or external servers were the source or endpoint for an activity.</td>
</tr>
<tr>
<td>- Participant: 🔴</td>
</tr>
<tr>
<td>- Non-participant: 🔵</td>
</tr>
</tbody>
</table>
**ELEMENT IN CORRELATION DATA GRAPH**

<table>
<thead>
<tr>
<th>Correlation - Details Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Hover over a correlation line to see more details about that correlation.</td>
</tr>
<tr>
<td>• Details include:</td>
</tr>
<tr>
<td>• Source IP, user name, and host name</td>
</tr>
<tr>
<td>• Destination IP</td>
</tr>
<tr>
<td>• Severity</td>
</tr>
<tr>
<td>• Detected URLs and SHA1s (if any)</td>
</tr>
<tr>
<td>• Protocols and number of transactions</td>
</tr>
<tr>
<td>• Reason</td>
</tr>
<tr>
<td>The listed reason corresponds to an activity in the <strong>Activity Legend</strong>.</td>
</tr>
<tr>
<td>• Earliest date and latest date</td>
</tr>
</tbody>
</table>
**Element in Correlation Data Graph**

**Correlation - Transactions Details Window**

You can view transaction details for a correlation.

- For each interaction, the number of transactions between the source and endpoint is specified within the transaction number icon (color-coded for the protocol used for those transactions).

  Examples of transaction number icons: [2], [3]

- Click on a transaction number icon to view details about all transactions for that correlation.

- Oldest transactions are at the top of the page. If necessary, scroll down to see newer transactions.

- Each transaction number in the list represents where the transaction falls in the timeline for all transactions in the correlation data graph (including transactions from other correlation lines).

The transaction detail window provides the following information:

- Source and destination for the correlation.
- The number of transactions and protocol for the correlation.
- Details for each transaction
  - Transaction number
  - Risk assigned to each transaction
  - Details specific to each protocol.
  - Date of each transaction

**Additional Actions**

You can click the plus-sign icon (+) located on the left-hand side of each internal host and external server to view a list of additional actions you can perform for that host.

Actions for Internal Hosts: View other correlations for this host

Actions for External Servers: Retrieve information for this external server from Threat Connect, VirusTotal, or Domain Tools
**Element in Correlation Data Graph**

<table>
<thead>
<tr>
<th>Special Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional icons provide information about elements in the correlation graph.</td>
</tr>
<tr>
<td>• Member of <strong>Priority Server List</strong>: ![Priority Server List Icon]</td>
</tr>
<tr>
<td>• Correlation event originated from an email: ![Email Icon]</td>
</tr>
</tbody>
</table>

From the indicated host, a user clicked on a URL, downloaded a file, or performed a related action that triggered a correlated event in the correlation time line. A correlation line for the SMTP transaction containing malicious content is not present in the correlation data; however, the email icon indicates that a malicious email was the origin of the subsequent correlated event. For example, if a user receives an email with a link to a malicious URL but does not click on the link, a correlation is not triggered. If the user clicks on the malicious URL, an HTTP correlation is triggered.

---

**Analysis Using Transaction Data**

The **Transaction Data** section provides details about each transaction included in the correlations from the **Correlation Graph** section.

The oldest transaction are listed first.

---

**Procedure**

- Scroll through the transaction data list to identify information useful for analysis.
- Note details such as the following:
  - Transaction number, protocol, source and destination IP address
  - Risk level
  - Transaction details, which vary for each protocol
  - Date of the transaction
Viewing Correlated Events - Detection Details

Procedure

1. To view detection details for any event, click the Details icon under the Details column on the Correlated Events screen.

   Detection details about the event are displayed.

2. In the Connection Details section, you may do the following:
   - Click View in Threat Connect to connect with Threat Connect, where you can search for current information about the threat.
   - Click Download and then select Detected File to download a password protected ZIP archive containing the detected file.
   - If a packet capture has been enabled and the detection matched a packet capture rule, click Download and then select PCAP File to download a password protected ZIP archive containing the pcap file.
     In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.
   - Click Download and then select All to download a password protected ZIP archive containing the detected file, the packet capture file, and the connection details.

   Important

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

   The password for the zip archive is "virus".

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

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

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

---

**Important**

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

The password for the zip archive is "virus".

---

4. In the **Suspicious Object and Related File Analysis Result** section, view suspicious object and related analyzed file information.

---

**Correlated Events - Detection Details**

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

• **Correlated Events - Detection Details - Connection Details on page 4-101**

• **Correlated Events - Detection Details - File Analysis Result on page 4-106**

• **Correlated Events - Detection Details - Suspicious Object and Related File Analysis Result on page 4-109**

---

**Correlated Events - Detection Details - Connection Details**

The **Connection Details** section of the **Correlated Events - Detection Details** screen can contain the following information:

• **Correlated Events - Detection Details - Detection Information on page 4-102**
• Correlated Events - Detection Details - Connection Summary on page 4-104
• Correlated Events - Detection Details - Protocol Information on page 4-105
• Correlated Events - Detection Details - File Information on page 4-106
• Correlated Events - Detection Details - Additional Information on page 4-106

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

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

If a packet capture has been enabled and the detection matched a packet capture rule, click Download and then select PCAP File to download a password protected ZIP archive containing the pcap file. In the pcap file, the comment "Detected Packet" in the "pkt_comment" field marks the packet that triggered the detection.

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

---

**Important**

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

- The password for the zip archive is "virus".

---

**Correlated Events - Detection Details - Detection Information**

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

- Activity detected
- Attack phase
- Correlation Rule ID (ICID)
- Detection name
- Detection rule ID
• Detection severity
• Event class
• Notable Object
• Protocol
• Reference
• Targeted attack campaign
• Targeted attack related
• Threat
• Threat description
• Detection type
• Timestamp
• URL category
• Virtual Analyzer risk level

**Note**
Additional information may appear for specific correlated incidents.

**Table 4-29. Detection Types**

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

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

### Correlated Events - Detection Details - Connection Summary

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

- A graphical display that includes the direction of the event and other information. The **Client** in the diagram is the host that initiated the connection.

- Host details may include the following:
• Host name
• IP address and port
• Last logon user
• MAC address
• Network group
• Network zone
• Operating system

Correlated Events - Detection Details - Protocol Information

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

• BOT command
• BOT URL
• Domain name
• Host name
• HTTP referer
• ICMP code
• ICMP type
• IRC channel name
• IRC nick name
• Message ID
• Protocol
• Queried domain
• Recipients
• Sender
• Subject
• Target share
• Transport Layer Security (TLS)
• URL
• User agent
• User name

**Correlated Events - Detection Details - File Information**

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

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

**Correlated Events - Detection Details - Additional Information**

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

• Attempted to disrupt connection
• Detected by
• Mitigation
• VLAN ID

**Correlated Events - Detection Details - File Analysis Result**

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

- **Correlated Events - Detection Details - File Analysis Result - File Information on page 4-107**
Click **View Virtual Analyzer Report** to view the Virtual Analyzer report.

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

---

**Tip**

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

---

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

---

**Important**

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

The password for the zip archive is "virus".

---

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

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

**Correlated Events - Detection Details - File Analysis Result - File Information**

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

- Child files
  - File name
  - File size (bytes)
  - File type
• File SHA-1
• File name
• File size
• File type
• File MD5
• File SHA-1
• File SHA-256
• Threat
• Virtual Analyzer risk level

**Correlated Events - Detection Details - File Analysis Result - Notable Characteristics**

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

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

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

- Correlated Events - Detection Details - Suspicious Object Information on page 4-109
- Correlated Events - Detection Details - Related Analyzed File Information on page 4-109

Correlated Events - Detection Details - Suspicious Object Information

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

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

Correlated Events - Detection Details - Related Analyzed File Information

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

- Child files
  - File name
  - File size (bytes)
  - File type
  - File SHA-1
- File name
- File size
- File type
• File MD5
• File SHA-1
• File SHA-256
• Threat
• Virtual Analyzer risk level

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

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

**Ignore Rules**

The **Ignore Rules** feature allows you to hide specific detection logs from the management console, and to ignore those detection logs when displaying information.
Ignore Rules Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an ignore rule</td>
<td>Ignore rules are created using the Network Detections or Email Messages Advanced Search filter. For details, see Creating an Ignore Rule on page 4-111.</td>
</tr>
<tr>
<td>View rule details</td>
<td>Hover on any text in the Criteria or Description columns to view the details of the ignore rule.</td>
</tr>
<tr>
<td>Delete rule</td>
<td>Select one or more ignore rules to delete and then click Delete.</td>
</tr>
<tr>
<td>Toggle rule status</td>
<td>Click on the toggle in the Status column to enable or disable the ignore rule.</td>
</tr>
</tbody>
</table>

**Important**

By default, ignore rules are disabled. Enabling a rule causes matching detection logs to be hidden from the management console, and to be ignored when displaying information.

Creating an Ignore Rule

**Procedure**

1. To create an ignore rule, go to Detections > Network Detections or Detections > Email Messages, and then click Advanced.

2. Select an attribute and an associated operator.

3. Do one of the following to provide an action:
   - Type a value in the text box.
   - Select a value from the drop-down list.
4. (Optional) Click **AND** or **OR** to include other criteria sets in the search filter.

5. Click **Create Ignore Rule**.

   The **Create Ignore Rule** dialog appears.

6. Type a name for this rule.

7. (Optional) Type a description for this rule.

8. Click **Save**.

   The ignore rule is created and can be enabled from the **Detections > Ignore Rules** screen.
Chapter 5

Threat Intelligence

Learn about threat intelligence and related tasks in the following topics:

- *Product Intelligence on page 5-2*
- *Custom Intelligence on page 5-11*
- *Feed Management on page 5-29*
- *Sharing Settings on page 5-31*
Product Intelligence

Deep Discovery Director (Consolidated Mode) consolidates threat intelligence from managed appliances.

Synchronized Suspicious Objects

The Synchronized Suspicious Objects screen displays a list of suspicious objects detected by Virtual Analyzer.

Suspicious object detections can be sorted by Object, Type, Risk Level, Sync Source, Expiration, and Detections.

Viewing Synchronized Suspicious Objects

View synchronized suspicious objects to understand your risk, find related detections, and assess the relative prevalence of the suspicious object.

Procedure

1. Go to Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects.

   The Synchronized Suspicious Objects screen appears.

2. Click the drop-down for detection type and then select one of the following detection types:
   - All (default)
   - IP addresses
   - URLs
   - File SHA-1
   - Domains

3. To configure display settings, hover over the Network Detections or Email Messages icon in the column title and select Display Settings.
The **Display Settings** dialog appears.

4. Select a time period.

5. Select which appliances to include as data source, and domains from which email messages should be displayed.

   **Note**
   
   The time period, data source, and monitored domain filters only affect the **Detections** numbers.

6. To run a search, type an IP address, domain, URL or SHA-1 hash value in the search text box, and then press ENTER or click the magnifying glass icon.

7. (Optional) Click a number in the **Network Detections** or **Email Messages** column to drill-down to the **Network Detections** or **Email Messages** screen with filters applied.

8. (Optional) Click on the column titles to sort the list of synchronized suspicious objects.

---

**Viewing Synchronized Suspicious Objects - Correlation Data**

Deep Discovery Director - Network Analytics is a transparent solution that provides advanced threat analysis using correlation data. If a suspicious object has correlation data, you can access it through Deep Discovery Director.

---

**Procedure**

1. Go to **Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects**.

2. To view correlation data for any event, click the **Correlation Data** icon in the **Object** field.
Note

- Deep Discovery Inspector must be integrated with Network Analytics servers to display correlation data.
- The Correlation Data icon is present only if there is correlation data for that event.

The Deep Discovery Director - Network Analytics Correlation Data screen appears.

3. Use the following sections for advanced analysis of malicious activity:

- **Summary**
  
  Provides a high-level overview of the malicious activity, risk level, and risk analysis for this correlation data.

- **Correlation Graph**
  
  Provides a visual representation of correlations made between the detection object selected in Deep Discovery Director and other related events as they occur over time.

- **Transaction Details**
  
  Provides details about each transaction represented in the correlation graph. Transactions are listed from oldest correlated events at the top to the most recent correlated event at the bottom.

Tip

Information displayed in the Deep Discovery Director - Network Analytics Correlation Data screen is created dynamically. The number of correlations and details about interactions and malicious activity between hosts presented in the Deep Discovery Director - Network Analytics Correlation Data screen can change over time. You can access the correlation data for a specific detection at a later time to see if additional analysis details are available.
4. For details on how to use the information displayed in the Deep Discovery Director - Network Analytics screen to assist in advanced analysis, see Analyzing Correlation Data Information on page 4-91.

Exporting Synchronized Suspicious Objects

The Synchronized Suspicious Objects list can be exported in CSV format for offline viewing.

Procedure

1. Go to Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects.

   The Synchronized Suspicious Objects screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see Viewing Synchronized Suspicious Objects on page 5-2.

3. Click Export to export the currently filtered list of synchronized suspicious objects.

   The Export dialog appears.

4. Confirm the filters and select a delimiter to use.

   • Comma
   • Semicolon
   • Space
   • Tab

5. Click Export to export and download the currently filtered list of synchronized suspicious objects to a CSV file with the chosen delimiter.
Moving Synchronized Suspicious Objects to Exceptions

Objects that you consider harmless can be moved to the **Exceptions** list. Exceptions are considered safe and will not be added to the **Synchronized Suspicious Objects** list if detected by Virtual Analyzer in the future.

**Note**

Objects may appear in both the **Exceptions** and **Synchronized Suspicious Objects** lists while newly registered Deep Discovery appliances are still syncing threat intelligence.

**Procedure**

1. Go to **Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects**.
   
The **Synchronized Suspicious Objects** screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing Synchronized Suspicious Objects* on page 5-2.

3. Select one or more objects that you consider harmless and then click **Move to Exceptions**.
   
The **Move To Exceptions** dialog appears.

4. Click **Move** to move the selected objects to the **Exceptions** list.

**Expanding Synchronized Suspicious Objects**

Expire objects to remove them from the **Synchronized Suspicious Objects** list. If the same object is detected by Virtual Analyzer in the future, it will be added to the **Synchronized Suspicious Objects** list again.

**Procedure**

1. Go to **Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects**.
The Synchronized Suspicious Objects screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see Viewing Synchronized Suspicious Objects on page 5-2.

3. Select one or more objects that you want to remove from the Synchronized Suspicious Objects list and then click Expire Now.

   The Expire Now dialog appears.

4. Click Expire to remove the selected objects from the Synchronized Suspicious Objects list.

---

**Setting Synchronized Suspicious Objects to Never Expire**

Objects that you consider harmful can be set to never expire and will never be removed from the Synchronized Suspicious Objects list.

---

**Procedure**

1. Go to Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects.

   The Synchronized Suspicious Objects screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see Viewing Synchronized Suspicious Objects on page 5-2.

3. Select one or more objects that you consider harmful and then click Never Expire.

   The Never Expire dialog appears.

4. Click Never Expire to set the selected objects to never expire and never remove from the Synchronized Suspicious Objects list.
Configuring Expiration Settings

By default, synchronized suspicious objects expire in 30 days. Newly synced suspicious objects can be configured to expire earlier.

Procedure

1. Go to Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects.

   The Synchronized Suspicious Objects screen appears.

2. Click the gear icon above the time period and data source filters.

   The Expiration Settings dialog appears.

3. Select Set newly synced suspicious objects to expire in:, and then select a days value from the drop-down list.

4. Click Save.

C&C Callback Addresses

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

C&C callback address detections can be sorted by Callback Address, C&C Risk Level, Type, Sync Source, Latest Callback, and Callbacks.

Viewing C&C Callback Addresses

Procedure

1. Go to Threat Intelligence > Product Intelligence > C&C Callback Addresses.

   The C&C Callback Addresses screen appears.
2. Click the drop-down for detection type and then select one of the following detection types:
   - All (default)
   - IP addresses
   - URLs
   - Domains

3. To configure display settings, hover over the **Callbacks** column title and select **Display Settings**.
   
The **Display Settings** dialog appears.

4. Select a time period.

5. Select which appliances to include as data source.

   **Note**
   
The time period and data source filters only affect the **Callbacks** numbers.

6. To run a partial match search, type a case-insensitive keyword in the search text box, and then press ENTER or click the magnifying glass icon.

7. (Optional) Click a number in the **Callbacks** column to drill-down to the **Network Detections** screen with filters applied.

8. (Optional) Click on the column titles to sort the list of C&C callback addresses.

---

**Exporting C&C Callback Addresses**

The **C&C Callback Addresses** list can be exported in CSV format for offline viewing.

**Procedure**

1. Go to **Threat Intelligence > Product Intelligence > C&C Callback Addresses**.
The **C&C Callback Addresses** screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-8.*

3. Click **Export** to export the currently filtered list of C&C callback addresses.

   The **Export** appears.

4. Confirm the filters and select a delimiter to use.

   - Comma
   - Semicolon
   - Space
   - Tab

5. Click **Export** to export and download the currently filtered list of C&C callback addresses to a CSV file with the chosen delimiter.

### Copying C&C Callback Addresses to User-Defined Suspicious Objects

C&C callback addresses that you consider harmful can be copied to the **User-Defined Suspicious Objects** list.

**Procedure**

1. Go to **Threat Intelligence > Product Intelligence > C&C Callback Addresses**.

   The **C&C Callback Addresses** screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-8.*

3. Select one or more C&C callback addresses that you consider harmful and then click **Copy to User-Defined SO**.

   The **Copy to User-Defined Suspicious Objects** dialog appears.
4. Click **Copy** to copy the selected C&C callback addresses to the **User-Defined Suspicious Objects** list.

### Copying C&C Callback Addresses to Exceptions

C&C callback addresses that you consider harmless can be copied to the **Exceptions** list.

#### Procedure

1. Go to **Threat Intelligence > Product Intelligence > C&C Callback Addresses**.

   The **C&C Callback Addresses** screen appears.

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-8*.

3. Select one or more C&C callback addresses that you consider harmless and then click **Copy to Exceptions**.

   The **Copy to Exceptions** dialog appears.

4. Click **Copy** to copy the selected C&C callback addresses to the **Exceptions** list.

### Custom Intelligence

Deep Discovery products provide different ways to protect against suspicious objects not yet identified within your network:

- **YARA Rules on page 5-12**
- **STIX on page 5-17**
- **User-Defined Suspicious Objects on page 5-19**
Deep Discovery Director (Consolidated Mode) allow you to exclude objects from the Synchronized Suspicious Objects list based on the file SHA-1 hash value, IP address, domain or URL:

- Exceptions on page 5-25

YARA Rules

Deep Discovery products use YARA rules to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

Deep Discovery Director (Consolidated Mode) supports a maximum of 5,000 YARA rules regardless of the number of YARA rule files.

The following table shows information about YARA rule files.

**TABLE 5-1. YARA Rules**

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Name of the YARA rule file.</td>
</tr>
<tr>
<td>Rules</td>
<td>Number of YARA rules contained in the YARA rule file.</td>
</tr>
<tr>
<td>Files To Analyze</td>
<td>File types to analyze using the YARA rules in the YARA rule file.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>Risk level of the YARA rules.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Only Deep Discovery Email Inspector utilizes these risk levels.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Date and time the YARA rule file was last updated.</td>
</tr>
<tr>
<td>Updated By</td>
<td>The account that last updated the YARA rule file.</td>
</tr>
</tbody>
</table>
Creating a YARA Rule File

Deep Discovery Director (Consolidated Mode) supports YARA rules that follow version 3.7.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

For more information about writing YARA rules, visit the following site:


A YARA rule file must fulfill certain requirements before it can be added to Virtual Analyzer for malware detection:

• File name must be unique
• File content cannot be empty

The following example shows a simple YARA rule:

```yaml
rule NumberOne
{
  meta:
  desc = "Sonala"
  weight = 10
  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
    $c = "UVODFRYSHLNWPEJXQZAKCBGMT"
  condition:
    $a or $b or $c
}
```

The following table lists the different parts of the YARA rule and how they are used:

**TABLE 5-2. YARA Rule Parts and Usage**

<table>
<thead>
<tr>
<th>PART</th>
<th>USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule</td>
<td>The YARA rule name. Must be unique and cannot contain spaces.</td>
</tr>
<tr>
<td>meta:</td>
<td>Indicates that the &quot;meta&quot; section begins. Parts in the meta section do not affect detection.</td>
</tr>
<tr>
<td>Part</td>
<td>Usage</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>desc</td>
<td>Optional part that can be used to describe the rule.</td>
</tr>
</tbody>
</table>
| weight | Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met:  
  - 1 to 9 = Low risk  
  - 10 = High risk |

**Note**  
- The weight value does not correspond to the risk level assigned by Deep Discovery products.  
- The weight value is ignored by Deep Discovery Email Inspector.

<table>
<thead>
<tr>
<th>strings:</th>
<th>Indicates that the &quot;strings&quot; section begins. Strings are the main means of detecting malware.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a / $b / $c</td>
<td>Strings used to detect malware. Must begin with a $ character followed by one of more alphanumeric characters and underscores.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>condition:</th>
<th>Indicates that the &quot;condition&quot; section begins. Conditions determine how your strings are used to detect malware.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a or $b or $c</td>
<td>Conditions are Boolean expressions that define the logic of the rule. They tell the condition under which a submitted object satisfies the rule or not. Conditions can range from the typical Boolean operators <code>and</code>, <code>or</code>, and <code>not</code>, to relational operators <code>&gt;=</code>, <code>&lt;=</code>, <code>&lt;</code>, <code>&gt;</code>, <code>==</code> and <code>!=</code>. Arithmetic operators <code>+</code>, <code>–</code>, <code>*</code>, <code>/</code>, <code>%</code> and bitwise operators <code>&amp;</code>, `</td>
</tr>
</tbody>
</table>

## Adding a YARA Rule File

YARA rules on managed appliances will be overwritten after syncing with Deep Discovery Director (Consolidated Mode). To ensure that no YARA rules are lost, export them from the managed appliances and add them to Deep Discovery Director (Consolidated Mode).
Procedure

1. Go to Threat Intelligence > Custom Intelligence > YARA Rules.

   The YARA Rules screen appears.

2. Click Add.

   The Add YARA Rule File dialog appears.

3. Click Select to locate a YARA rule file to add.

4. To specify the file types that Virtual Analyzer processes specific to this YARA rule file, select or type to search a file type and press ENTER. Select All file types to let Virtual Analyzer process all file types with this YARA rule file.

   - Trend Micro recommends only specifying the file types targeted by the YARA rules. The All file types option includes additional file types that are not supported by Virtual Analyzer. Only Deep Discovery Email Inspector utilizes those additional file types.

   - File types that are not supported by Virtual Analyzer can be added as custom file types. Only Deep Discovery Email Inspector utilizes custom file types.

5. Select the risk level for the YARA rules in the file.

   - Only Deep Discovery Email Inspector utilizes these risk levels.

6. (Optional) Type a description for this YARA rule file.

7. Click Add.

   The YARA rule file appears in the YARA Rules list. Registered appliances receive the updated YARA Rules list during the next synchronization.
Editing a YARA Rule File

Procedure

1. Go to Threat Intelligence > Custom Intelligence > YARA Rules.
   
   The YARA Rules screen appears.

2. Click the file name of the YARA rule file you want to edit.
   
   The Edit YARA Rule File dialog appears.

3. Modify the settings.

4. Click Save.

Exporting YARA Rule Files

The YARA rule files can be exported for use in other YARA compatible products.

Procedure

1. Go to Threat Intelligence > Custom Intelligence > YARA Rules.
   
   The YARA Rules screen appears.

2. Do one of the following to export the YARA rule files:
   
   • To export all YARA rule files, click Export without selecting any YARA rule files.
   
   • To export specific YARA rule files, select the YARA rule files to export and click Export Selected.

   Deep Discovery Director (Consolidated Mode) creates a ZIP archive with the YARA rule files.

   Note

   Regardless of the original encoding used when the YARA rule files were imported, exported YARA rule files will always use UTF-8 encoding.
3. Download and save the ZIP archive.

Deleting YARA Rule Files

Delete unused YARA rule files to reduce the number of rules in use, or to free up database disk space.

Procedure

1. Go to Threat Intelligence > Custom Intelligence > YARA Rules.

   The YARA Rules screen appears.

2. Select one or more YARA rule files to delete and then click Delete.

   The YARA rule files are deleted from the YARA Rules list. Registered appliances receive the updated YARA Rules list during the next synchronization.

STIX

Deep Discovery Director (Consolidated Mode) enables you to import objects to the User-Defined Suspicious Objects list using the Structured Threat Information eXpression (STIX) format.

The following table shows information about STIX files.

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Name of the STIX file.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the STIX file.</td>
</tr>
<tr>
<td>Imported</td>
<td>Date and time the STIX file was imported.</td>
</tr>
<tr>
<td>Imported By</td>
<td>The account that imported the STIX file.</td>
</tr>
</tbody>
</table>
Importing Objects From STIX

Procedure

1. Go to Threat Intelligence > Custom Intelligence > STIX.
   The STIX screen appears.

2. Click Import.
   The Import Objects From STIX dialog appears.

3. Click Select to locate a STIX file to import.

4. (Optional) Type a description for this STIX file.

5. Click Import.

Note

- Only IP addresses, domains, URLs, and file SHA-1 hash values will be added to the User-Defined Suspicious Objects list.
- The STIX file and object information can be shared as part of threat intelligence.

The objects appear in the User-Defined Suspicious Objects list. Registered appliances receive the updated User-Defined Suspicious Objects list during the next synchronization.

Exporting STIX Files

The STIX files can be exported for use in other STIX compatible products.

Procedure

1. Go to Threat Intelligence > Custom Intelligence > STIX.
   The STIX screen appears.
2. Do one of the following to export the STIX files:

- To export all STIX files, click **Export** without selecting any STIX files.
- To export specific STIX files, select the STIX files to export and click **Export Selected**.

Deep Discovery Director (Consolidated Mode) creates a ZIP archive with the STIX files.

---

**Deleting STIX Files**

---

**Procedure**

1. Go to **Threat Intelligence > Custom Intelligence > STIX**.

   The **STIX** screen appears.

2. Select one or more STIX files to delete and then click **Delete**.

   The STIX files are deleted from the **STIX** list.

---

**Note**

Deleting the STIX files does not affect already imported objects.

---

**User-Defined Suspicious Objects**

The **User-Defined Suspicious Objects** list allows you to define suspicious file SHA-1 hash value, IP address, URL, and domain objects that Deep Discovery products with Virtual Analyzer have not yet detected on your network. Supported Deep Discovery products can take action on the objects found in the list to prevent the spread of unknown threats.
Viewing User-Defined Suspicious Objects

Procedure

1. Go to Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects.

   The User-Defined Suspicious Objects screen appears.

2. Click the drop-down for detection type and then select one of the following detection types:
   - All (default)
   - IP addresses
   - URLs
   - File SHA-1
   - Domains

3. To configure display settings, hover over the Network Detections or Email Messages icon in the column title and select Display Settings.

   The Display Settings dialog appears.

4. Select a time period.

5. Select which appliances to include as data source, and domains from which email messages should be displayed.

   **Note**
   The time period, data source, and monitored domain filters only affect the Detections numbers.

6. To run a search, type an IP address, domain, URL, SHA-1 hash value, or description keyword in the search text box, and then press ENTER or click the magnifying glass icon.
7. (Optional) Click a number in the Network Detections or Email Messages column to drill-down to the Network Detections or Email Messages screen with filters applied.

8. (Optional) Click on the column titles to sort the list of user-defined suspicious objects.

Viewing User-Defined Suspicious Objects - Correlation Data

Deep Discovery Director - Network Analytics is a transparent solution that provides advanced threat analysis using correlation data. If a suspicious object has correlation data, you can access it through Deep Discovery Director.

Procedure

1. Go to Threat Intelligence > Product Intelligence > User-Defined Suspicious Objects.

2. To view correlation data for any event, click the Correlation Data icon in the Object field.

   Note
   • Deep Discovery Inspector must be integrated with Network Analytics servers to display correlation data.
   • The Correlation Data icon is present only if there is correlation data for that event.

The Deep Discovery Director - Network Analytics Correlation Data screen appears.

3. Use the following sections for advanced analysis of malicious activity:

   • Summary

   Provides a high-level overview of the malicious activity, risk level, and risk analysis for this correlation data.
• **Correlation Graph**
  Provides a visual representation of correlations made between the detection object selected in Deep Discovery Director and other related events as they occur over time.

• **Transaction Details**
  Provides details about each transaction represented in the correlation graph. Transactions are listed from oldest correlated events at the top to the most recent correlated event at the bottom.

---

**Tip**
Information displayed in the Deep Discovery Director - Network Analytics Correlation Data screen is created dynamically. The number of correlations and details about interactions and malicious activity between hosts presented in the Deep Discovery Director - Network Analytics Correlation Data screen can change over time. You can access the correlation data for a specific detection at a later time to see if additional analysis details are available.

---

4. For details on how to use the information displayed in the Deep Discovery Director - Network Analytics screen to assist in advanced analysis, see Analyzing Correlation Data Information on page 4-91.

---

**Adding a User-Defined Suspicious Objects**

**Procedure**

1. Go to Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects.

   The User-Defined Suspicious Objects screen appears.

2. Click Add.

   The Add Object dialog appears.

3. Select the object type:
• **IP address**: type an IP address or a hyphenated range.

  ![Note]
  IPv4 and IPv6 addresses and subnet mask bits are supported.

• **URL**: type a URL.

  ![Note]
  HTTP and HTTPS URLs are supported.

• **File SHA-1**: type the SHA-1 hash value of a file.

• **Domain**: type a domain name.

  ![Note]
  One wildcard (*) connected with a "." in the domain prefix is supported.

4. (Optional) Type a description for this object.

5. Click **Add**.

The object appears in the **User-Defined Suspicious Objects** list. Registered appliances receive the updated **User-Defined Suspicious Objects** list during the next synchronization.

---

**Tip**

Objects can also be added from product intelligence. For details, see *Copying C&C Callback Addresses to User-Defined Suspicious Objects on page 5-10*.

---

**Editing a User-Defined Suspicious Objects**

**Procedure**

1. Go to **Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects**.
The **User-Defined Suspicious Objects** screen appears.

2. Click the object you want to edit.

   The **Edit Object** dialog appears.

3. Modify the settings.

   __Note__
   
   The object type cannot be modified.

4. Click **Save**.

---

**Importing User-Defined Suspicious Objects**

Deep Discovery Director (Consolidated Mode) supports importing objects from a properly formatted CSV file.

---

**Procedure**

1. Go to **Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects**.

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Import**.

   The **Import Objects From CSV** dialog appears.

3. Click **Select** to locate a CSV file to import.

   __Tip__
   
   If you are importing a CSV for the first time, click **Download sample CSV** and save the file. Populate the CSV file properly formatted objects (see the instructions in the CSV file), save the file, and then click **Select** to locate the CSV file.

4. Click **Import**.
The objects appear in the **User-Defined Suspicious Objects** list. Registered appliances receive the new object information during the next synchronization.

---

**Deleting User-Defined Suspicious Objects**

Delete unused user-defined suspicious objects to reduce the number of objects. When the maximum number of objects has been reached, adding or importing objects overwrites the oldest objects.

**Procedure**

1. Go to **Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects**.

   The **User-Defined Suspicious Objects** screen appears.

2. Select one or more objects to delete and then click **Delete**.

   The object is deleted from the **User-Defined Suspicious Objects** list. Registered appliances receive the updated **User-Defined Suspicious Objects** list during the next synchronization.

---

**Exceptions**

Objects that you consider harmless can be added to the **Exceptions** list. Exceptions are considered safe and will not be added to the **Synchronized Suspicious Objects** list if detected by Virtual Analyzer in the future.

---

**Note**

Objects may appear in both the **Exceptions** and **Synchronized Suspicious Objects** lists while newly registered Deep Discovery appliances are still syncing threat intelligence.
Viewing Exceptions

Procedure

1. Go to Threat Intelligence > Custom Intelligence > Exceptions.
   The Exceptions screen appears.

2. Click the drop-down for detection type and then select one of the following detection types:
   - All (default)
   - IP addresses
   - URLs
   - File SHA-1
   - Domains

3. To run a search, type an IP address, domain, URL, SHA-1 hash value, or description keyword in the search text box, and then press ENTER or click the magnifying glass icon.

4. (Optional) Click on the column titles to sort the list of exceptions.

Adding an Exception

Procedure

1. Go to Threat Intelligence > Custom Intelligence > Exceptions.
   The Exceptions screen appears.

2. Click Add.
   The Add Exception dialog appears.

3. Select the object type:
• **IP address:** type an IP address or a hyphenated range.

  ![Note]
  IPv4 and IPv6 addresses and subnet mask bits are supported.

• **URL:** type a URL.

  ![Note]
  HTTP and HTTPS URLs are supported.

• **File SHA-1:** type the SHA-1 hash value of a file.

• **Domain:** type a domain name.

  ![Note]
  One wildcard (*) connected with a "." in the domain prefix is supported.

4. (Optional) Type a description for this object.

5. Click **Add**.

The object appears in the **Exceptions** list. Registered appliances receive the updated **Exceptions** list during the next synchronization.

![Tip]
Exceptions can also be added from product intelligence. For details, see the following topics:

• *Moving Synchronized Suspicious Objects to Exceptions on page 5-6*

• *Copying C&C Callback Addresses to Exceptions on page 5-11*
Importing Exceptions

Procedure

1. Go to Threat Intelligence > Custom Intelligence > Exceptions.
   The Exceptions screen appears.

2. Click Import.
   The Import Objects From CSV dialog appears.

3. Click Select to locate a CSV file to import.

   **Tip**
   If you are importing a CSV for the first time, click Download sample CSV and save the file. Populate the CSV file properly formatted objects (see the instructions in the CSV file), save the file, and then click Select to locate the CSV file.

4. Click Import.
   The objects appear in the Exceptions list. Registered appliances receive the new object information during the next synchronization.

Deleting Exceptions

Delete unused exceptions to reduce the number of objects. When the maximum number of objects has been reached, adding or importing objects overwrites the oldest objects.

Procedure

1. Go to Threat Intelligence > Custom Intelligence > Exceptions.
   The Exceptions screen appears.

2. Select one or more objects to delete and then click Delete.
The object is deleted from the **Exceptions** list. Registered appliances receive the updated **Exceptions** list during the next synchronization.

---

**Feed Management**

Deep Discovery Director (Consolidated Mode) allows you to subscribe to and monitor intelligence feeds for threat information that can be used to complement your product and custom intelligence.

The following table shows information about intelligence feeds.

**Table 5-4. Intelligence Feeds**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed Name</td>
<td>Name of the intelligence feed.</td>
</tr>
<tr>
<td>Collection</td>
<td>Collection that is selected from the intelligence feed.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Frequency at which the intelligence feed is polled for information.</td>
</tr>
<tr>
<td>Last Polled</td>
<td>Date and time the intelligence feed was last polled for information.</td>
</tr>
<tr>
<td>Status</td>
<td>Click the toggle to enable or disable polling the intelligence feed for information.</td>
</tr>
</tbody>
</table>

**Adding an Intelligence Feed**

**Procedure**

1. Go to **Threat Intelligence > Feed Management**.
   
   The **Feed Management** screen appears.

2. Click **Add**.
   
   The **Add Intelligence Feed** screen appears.

3. Enable the intelligence feed.
4. Type a name for this intelligence feed.

5. Type the discovery URL for this intelligence feed.

6. (Optional) Select **Use server certificate** if the server uses it, and then click **Select** to locate the server certificate file.

   **Note**
   
   The key of the certificate must be at least 1024 bit.

7. (Optional) Select **Specify authentication credentials** if the server requires it, and then type the user name and password used for authentication.

8. (Optional) Select **Server requires client authentication** if the server requires it, and then click **Select** to locate the client certificate file.

   **Note**
   
   The key of the certificate must be at least 1024 bit.

9. (Optional) Type the client certificate passphrase.

10. Click **Discover** to find and then select an available collection.

11. Select the frequency at which the intelligence feed is polled for information.

12. Select how far in the past you want to begin polling information from.

13. Click **Add**.

   The intelligence feed appears in the **Feed Management** list. Polled information that contains IP addresses, domains, URLs and SHA-1 hash values will be added to the **User-Defined Suspicious Objects** list. Registered appliances receive the updated **User-Defined Suspicious Objects** list during the next synchronization.
Editing an Intelligence Feed

Procedure

1. Go to Threat Intelligence > Feed Management.

   The Feed Management screen appears.

2. Click the feed name of the intelligence feed you want to edit.

   The Edit Intelligence Feed screen appears.

3. Modify the settings.

4. Click Save.

Deleting Intelligence Feeds

Procedure

1. Go to Threat Intelligence > Feed Management.

   The Feed Management screen appears.

2. Select one or more intelligence feeds to delete and then click Delete.

   The intelligence feeds are deleted from the Feed Management list. STIX files that were obtained from the intelligence feeds and that were added to the STIX list will be deleted. Deleting the STIX files does not affect already imported objects.

Sharing Settings

Deep Discovery Director (Consolidated Mode) provides various methods to share threat intelligence data with other products or services:

- TAXII on page 5-32
TAXII

Deep Discovery Director (Consolidated Mode) can share threat intelligence data with other products or services through TAXII.

Configuring TAXII Settings

Procedure

1. Go to Threat Intelligence > Sharing Settings > TAXII.
   The TAXII screen appears.

2. Select Enable TAXII server to allow exchange of threat intelligence with integrated products/services.

3. Type the user name and password used for authentication.

4. Select the risk level of the objects to be included in the threat intelligence data file.

5. Click Save.

6. (Optional) Click Generate Now.

7. Deep Discovery Director (Consolidated Mode) automatically generates threat information every 10 minutes. Configure an integrated product/service to subscribe to and monitor the Deep Discovery Director (Consolidated Mode) discovery URL for threat information. For more information, see the documentation for the integrated product/service.
Web Service

Deep Discovery Director (Consolidated Mode) can share threat intelligence data with other products or services (for example, a Blue Coat ProxySG device) through HTTP or HTTPS web service.

Configuring Web Service Settings

Procedure

1. Go to Threat Intelligence > Sharing Settings > Web Service.

   The Web Service screen appears.

2. Select Enable web service to allow integrated products/services to obtain information from Deep Discovery Director.

3. (Optional) By default, Deep Discovery Director (Consolidated Mode) shares threat intelligence data through HTTPS web service. You can also enable HTTP web service for data sharing. Under Server Settings, select Share information using HTTP (in addition to HTTPS) and specify the HTTP server port number.

4. Under Criteria, select which objects to include in the threat intelligence data file.

5. Under Criteria, select the risk level of the objects to be included in the threat intelligence data file.

The objects appear in the generated file under the following categories.

**TABLE 5-5. Object Categories in Generated File**

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>CATEGORY IN GENERATED FILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronized Suspicious Objects</td>
<td>DDD_so_blacklists</td>
</tr>
<tr>
<td>User-Defined Suspicious Objects</td>
<td>DDD_so_blacklists</td>
</tr>
<tr>
<td>C&amp;C Callback Addresses</td>
<td>DDD_cnc_blacklists</td>
</tr>
</tbody>
</table>
6. Click **Save**.

7. (Optional) Click **Generate Now**.

---

**Note**

After the file generation is successful, you can click the URL to download the threat intelligence data file to view the content.

8. Configure an integrated product/service (for example, Blue Coat ProxySG device) to obtain threat intelligence data from Deep Discovery Director (Consolidated Mode). For more information, see the documentation for the integrated product/service.

---

**Auxiliary Products/Services**

To help provide effective detection and blocking at the perimeter, Deep Discovery Director (Consolidated Mode) can distribute threat intelligence data to auxiliary products and services.

Deep Discovery Director (Consolidated Mode) integrates with the following solutions:

**TABLE 5-6. Supported Solutions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro TippingPoint Security Management System (SMS)</td>
<td>SMS 4.6.0 or later</td>
</tr>
<tr>
<td>Check Point Open Platform for Security (OPSEC)</td>
<td>Check Point R80.10 or later</td>
</tr>
<tr>
<td>IBM Security Network Protection (XGS)</td>
<td>XGS 5.2 or later</td>
</tr>
</tbody>
</table>
## Threat Intelligence

<table>
<thead>
<tr>
<th>NAME</th>
<th>VERSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto Panorama</td>
<td>PAN-OS 7.0.1 or later</td>
</tr>
<tr>
<td>Palo Alto Firewalls</td>
<td>PAN-OS 4.1.0 or later</td>
</tr>
</tbody>
</table>

### Trend Micro TippingPoint Security Management System (SMS)

Deep Discovery Director (Consolidated Mode) can send synchronized suspicious objects, user-defined suspicious objects and C&C callback addresses to Trend Micro TippingPoint Security Management System (SMS).

**Note**

The following actions will remove suspicious objects from Trend Micro TippingPoint Security Management System (SMS):

- Moving synchronized suspicious objects to Exceptions
- Expiring synchronized suspicious objects
- Deleting user-defined suspicious objects

Deep Discovery Director (Consolidated Mode) sends each C&C callback address and suspicious object with the following optional information:

- Trend Micro Severity: Severity of each suspicious object or C&C callback attempt
- Trend Micro Publisher: Trend Micro Deep Discovery Director (Consolidated Mode)
- Trend Micro Source: Deep Discovery Director (Consolidated Mode) host name
- Trend Micro Detection Category: Suspicious object or C&C callback attempt
Configuring Trend Micro TippingPoint Security Management System (SMS)

Procedure

1. On the Deep Discovery Director (Consolidated Mode) management console, go to Threat Intelligence > Sharing Settings > Auxiliary Products/Services.

   The Auxiliary Products/Services screen appears.

2. Select Distribute objects to auxiliary products/services.


4. Type the server address.

   Note
   The server address must be the IPv4 address or FQDN of the auxiliary product/service.

5. Type the user name and password used for authentication.

6. (Optional) Click Test Connection.

7. To send object information from Deep Discovery Director (Consolidated Mode) to this auxiliary product/service, configure the following criteria:

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

   Note
   Only supported by SMS 5.0 or higher.
• Suspicious Object
• IPv4 address
• Domain
• URL

Note
Only supported by SMS 5.0 or higher.

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

8. Click Save.

The following tag categories are displayed in the TippingPoint SMS Reputation Database.

<table>
<thead>
<tr>
<th>TAG CATEGORY</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro Source</td>
<td>The host name of Deep Discovery Director (Consolidated Mode)</td>
</tr>
<tr>
<td>Trend Micro Severity</td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td>• Low</td>
</tr>
<tr>
<td>Trend Micro Publisher</td>
<td>The product name of Deep Discovery Director (Consolidated Mode)</td>
</tr>
<tr>
<td>Trend Micro Detection Category</td>
<td>The detection type of the threat.</td>
</tr>
</tbody>
</table>

9. (Optional) To view distributed C&C callback addresses and suspicious objects in TippingPoint SMS, do the following:
a. Verify that the following tag categories exist in the Tag Categories list of the TippingPoint SMS Client.
   • Trend Micro Severity
   • Trend Micro Source
   • Trend Micro Publisher
   • Trend Micro Detection Category
b. On the Profile tab, go to Reputation Database > Search.

![Image of TippingPoint SMS Client interface]

c. On the Entry Criteria screen, type search parameters and then click Search.

Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Consolidated Mode) are displayed.
Check Point Open Platform for Security (OPSEC)

Check Point Open Platform for Security (OPSEC) manages network security through an open, extensible management framework.

Deep Discovery Director (Consolidated Mode) integrates with Check Point OPSEC via the Suspicious Activities Monitoring (SAM) API.

The SAM API implements communications between the SAM client (Deep Discovery Director (Consolidated Mode)) and the Check Point firewall, which acts as a SAM Server. Deep Discovery Director (Consolidated Mode) uses the SAM API to request that the Check Point firewall take specified actions for certain connections.

For example, Deep Discovery Director (Consolidated Mode) may ask Check Point OPSEC to block a connection with a client that is attempting to issue illegal commands or repeatedly failing to log on.

Configuring Check Point Open Platform for Security (OPSEC)

Procedure

1. On the Deep Discovery Director (Consolidated Mode) management console, go to Threat Intelligence > Sharing Settings > Auxiliary Products/Services.

   The Auxiliary Products/Services screen appears.

2. Select Distribute objects to auxiliary products/services.


4. Click Legal Statement.

   The Legal Statement dialog appears.

5. Read and accept the Legal Statement.

   ! Important
   To enable integration with this auxiliary product/service, you must accept the Legal Statement.
6. Select a connection type.

**Note**
Ensure that your network configuration allows Deep Discovery Director (Consolidated Mode) to connect to the Check Point appliance.

Deep Discovery Director (Consolidated Mode) may connect to the Check Point appliance through the secured connection port or clear connection port that is configured on the Check Point appliance. Deep Discovery Director (Consolidated Mode) also pulls the certificate from the Check Point appliance through port 18210.

7. Type the server address.

**Note**
The server address must be the IPv4 address the auxiliary product/service.

8. Type the port.

**Note**
This port must be the same port that is configured on the security gateway. For details, see *Preconfiguring a Security Gateway on page 5-45*.

9. If you selected **Secured connection**, type the **OPSEC application name** and **SIC one-time password**.

For more details, see *Configuring a Secured Connection on page 5-47*.

**Note**
If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

10. (Optional) Click **Test Connection**.

11. On your Check Point firewall appliance, preconfigure a security gateway. For details see *Preconfiguring a Security Gateway on page 5-45*. 
12. On the Check Point SmartConsole, do the following to configure your Check Point appliance for deploying suspicious objects and C&C callback addresses from Deep Discovery Director (Consolidated Mode):

a. On the left pane, click **Security Policies**.

b. On the **Standard** tab, under **Access Control**, click **Policy**.

c. To add a rule, click the **Add rule above** icon.

d. Right-click the source and select **Add new items**.

e. Click the **New** icon, and select **Address Ranges > Address Range**.
The **New Address Range** window appears.

![New Address Range Window](image)

f. Type **DDD** as name.

g. In **First IP address**, type the Deep Discovery Director (Consolidated Mode) IP address.

h. In **Last IP address**, type the Deep Discovery Director (Consolidated Mode) IP address.

i. Click **OK**.

An item named **DDD** should be created and automatically selected as the source.
j. Right-click the destination and select your CheckPoint appliance.

k. Right-click the action and select **Accept**.

l. Click **Install Policy**.

   The Check Point SmartConsole will prompt you to publish your changes before installing the policy.

m. Click **Publish & Install**.

   The **Install Policy** dialog appears.

n. Click **Install**.

   The Check Point appliance is enabled to receive suspicious objects and C&C callback addresses from Deep Discovery Director (Consolidated Mode).

13. On the Deep Discovery Director (Consolidated Mode) management console, configure the following criteria to send suspicious object and C&C callback address information from Deep Discovery Director (Consolidated Mode) to this inline product/service:

   • **Object type:**
     - C&C Callback Address
       - IPv4 address
     - Suspicious Object
       - IPv4 address

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

14. Under **Advanced Settings**, click one of the following actions:

   • **Reject**: Packets will be rejected and a notification sent to the communicating peer that the packet has been rejected.
• **Drop**: Packets will be dropped without sending the communicating peer a notification.

• **Notify**: A notification about the defined activity will be sent but the activity will not be blocked.

15. Click **Save**.

   The **Distribute Now** option appears.

16. (Optional) Click **Distribute Now** to distribute suspicious objects and C&C callback addresses to Check Point immediately.

17. To view suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Consolidated Mode) on the Check Point SmartConsole, do the following:
   
   a. On the left pane, click **Logs & Monitor**.

   b. Create a new tab by clicking the ![icon](image)

   c. On the new tab, click **Tunnel & User Monitoring**.

   The **SmartView Monitor** screen appears.

   d. On the **SmartView Monitor** screen, click **Launch Menu** icon, and then select **Tools > Suspicious Activity Rules**.

   The **Enforced Suspicious Activity Rules** dialog appears.

   e. At **Show On**, select your Check Point appliance.

   f. Click **Refresh**.

   Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Consolidated Mode) are displayed.
Preconfiguring a Security Gateway

Procedure

1. Log on to your Check Point appliance.

2. (Optional) Set a password for expert mode.

3. Type the password to enter expert mode.

4. Use the vi editor to open /var/opt/CPsuite-R80/fw1/conf/fwopsec.conf.
5. In `fwopsec.conf`, configure the SAM communication mode ports using one of the following options:

- **Secured connection (default port)**
  - No changes in `fwopsec.conf` are necessary. The default port 18183 is used for the `sam_server auth_port` setting.

- **Secured connection (user-defined port)**
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server auth_port: 18183` and then change the port number.

- **Clear connection (user-defined port)**
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server port: 0` and then change the port number.
Note

Configure the same port in fwopsec.conf and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Director (Consolidated Mode) at.

6. If changes were made to the fwopsec.conf file, save the fwopsec.conf file and restart your Check Point appliance.

Configuring a Secured Connection

Procedure

1. Open the Check Point SmartConsole and click the main menu icon.

2. Go to **New object > More object types > Server > OPSEC Application > New Application**...
The **OPSEC Application Properties** window appears.

![Image of OPSEC Application Properties window]

- **Name:**
- **Comment:**
- **Color:** Black
- **Host:**
- **Vendor:** User defined
- **Product:**
- **Version:**
- **Server Entities:**
  - CVP
  - UFP
  - AMON
- **Client Entities:**
  - ELA
  - LEA
  - SAM
  - CPMI
  - OMI
  - UAA
- **Secure Internal Communication**
  - **Communication:**
  - **DN:**
3. **Type a Name.**

**Note**
- Use this name as the **OPSEC application name** in Deep Discovery Director (Consolidated Mode).
- The application name must be less than 101 characters, start with an English alphabetical letter, and contain only English alphabetical letters, periods, underscores, or dashes.

4. **Select a Host.**

5. Under **Client Entities**, select **SAM**.

6. Click **Communication**....

The **Communication** window appears.

- **One-time password:**
- **Confirm one-time password:**
- **Trust state:** **Uninitialized**

[Communication window with fields and buttons]
7. Type a password in **One-time password** and type the same password in **Confirm one-time password**.

**Note**

Use this password as the **SIC one-time password** in Deep Discovery Director (Consolidated Mode).

**Note**

If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

8. Click **Initialize**.

The **Trust state** becomes **Initialized but trust not established**.

9. Install the policy.

   a. In the **Check Point SmartConsole** main window, click ![Install policy...] and select **Install policy**.

      The **Install Policy** window appears.

   b. Choose the installation components and then click **OK**.

      The policy starts installing.

---

**IBM Security Network Protection (XGS)**

IBM Security Network Protection (XGS) provides a web services API that enables third-party applications such as Deep Discovery Director (Consolidated Mode) to directly submit suspicious objects. IBM XGS can perform the following functions:

- Quarantine hosts infected with malware
- Block communication to C&C servers
- Block access to URLs found to be distributing malware
To integrate Deep Discovery Director (Consolidated Mode) with IBM XGS, configure a generic agent to do the following:

- Accept alerts that adhere to a specific schema
- Create quarantine rules based on a generic ATP translation policy

The ATP translation policy allows several categories of messages to take different actions on IBM XGS, including blocking and alerting.

**Configuring IBM Security Network Protection (XGS)**

**Procedure**

1. On the IBM XGS console, do the following to configure the generic agent:
   a. Go to **Manage System Settings > Network Settings > Advanced Threat Protection Agents**.
      
      The **Advanced Threat Protection Agents** window opens.
   b. Click **New**.
   c. Provide the following information:
      - Name: Type a name
      - Agent Type: Select **Generic**
      - Address: Deep Discovery Director (Consolidated Mode) management port IP address in IPv4 or IPv6 format
      - User name: Existing authentication credential
• Password: Existing authentication credential

**Table 5-7. Valid Character Sets**

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

2. Click **Save Confirmation**.

The **Deploy Pending Changes** window opens.

3. To apply changes to IBM XGS, click **Deploy**.
The new agent appears in the **Advanced Threat Protection Agents** list.

4. On the Deep Discovery Director (Consolidated Mode) management console, go to **Threat Intelligence > Sharing Settings > Auxiliary Products/Services**.

The **Auxiliary Products/Services** screen appears.

5. Select **Distribute objects to auxiliary products/services**.

6. Select **IBM Security Network Protection (XGS)**.

7. Click **Legal Statement**.

The **Legal Statement** dialog appears.

8. Read and accept the **Legal Statement**.

---

**Important**

To enable integration with this auxiliary product/service, you must accept the **Legal Statement**.

---

9. Type the server address.
Note
The server address must be the IPv4 address or FQDN of the auxiliary product/service.

10. Type the user name and password used for authentication.

11. (Optional) Click Test Connection.

12. To send object information from Deep Discovery Director (Consolidated Mode) to this auxiliary product/service, configure the following criteria:
   • Object type:
     • C&C Callback Address
       • IPv4 address
       • URL
     • Suspicious Object
       • IPv4 address
       • URL
   • Risk level:
     • High only
     • High and medium
     • High, medium, and low

13. Click Save.

14. (Optional) On the IBM XGS console, go to Secure Policy Configuration > Security Policies > Active Quarantine Rules to view suspicious objects and C&C callback addresses sent by Deep Discovery Director (Consolidated Mode) to IBM XGS.
**Note**

Suspicious objects with a low risk level do not appear in the IBM XGS **Active Quarantine Rules**. To view all suspicious objects sent by Deep Discovery Director (Consolidated Mode), go to **Security Policy Configuration > Advanced Threat Policy** and specify the following settings:

- **Agent Type**: Generic
- **Alert Type**: Reputation
- **Alert Severity**: Low

Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Consolidated Mode) are displayed.

---

**Palo Alto Panorama or Firewalls**

Palo Alto Networks® firewalls identify and control applications, regardless of port, protocol, encryption (SSL or SSH) or evasive characteristics.

Deep Discovery Director (Consolidated Mode) generates IPv4, domain, and URL suspicious objects that can be downloaded to the URL category of Palo Alto Firewall or Palo Alto Panorama™ as match criteria to allow for exception-based behavior.

Use URL categories in policies as follows:

- Identify and allow exceptions to general security policies for users who belong to multiple groups within Active Directory

  Example: Deny access to malware and hacking sites for all users, while allowing access to users that belong to the security group.

- Allow access to streaming media category, but apply quality of service policies to control bandwidth consumption

- Prevent file download and upload for URL categories that represent higher risks

  Example: Allow access to unknown sites, but prevent upload and download of executable files from unknown sites to limit malware propagation.
• Apply SSL decryption policies that allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.

Configuring Palo Alto Panorama or Firewalls

Procedure

1. On the Deep Discovery Director (Consolidated Mode) management console, go to Threat Intelligence > Sharing Settings > Auxiliary Products/Services.
   The Auxiliary Products/Services screen appears.
2. Select Distribute objects to auxiliary products/services.
3. Select Palo Alto Panorama or Firewalls.
4. Click Legal Statement.
   The Legal Statement dialog appears.
5. Read and accept the Legal Statement.

   **Important**

   To enable integration with this auxiliary product/service, you must accept the Legal Statement.

6. (Optional) By default, Deep Discovery Director (Consolidated Mode) shares threat intelligence data through HTTPS. You can also share using HTTP. Under Server Settings, select Share information using HTTP and specify the port number.

7. Under Criteria, select the risk level of the objects to be included in the threat intelligence data file.

8. Click Save.

9. (Optional) Click Generate Now.

   **Note**

   After the file generation is successful, you can click the URL to download the threat intelligence data file to view the content.
10. Configure Palo Alto Firewall or Palo Alto Panorama™ to obtain threat intelligence data from Deep Discovery Director (Consolidated Mode). For more information, see the documentation for the integrated product/service.
Chapter 6

Appliances

Learn how to manage appliances, perform plan related tasks, maintain the repository, and view appliance logs in the following topics:

•  Directory on page 6-2
•  Plans on page 6-8
•  Repository on page 6-29
•  Logs on page 6-33
Directory

The Directory displays information about Deep Discovery appliances that are registered to Deep Discovery Director (Consolidated Mode).

- Left pane: Appliance tree with groups (represented by folders) and appliances (identified by display names, initially identical to their host names)

  Note
  An exclamation mark icon attached to the appliance icon indicates that the connection with this appliance has been lost.

- Right pane: Information about plans, appliances, installed or hosted update files, etc.

On fresh installations, the Directory is empty and only displays the following default groups:

- **Managed**: Appliances placed in this group can receive plan information, updates, and Virtual Analyzer images from Deep Discovery Director. Appliances can also replicate their configuration to and from other compatible appliances.

- **Unmanaged**: Appliances placed in this group cannot receive plan information, updates, Virtual Analyzer images, or replicate their configuration.

Appliances can register to Deep Discovery Director (Consolidated Mode) on their respective management consoles. Newly registered appliances first appear in the Unmanaged group but can be moved to the Managed group at any time.

Directory Tasks

You can use the Directory mainly to view information about groups and appliances, and plans that are associated with these objects. Selecting an object in the left pane displays information in the right pane.

The following table describes the three object types and the available information for each object.
## TABLE 6-1. Directory Object Types

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
</table>
| Appliances  | • **Plan**: Plans that were or will be deployed to the appliance  
                        • **Appliance**: Identifiers such as IP address, virtual IP address, host name and display name, threat intelligence sync times, and other information |
|             | **Note**  
                        For Deep Discovery Analyzer clusters, Deep Discovery Director (Consolidated Mode) also displays the following:  
                        • **Active primary appliance**: Information on the active primary appliance (high availability cluster and load balancing cluster)  
                        • **Passive primary appliance**: Information on the passive primary appliance (high availability cluster)  
                        • **Secondary appliances**: Information on the secondary appliance (load balancing cluster)  
                        For Deep Discovery Director - Network Analytics servers, Deep Discovery Director (Consolidated Mode) also displays the license status and connected data sources.  
                        • **Updates**: Build number and installation date of all installed updates, and information about where and when the appliance's configuration settings were replicated from  
                        • **Virtual Analyzer**: Information about the Virtual Analyzer configuration of the appliance, such as source, internal Virtual Analyzer maximum images and instances, and deployed images and instances |
|             | **Note**  
                        For Deep Discovery Analyzer active primary appliances, click on **All Nodes** to display the total number of instances in use for all nodes in the cluster.|

---
### Object Displayed Information

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Overview of appliances and plans associated with that group, including statuses and connection information.</td>
</tr>
</tbody>
</table>

### Other Directory Tasks

You can also perform the following actions:

**TABLE 6-2. Other Directory Tasks**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add groups</td>
<td>Add groups to better organize appliances, such as by location or business unit.</td>
</tr>
<tr>
<td></td>
<td>To add a group:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the group name and then select <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the text box, type a name with a maximum of 256 characters.</td>
</tr>
<tr>
<td>Edit group or appliance names</td>
<td>To edit a group or appliance name:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the group or appliance name and then select <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the text box, type a name with a maximum of 256 characters.</td>
</tr>
<tr>
<td>Sync Threat Intelligence</td>
<td>Tells the appliance to sync threat intelligence from Deep Discovery Director (Consolidated Mode).</td>
</tr>
<tr>
<td></td>
<td>To sync threat intelligence, click the menu icon beside the appliance name and then select <strong>Sync Threat Intelligence</strong>.</td>
</tr>
</tbody>
</table>

**Note**

Appliances automatically sync threat intelligence from Deep Discovery Director (Consolidated Mode). Syncing threat intelligence requires some time to complete. Avoid using this action if possible.
<table>
<thead>
<tr>
<th><strong>Action</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **Move groups or appliances** | To move a group or an appliance to a different group:  
1. Click the menu icon beside the group or appliance name and then select **Move**.  
2. In the window, select the new folder and then click **Move**.  
This function is disabled whenever:  
• Deployment of one or more associated plans is pending or in progress.  
• The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**. |
| **Delete groups** | Delete empty or unused groups to simplify the Directory.  
To delete a group, click the menu icon beside the group name and then select **Delete**.  
---  
**WARNING!**  
Deleting a group cancels the plans associated with that group and moves appliances to the **Unmanaged** group. Only groups without unfinished plans can be deleted.  
---  
This function is disabled whenever:  
• Deployment of one or more associated plans is pending or in progress.  
• The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**. |
<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete appliances</td>
<td>To delete an appliance, click the menu icon beside the display name and then select <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>This function is disabled whenever the appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to <strong>All</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong></td>
</tr>
<tr>
<td></td>
<td>• Deleting an appliance unregisters it from Deep Discovery Director (Consolidated Mode), stops all connections, and cancels all associated plans.</td>
</tr>
<tr>
<td></td>
<td>• Deleting a Deep Discovery Inspector appliance causes that Deep Discovery Inspector appliance to automatically unregister from Deep Discovery Director - Network Analytics. Correlated events that were derived from data provided by that Deep Discovery Inspector appliance become unavailable.</td>
</tr>
<tr>
<td></td>
<td>Re-registering that Deep Discovery Inspector appliance to Deep Discovery Director does not automatically re-register it to Deep Discovery Director - Network Analytics. To restore full functionality, go to the management console of the Deep Discovery Inspector appliance and re-register it to its originally registered Deep Discovery Director - Network Analytics server.</td>
</tr>
<tr>
<td>Switch views</td>
<td>To switch between custom views, click on the name beside <strong>Views</strong> and then select the view to switch to.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Customize columns| Customize columns and save new custom views to better organize all the information.  
To create a custom view:  
1. Click on the name beside **Views** and then select **Customize columns**.  
2. Type a unique custom view name.  
3. Select any combination of columns to include in the custom view.  
4. Click **Save**.  

  **Tip**  
  The column order can be rearranged using drag-and-drop. |
| Edit custom views| To edit a custom view:  
1. Click on the name beside **Views** and then select the **pencil** icon beside the view.  
2. (Optional) Edit the custom view name.  
3. Edit the combination of columns.  
4. Click **Save**. |
| Delete custom views| To delete a custom view, click on the name beside **Views** and then select the **trash can** icon beside the view. |
Open management console

Open the management console of the Deep Discovery Director - Network Analytics server to configure the server.

Do one of the following to open the management console:

- Click the menu icon beside the Deep Discovery Director - Network Analytics server name and then select Management Console.
- Click Management Console next to a Deep Discovery Director - Network Analytics server name in the Display Name column.
- On the left pane, click on the Deep Discovery Director - Network Analytics server name, and then click Management console on the right side of the right pane.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open management console</td>
<td>Open the management console of the Deep Discovery Director - Network Analytics server to configure the server. Do one of the following to open the management console:</td>
</tr>
<tr>
<td></td>
<td>• Click the menu icon beside the Deep Discovery Director - Network Analytics server name and then select Management Console.</td>
</tr>
<tr>
<td></td>
<td>• Click Management Console next to a Deep Discovery Director - Network Analytics server name in the Display Name column.</td>
</tr>
<tr>
<td></td>
<td>• On the left pane, click on the Deep Discovery Director - Network Analytics server name, and then click Management console on the right side of the right pane.</td>
</tr>
</tbody>
</table>

**Plans**

Plans define the scope and schedule of deployments to target appliances.

Each plan is created for a specific set of target appliances and is deployed only once during a user-defined period. The plan to be deployed must match the product and language of the target appliances.

When a plan is deployed, Deep Discovery Director (Consolidated Mode) sends instructions to the target appliances on when to download required files, and on when to execute the plan. If the plan is not deployed immediately, appliances download files and execute the plan according to a schedule with the following factors:

- Deployment start
- Download period
- Execution start

---

**Important**

All times are based on appliance local time
The Plans screen displays a list of all created plans with the following information:

**TABLE 6-3. Plans**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specified during plan creation</td>
</tr>
<tr>
<td>Type</td>
<td>Type of plan deployed to targets. Deep Discovery Director (Consolidated Mode) currently supports the following plan types:</td>
</tr>
<tr>
<td></td>
<td>• Hotfix / Critical patch / Firmware</td>
</tr>
<tr>
<td></td>
<td>• Virtual Analyzer images</td>
</tr>
<tr>
<td></td>
<td>• Configuration replication</td>
</tr>
<tr>
<td>Status</td>
<td>A plan can have any of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• In progress: Deployment started at the specified time and at least one appliance has executed the plan.</td>
</tr>
<tr>
<td></td>
<td>• Pending: Deployment has not started or no appliances have received plan information from Deep Discovery Director (Consolidated Mode).</td>
</tr>
<tr>
<td></td>
<td>• Completed: Deployment started at the specified time and all appliances successfully executed the plan.</td>
</tr>
<tr>
<td></td>
<td>• Unsuccessful: Deployment did not start at the specified time or at least one appliance was unable to execute the plan.</td>
</tr>
<tr>
<td>Schedule</td>
<td>When a plan is scheduled to deploy and execute. Can display one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Custom: Plan deployment, required file downloads, and plan execution happen according to a schedule. All times are based on appliance local time.</td>
</tr>
<tr>
<td></td>
<td>• Immediate: Plan is deployed immediately, and appliances execute the plan immediately after downloading required files. All times are based on server local time.</td>
</tr>
<tr>
<td>Deployment Start</td>
<td>Date and time deployment starts or started</td>
</tr>
<tr>
<td>Description</td>
<td>Specified during plan creation</td>
</tr>
<tr>
<td>Creator</td>
<td>User account that created the plan</td>
</tr>
</tbody>
</table>
Tip
The list view can be filtered by clicking the Filters button and using the drop-down lists and search box that appear.

Plan Tasks

Clicking a plan name opens the details screen for that specific plan.

<table>
<thead>
<tr>
<th>TABLE 6-4. Plan Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK</strong></td>
</tr>
<tr>
<td>Plan information</td>
</tr>
<tr>
<td>Appliance information</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Appliance Statuses

Deep Discovery Director (Consolidated Mode) displays any of the following appliance statuses.

<table>
<thead>
<tr>
<th>TABLE 6-5. Appliance Statuses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STATUS</strong></td>
</tr>
<tr>
<td>Pending</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>In progress</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Suspended</td>
</tr>
<tr>
<td>Completed</td>
</tr>
<tr>
<td>Unsuccessful</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Unreachable</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cancelled</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Other Plan Tasks

You can also perform the following tasks:

**TABLE 6-6. Other Tasks**

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add one of the following types of plans to Deep Discovery Director (Consolidated Mode).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hotfix / Critical Patch / Firmware</strong>: For details, see <em>Adding a Hotfix / Critical Patch / Firmware Deployment Plan on page 6-13</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Analyzer images</strong>: For details, see <em>Adding a Virtual Analyzer Images Deployment Plan on page 6-14</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration replication</strong>: For details, see <em>Adding a Configuration Replication Plan on page 6-17</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director (Consolidated Mode) does not allow the creation of new plans when the license status is <strong>Not Activated</strong> or <strong>Expired</strong>. Existing plans will deploy and execute as usual.</td>
</tr>
<tr>
<td></td>
<td>To activate Deep Discovery Director (Consolidated Mode), see <em>License on page 8-42</em>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click a plan name with the status <strong>Pending</strong> and then click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Only plans that have not been deployed can be edited.</td>
</tr>
<tr>
<td>Cancel plan</td>
<td>Click a plan name with any of the following statuses and then click <strong>Cancel Plan</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>In progress</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suspended</strong></td>
</tr>
</tbody>
</table>
Adding a Hotfix / Critical Patch / Firmware Deployment Plan

Use this type of plan to deploy product updates and upgrades to compatible appliances.

**Procedure**

1. Go to Appliances > Plans and click on Add.
   
   The Add Plan screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select Hotfix / Critical patch / Firmware as type.

4. (Optional) Type a description.

5. Select a hotfix, critical patch, or firmware file from the list.

   **Note**
   
   Deep Discovery Director (Consolidated Mode) displays the list of files that are available in the repository. Verify that the file matches the product and language of the target appliances.

6. Select target appliances. Deep Discovery Director (Consolidated Mode) only displays compatible appliances.

   **Note**
   
   Installing updates automatically restarts the target appliances.

---

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Select a plan in the list and click Copy.</td>
</tr>
<tr>
<td>Create plan</td>
<td>Click a plan with the status Unsuccessful and then click Create Plan. Deep Discovery Director (Consolidated Mode) will create a new plan based on the settings of the unsuccessfully deployed plan.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select a plan in the list with the status Pending and click Delete.</td>
</tr>
</tbody>
</table>
7. Specify the schedule.
   
   • **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.
   
   • **Deployment start**: Date at which this plan will be deployed.

   **Note**
   Plans are always deployed at 12:00 am (00:00) of the selected date.

   • **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

   **Note**
   • If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
   
   • Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

   • **Execution start**: Date and time at which this plan will be executed.

   **Tip**
   Select **By schedule** to prevent the plan from executing at an unexpected time.

   • **Immediate**: Starts immediately after the plan is saved.

8. Click **Save**.

---

**Adding a Virtual Analyzer Images Deployment Plan**

Use this type of plan to deploy Virtual Analyzer images to compatible appliances.

The following table lists requirements that must be fulfilled by compatible appliances:
**TABLE 6-7. Requirements for Compatible Appliances**

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| License                                          | • **Status**: Activated  
• **Type**: Full                                                                 |
| Virtual Analyzer                                 | • **Status**: Enabled  
| Note                                             | Virtual Analyzer images can be deployed to Deep Discovery Inspector appliances whose Virtual Analyzer status is disabled. Deep Discovery Inspector automatically enables Virtual Analyzer after the images have been deployed.  
• **Source**: Internal                                                                 |
| Deep Discovery Director (Consolidated Mode)      | • Integration with Deep Discovery Director (Consolidated Mode) 1.1  
• Must be registered to Deep Discovery Director (Consolidated Mode)  
• Must be in a Managed group                                                                 |

**Procedure**

1. Go to **Appliances** > **Plans** and click on **Add**.  
The **Add Plan** screen appears.
2. Type a plan name with a maximum of 256 characters.
3. Select **Virtual Analyzer images** as type.
4. (Optional) Type a description.
5. Select a product from the list.
6. Select a maximum images value from the list.
7. Select a maximum instances value from the list.
8. Click **Images**.

The **Virtual Analyzer Images** dialog appears.

---

**Note**

Deep Discovery Director (Consolidated Mode) displays the list of Virtual Analyzer images that are available in the repository.

---

9. Select the final configuration of Virtual Analyzer images to deploy and click **Save**.

---

**Important**

- The selected configuration replaces any configuration currently deployed on target appliances.
- To keep currently deployed images on target appliances, select them as part of the final configuration. The target appliances will automatically determine if the selected images are identical and need to be deployed.

---

10. (Optional) Modify the instances allocated to any image.

11. Select target appliances. Deep Discovery Director (Consolidated Mode) only displays compatible appliances.

---

**Note**

Deep Discovery Analyzer secondary appliances are not displayed because Virtual Analyzer images and settings are automatically synced from the primary appliance. To deploy Virtual Analyzer images to Deep Discovery Analyzer secondary appliances, select the corresponding primary appliance.

---

12. Specify the schedule.

- **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.
- **Deployment start**: Date at which this plan will be deployed.

---

**Note**

Plans are always deployed at 12:00 am (00:00) of the selected date.
• **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

---

**Note**

• If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.

• Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

---

• **Execution start**: Date and time at which this plan will be executed.

---

**Tip**

Select **By schedule** to prevent the plan from executing at an unexpected time.

---

• **Immediate**: Starts immediately after the plan is saved.

13. Click **Save**.

---

**Adding a Configuration Replication Plan**

Use this type of plan to replicate the configuration settings of one appliance to compatible appliances.

Each Deep Discovery product supports the replication of a different combination of configuration settings. For details, see the following:

• *Deep Discovery Analyzer Replicated Configuration Settings on page 6-19*

• *Deep Discovery Email Inspector Replicated Configuration Settings on page 6-21*

• *Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings on page 6-23*

• *Deep Discovery Inspector 5.0 Replicated Configuration Settings on page 6-26*
Procedure

1. Go to Appliances > Plans and click on Add.
   The Add Plan screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select Configuration replication as type.

4. (Optional) Type a description.

5. Select the replication source from the list.

   Tip
   Select a product from the View drop-down list to only display the selected product's appliances.

6. Select target appliances. Deep Discovery Director (Consolidated Mode) only displays compatible appliances.

7. Specify the schedule.
   • Custom: Deploys the plan, downloads the files, and executes the plan as specified.
     • Deployment start: Date at which this plan will be deployed.

   Note
   Plans are always deployed at 12:00 am (00:00) of the selected date.

   • Download period: Period during which appliances are allowed to download the files required to execute the plan.
• **Note**

  - If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
  
  - Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

• **Execution start**: Date and time at which this plan will be executed.

• **Tip**

  Select **By schedule** to prevent the plan from executing at an unexpected time.

• **Immediate**: Starts immediately after the plan is saved.

8. Click **Save**.

---

**Deep Discovery Analyzer Replicated Configuration Settings**

The following table shows the screens and elements with replicated configuration settings.

**TABLE 6-8. Deep Discovery Analyzer Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>All widgets and settings</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>Submissions</td>
</tr>
<tr>
<td></td>
<td>Filter settings</td>
</tr>
<tr>
<td>Suspicious Objects &gt;</td>
<td>User-defined Match List</td>
</tr>
<tr>
<td>User-defined Match List</td>
<td></td>
</tr>
<tr>
<td>Exceptions</td>
<td>Exceptions list</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Sandbox Management</td>
<td>Archive Passwords</td>
</tr>
<tr>
<td></td>
<td>Submission Settings</td>
</tr>
<tr>
<td></td>
<td>Smart Feedback</td>
</tr>
<tr>
<td></td>
<td>Cloud Sandbox</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Alerts</td>
<td>Rules</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports</td>
<td>Schedules</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
</tr>
<tr>
<td>Administration &gt; Updates &gt; Component Update Settings</td>
<td>Log Settings</td>
</tr>
<tr>
<td></td>
<td>Smart Protection</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services</td>
<td>Proxy</td>
</tr>
<tr>
<td></td>
<td>SMTP</td>
</tr>
<tr>
<td></td>
<td>Time</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>Password Policy</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts</td>
<td>Accounts</td>
</tr>
<tr>
<td></td>
<td>Contacts</td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Back Up</td>
<td>Automatic backup settings</td>
</tr>
</tbody>
</table>
Deep Discovery Email Inspector Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

**TABLE 6-9. Deep Discovery Email Inspector Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>All widgets and settings</td>
</tr>
<tr>
<td>Policy &gt; Policy</td>
<td>Actions</td>
</tr>
<tr>
<td>Policy &gt; Policy</td>
<td>Recipient Notification</td>
</tr>
<tr>
<td>Policy &gt; Policy</td>
<td>Message Tags</td>
</tr>
<tr>
<td>Policy &gt; Policy</td>
<td></td>
</tr>
<tr>
<td>Policy &gt; Exceptions</td>
<td>Messages</td>
</tr>
<tr>
<td>Policy &gt; Exceptions</td>
<td>Objects</td>
</tr>
<tr>
<td>Policy &gt; Exceptions</td>
<td>URL Keywords</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Alerts &gt; Rules</td>
<td>All alert notification rule settings</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports &gt; Schedules</td>
<td>All report schedules</td>
</tr>
<tr>
<td>Administration &gt; Component Updates</td>
<td>Schedule</td>
</tr>
<tr>
<td>Administration &gt; Component Updates</td>
<td>Source</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Administration &gt; System Settings</td>
<td><strong>Operation Mode</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Proxy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SMTP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Time</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SNMP</strong></td>
</tr>
<tr>
<td>Administration &gt; Mail Settings</td>
<td><strong>Connections</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Message Delivery</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Limits and Exceptions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SMTP Greeting</strong></td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services</td>
<td><strong>Microsoft Active Directory</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Log Settings</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SFTP</strong></td>
</tr>
<tr>
<td>Administration &gt; Scanning / Analysis</td>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td></td>
<td><strong>File Passwords</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Smart Protection</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Smart Feedback</strong></td>
</tr>
<tr>
<td></td>
<td><strong>YARA Rules</strong></td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Storage Maintenance</td>
<td>Storage maintenance values</td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts</td>
<td><strong>Accounts</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Contacts</strong></td>
</tr>
</tbody>
</table>
Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

** TABLE 6-10. Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings **

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>Affected Hosts</td>
</tr>
<tr>
<td></td>
<td>Only Saved Searches</td>
</tr>
<tr>
<td></td>
<td>Affected Hosts - Host</td>
</tr>
<tr>
<td></td>
<td>Details</td>
</tr>
<tr>
<td></td>
<td>All Detections</td>
</tr>
<tr>
<td>Reports</td>
<td>Schedules</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Notifications</td>
<td>Notification Settings &gt; Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Risk Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Suspicious Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Network Traffic</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Unanalyzed Sample Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Virtual Analyzer Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Deny List</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Retro Scan Detections</td>
</tr>
<tr>
<td></td>
<td>Delivery Options &gt; Email Settings</td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning</td>
<td>Hosts / Ports</td>
</tr>
<tr>
<td></td>
<td>Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Web Reputation</td>
</tr>
<tr>
<td></td>
<td>Application Filters</td>
</tr>
<tr>
<td></td>
<td>Deny List / Allow List</td>
</tr>
<tr>
<td></td>
<td>Detection Rules</td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer</td>
<td>File Submissions</td>
</tr>
<tr>
<td></td>
<td>Internal Virtual Analyzer &gt; Passwords</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets</td>
<td>Network Groups</td>
</tr>
<tr>
<td></td>
<td>Registered Domains</td>
</tr>
<tr>
<td></td>
<td>Registered Services</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/</td>
<td>Syslog</td>
</tr>
<tr>
<td>Services</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; System Settings</td>
<td>Proxy</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>Time</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
</tr>
<tr>
<td>Administration &gt; Accounts</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt;</td>
<td></td>
</tr>
<tr>
<td>Storage Maintenance</td>
<td></td>
</tr>
</tbody>
</table>
Deep Discovery Inspector 5.0 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

**TABLE 6-11. Deep Discovery Inspector 5.0 Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>Affected Hosts</td>
</tr>
<tr>
<td></td>
<td>Only Saved Searches</td>
</tr>
<tr>
<td></td>
<td>Affected Hosts - Host Details</td>
</tr>
<tr>
<td></td>
<td>All Detections</td>
</tr>
<tr>
<td>Reports</td>
<td>Schedules</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Notifications</td>
<td>Notification Settings &gt; Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Risk Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Suspicious Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Network Traffic</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Unanalyzed Sample Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Virtual Analyzer Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Deny List</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Retro Scan Detections</td>
</tr>
<tr>
<td></td>
<td>Delivery Options &gt; Email Settings</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning</td>
<td>Hosts / Ports</td>
</tr>
<tr>
<td></td>
<td>Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Web Reputation</td>
</tr>
<tr>
<td></td>
<td>Application Filters</td>
</tr>
<tr>
<td></td>
<td>Deny List / Allow List</td>
</tr>
<tr>
<td></td>
<td>Detection Rules</td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
</tr>
<tr>
<td></td>
<td>Packet Capture</td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer Setup</td>
<td>Setup</td>
</tr>
<tr>
<td></td>
<td>Only the internal Virtual Analyzer proxy settings and the cloud sandboxes setting.</td>
</tr>
<tr>
<td></td>
<td>File Submissions</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
<tr>
<td></td>
<td>Internal Virtual Analyzer &gt; Passwords</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets</td>
<td>Network Groups</td>
</tr>
<tr>
<td></td>
<td>Registered Domains</td>
</tr>
<tr>
<td></td>
<td>Registered Services</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/</td>
<td>Threat Intelligence Sharing</td>
</tr>
<tr>
<td>Services</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
</tbody>
</table>
The Repository screen displays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here.

- **Uploading a Hotfix / Critical Patch / Firmware File on page 6-30**
- **Uploading Virtual Analyzer Images on page 6-31**
- **Upload Center on page 6-32**

### Hotfixes / Critical Patches / Firmware

Use the **Hotfixes / Critical Patches / Firmware** screen, in **Appliances > Repository > Hotfixes / Critical Patches / Firmware**, to view already uploaded update files, delete unused update files, and upload new update files for deployment.

Use filters to search by update or upgrade type, product, language, and file name or version.

To delete a file, select the file from the list and then click **Delete**.
Uploading a Hotfix / Critical Patch / Firmware File

Deep Discovery Director (Consolidated Mode) supports simultaneous uploading of up to five files through single-file upload sessions.

---

**Important**

Closing the browser or tab that contains the management console cancels all uploads in progress.

---

**Procedure**

1. Go to Appliances > Repository > Hotfixes / Critical Patches / Firmware.
2. Click Upload.
3. Click Select and then select a valid TAR file.
4. (Optional) Type or paste the 64-character SHA-256 hash value of the selected file for verification.
5. (Optional) Type a description.
6. Click Upload.

---

**Virtual Analyzer Images**

Use the Virtual Analyzer Images screen, in Appliances > Repository > Virtual Analyzer Images, to view already uploaded image files, delete unused image files, and upload new image files for deployment.

To delete a file, select the file from the list and then click Delete.
**Important**


### Uploading Virtual Analyzer Images

Deep Discovery Director (Consolidated Mode) supports consecutive uploading of up to three Virtual Analyzer image files through SFTP or network folder. Deep Discovery Director (Consolidated Mode) opens a connection to the SFTP or network server in the background for the upload session, allowing you to navigate away from the screen and perform other tasks while waiting for the upload to complete.

**Procedure**

1. Go to **Appliances > Repository > Virtual Analyzer Images**.
2. Click **Upload**.
3. Select a source from the list.
   - **SFTP**
   - **Network Folder**
4. Type the server details.
   - **SFTP**: Type the IP address or FQDN of the server, the port number, the user name, and the password.
   - **Network Folder**: Type the user name and password.

**Note**

Deep Discovery Director (Consolidated Mode) saves the server information and logon credentials automatically.

5. Type the details of at least one Virtual Analyzer image file.
a. Type file paths.
b. Type unique image names.
c. (Optional) Type descriptions.

6. Click **Upload**.

---

**Upload Center**

Information about files that are uploading and that have been uploaded can be displayed using the Upload Center panel. Toggle the panel by clicking on the up-arrow-drawer icon in the top right corner of the screen. The panel is divided into the following two tabs:

- **Uploading Files on page 6-32**
- **Upload History on page 6-33**

**Uploading Files**

Information about files that are being uploaded to Deep Discovery Director (Consolidated Mode) is displayed in this tab.

To cancel a file upload, click on the x beside the upload.

File uploads are done in the following stages:

**Table 6-12. File Upload Stages**

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Calculating</td>
<td>The first parts of the file upload are being verified to ensure that the file upload is valid.</td>
</tr>
<tr>
<td>2: Uploading to the repository</td>
<td>The file is being uploaded to the repository. All SFTP server and network folder file uploads can be cancelled by any user.</td>
</tr>
<tr>
<td>3: Processing</td>
<td>The file upload to the repository has completed and integrity is being verified. File uploads cannot be cancelled in this stage.</td>
</tr>
</tbody>
</table>

File uploads display the following information:
<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>The file name.</td>
</tr>
<tr>
<td>(X KB / MB / GB)</td>
<td>The file size in KB / MB / GB.</td>
</tr>
<tr>
<td>Time left</td>
<td>The estimated time until the file upload is complete based on the file size and upload speed.</td>
</tr>
<tr>
<td>(X KB/s / MB/s / GB/s)</td>
<td>The upload speed in KB/s / MB/s / GB/s.</td>
</tr>
</tbody>
</table>

**Upload History**

Information about files that have been uploaded to Deep Discovery Director (Consolidated Mode) is displayed in this tab.

To clear the upload history, click **Clear All**.

Uploaded files display the following information:

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>One of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Successful</strong>: The file upload was successful.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unsuccessful</strong>: The file upload was unsuccessful.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cancelled</strong>: The file upload was cancelled.</td>
</tr>
<tr>
<td>File name</td>
<td>The file name.</td>
</tr>
</tbody>
</table>

**Logs**

The **Logs** screen displays various logs from Deep Discovery appliances that are registered to Deep Discovery Director (Consolidated Mode).
Email Message Tracking

Track any email message that passed through Deep Discovery Email Inspector, including blocked and delivered messages. Deep Discovery Email Inspector records message details, including the sender, recipients, and the taken policy action.

Email message tracking logs indicate if an email message was received or sent by Deep Discovery Email Inspector. Email message tracking logs also provide evidence about Deep Discovery Email Inspector investigating an email message.

Display Options and Search Filters

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

**TABLE 6-15. Display Options and Search Filters: Email Message Tracking**

<table>
<thead>
<tr>
<th>FILTER OPTIONS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level</td>
<td>Filter options include the following risk level settings:</td>
</tr>
<tr>
<td>High</td>
<td>Displays high-risk email messages</td>
</tr>
<tr>
<td>Medium</td>
<td>Displays medium-risk email messages</td>
</tr>
<tr>
<td>Low</td>
<td>Displays low-risk email messages</td>
</tr>
<tr>
<td>No risk</td>
<td>Displays no-risk email messages</td>
</tr>
<tr>
<td>Unrated</td>
<td>Displays email messages that were unable to be scanned</td>
</tr>
<tr>
<td>Unavailable</td>
<td>Displays spam/graymail messages and email messages with content violation</td>
</tr>
<tr>
<td>All</td>
<td>Displays all email messages</td>
</tr>
</tbody>
</table>
### Filter Options

<table>
<thead>
<tr>
<th>Period</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 hours</td>
<td></td>
</tr>
<tr>
<td>Last 7 days</td>
<td></td>
</tr>
<tr>
<td>Last 14 days</td>
<td></td>
</tr>
<tr>
<td>Last 30 days</td>
<td></td>
</tr>
<tr>
<td>Last 60 days</td>
<td></td>
</tr>
<tr>
<td>Custom range</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitored domain</th>
<th>Select domains from which email messages should be displayed.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Basic search</th>
<th>Type a case-insensitive keyword in the basic search field to search a partial sender, email header (from), recipient or email header (to) match.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Advanced Search</th>
<th>Search by user-defined criteria sets. Each set includes one or more of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Attributes</td>
</tr>
<tr>
<td></td>
<td>• Operators</td>
</tr>
<tr>
<td></td>
<td>• Associated values</td>
</tr>
</tbody>
</table>

### Viewing Email Message Tracking Logs

**Procedure**

1. Go to **Appliances > Logs > Email Message Tracking**.
   
   The **Email Message Tracking** screen appears.

2. Select the risk level by using the drop-down control.

3. Select a time period.

4. Select domains from which email messages should be displayed.
5. To run a basic search, type a keyword in the search text box, and then press ENTER or click the magnifying glass icon.

By default, Deep Discovery Director (Consolidated Mode) searches Email Messages by Recipients, Email Header (To), Sender, Email Header (From).

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

For details, see Email Message Tracking Advanced Search Filters on page 6-36.

7. (Optional) Click the Export icon, select a delimiter to use, and then click OK to export and download the currently filtered list of email message tracking logs to a CSV file with the chosen delimiter.

---

**Email Message Tracking Advanced Search Filters**

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

For details, see Adding an Email Message Tracking Advanced Search Filter on page 6-37.

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

**TABLE 6-16. Search Criteria: Email Message Tracking**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Recipient</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Header (From)</td>
<td>Has from/No from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Email Header (To)</td>
<td>Equals/Contains/Does not contain</td>
<td>Type a value</td>
</tr>
<tr>
<td>Message ID</td>
<td>Contains/Does not contain</td>
<td>Type a value</td>
</tr>
</tbody>
</table>
### Adding an Email Message Tracking Advanced Search Filter

**Procedure**

1. To create an Email Message Tracking advanced search filter, go to Appliances > Logs > Email Message Tracking, and then click Advanced.

2. Select an attribute and an associated operator.

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

4. (Optional) Click AND or OR to include other criteria sets in the search filter.

---

#### Attribute, Operator, and Action Table

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>OPERATOR</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td>Source IP</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>Sender IP</td>
<td>Contains/Does not contain/Equals</td>
<td>Type a value</td>
</tr>
<tr>
<td></td>
<td>In range/Not in range</td>
<td>Type a range</td>
</tr>
<tr>
<td>Latest Status</td>
<td>In/Not in</td>
<td>Select one or more statuses</td>
</tr>
</tbody>
</table>

---

**Tip**

Type a keyword to search a partial match.

**Note**

You can add multiple criteria entries by pressing ENTER after typing a value.
5. Click **Apply**.

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

6. (Optional) Click the right-arrow icon beside the **Risk level** drop-down list to close the advanced search feature.

---

**MTA**

View connection details about Postfix and SMTP activity on your network.

**Querying MTA Logs**

**Procedure**

1. Go to **Appliances > Logs > MTA**.

   The **MTA** screen appears.

2. Select a time period.

3. Select which appliances to query for MTA logs.

4. Type a description keyword in the search text box and then click **Query**.

   Deep Discovery Director (Consolidated Mode) queries the selected appliances for matching MTA logs. This action may take several minutes.

   **Note**

   By default, results are sorted by **Data Source**, then by **Timestamp**.

5. (Optional) Click the **Export** icon, select a delimiter to use, and then click **OK** to export and download the currently filtered list of MTA logs to a CSV file with the chosen delimiter.
Chapter 7

Alerts

Learn about alert notifications and how to configure them in the following topics:

• About Alerts on page 7-2
• Triggered Alerts on page 7-2
• Built-in Rules on page 7-3
• Custom Rules on page 7-6
# About Alerts

Deep Discovery Director (Consolidated Mode) monitors a variety of events and can be configured to generate alerts to inform users of those events.

## Triggered Alerts

The **Triggered Alerts** screen displays the following information:

<table>
<thead>
<tr>
<th><strong>COLUMN</strong></th>
<th><strong>INFORMATION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered</td>
<td>The date and time when the alert was triggered.</td>
</tr>
<tr>
<td>Alert Level</td>
<td>An alert can be classified as any of the following levels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>: The event requires immediate attention</td>
</tr>
<tr>
<td></td>
<td>• <strong>Important</strong>: The event requires observation</td>
</tr>
<tr>
<td></td>
<td>• <strong>Informational</strong>: The event requires limited observation</td>
</tr>
<tr>
<td>Type</td>
<td>The type of rule that can trigger an alert can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System</strong>: A built-in, system related rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email Security</strong>: An email security related rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Network Security</strong>: A network security related rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong>: A user-specified custom rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggered the alert.</td>
</tr>
<tr>
<td>Criteria</td>
<td>The summarized criteria of the rule.</td>
</tr>
<tr>
<td></td>
<td>For custom rules, displays the advanced search filter.</td>
</tr>
<tr>
<td>COLUMN</td>
<td>INFORMATION</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Events</td>
<td>The triggered alert occurrences. Click the number to drill down to the Network Detections or Email Messages screen.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The number of records displayed on the Network Detections or Email Messages screen may differ from the number of events displayed on the Triggered Alerts screen because the related detection logs have been purged, or because appliances with related detections have been:</td>
</tr>
<tr>
<td></td>
<td>• Moved to the Unmanaged group</td>
</tr>
<tr>
<td></td>
<td>• Deleted from Deep Discovery Director (Consolidated Mode)</td>
</tr>
<tr>
<td></td>
<td>• Unregistered from Deep Discovery Director (Consolidated Mode)</td>
</tr>
<tr>
<td>Details</td>
<td>Click the icon to view the full alert details, including the list of recipients, subject, and message of the alert.</td>
</tr>
</tbody>
</table>

**Tip**

The list view can be filtered by clicking the Filters button and using the drop-down lists and search box that appear.

### Built-in Rules

The Built-in Rules screen displays the following information:
### Table 7-2. Built-in Rules Columns

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Level</td>
<td>An alert can be classified as any of the following levels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>: The event requires immediate attention</td>
</tr>
<tr>
<td></td>
<td>• <strong>Important</strong>: The event requires observation</td>
</tr>
<tr>
<td></td>
<td>• <strong>Informational</strong>: The event requires limited observation</td>
</tr>
<tr>
<td>Type</td>
<td>The type of rule that can trigger an alert can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System</strong>: A built-in, system related rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email Security</strong>: An email security related rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Network Security</strong>: A network security related rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggers the alert.</td>
</tr>
<tr>
<td></td>
<td>To edit a rule, click on any link in the <strong>Rule</strong> column.</td>
</tr>
<tr>
<td>Criteria</td>
<td>The summarized criteria of the rule.</td>
</tr>
<tr>
<td>Alert Frequency</td>
<td>The frequency at which the alert is generated when the rule criteria are met or exceeded.</td>
</tr>
<tr>
<td>Last Triggered</td>
<td>The date and time when the alert was last triggered.</td>
</tr>
<tr>
<td>Status</td>
<td>Click the toggle to enable or disable the rule.</td>
</tr>
</tbody>
</table>

### Editing a Built-in Rule

Edit rules to modify the frequency at which alerts are generated, the criteria, and the alert recipients.

---

**Note**

- By default, built-in rules are enabled and configured to send alerts to all contacts with valid email addresses.
- Only the criteria of **Email Security** rules can be modified.
Alerts

Procedure

1. Go to Alerts > Built-in Rules.
   
The Built-in Rules screen appears.

2. Click the name of the rule you want to edit in the Rule column.
   
The Edit Rule screen appears.

3. Toggle the status of this rule.

4. Configure how often alerts are generated:
   
   • **Check frequency**: Select the frequency at which the rule criteria are checked
   
   • **Alert frequency**: Select the frequency at which the alert is generated when the rule criteria are met or exceeded

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Shorter frequencies mean that the alert will be generated more often. Select longer frequencies to reduce the noise the alert generates.</td>
</tr>
<tr>
<td>• System rules are configured to continuously check the rule criteria. Only the Alert frequency can be modified.</td>
</tr>
<tr>
<td>• Security and custom rules are configured to immediately generate alerts if rule criteria are met or exceeded. Only the Check frequency can be modified.</td>
</tr>
</tbody>
</table>

5. For Email Security alerts, configure the following:
   
   • **Recipient watchlist**: Type an email address and press ENTER to add the specified email address to the recipient watchlist.
   
   • **Threshold**: Specify the detection threshold.
   
   • **Risk level**: Select the risk level and then click Apply.

6. (Optional) Select or disable **Send to all accounts**.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>This setting can be used in combination with the additional recipients field.</td>
</tr>
</tbody>
</table>
7. (Optional) Select a contact, type to search, or type an email address and press ENTER.

The contact or account is added to the recipients.

8. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

9. Click Save.

---

**Tip**

Click *Restore Defaults* to restore this rule to its default values.

---

**Custom Rules**

The **Custom Rules** screen displays the following information:

**TABLE 7-3. Custom Rules Columns**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Level</td>
<td>An alert can be classified as any of the following levels.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Critical</strong>: The event requires immediate attention</td>
</tr>
<tr>
<td></td>
<td>- <strong>Important</strong>: The event requires observation</td>
</tr>
<tr>
<td></td>
<td>- <strong>Informational</strong>: The event requires limited observation</td>
</tr>
<tr>
<td>Type</td>
<td>The type of rule that can trigger an alert can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Email Security</strong>: An email security related rule.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network Security</strong>: A network security related rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggers the alert.</td>
</tr>
<tr>
<td>Criteria</td>
<td>The advanced search filter used as criteria for this rule.</td>
</tr>
</tbody>
</table>
### Adding a Custom Rule

Add custom rules based on saved search filters to be alerted of specific threats.

**Note**

A maximum of 500 custom rules can be added.

**Procedure**

1. Go to Alerts > Custom Rules, and then click Add Rule.
   
   The Add Rule screen appears.

2. Toggle the status of this rule.

3. Type a name for this rule.

4. Select the alert level to assign to this rule.

5. Click Select Filter, select a Network Detections or Email Messages saved search to use as criteria for this rule, and then click Apply.

   **Important**

   Subsequent changes made to the selected filter will not be applied after the rule is created.

6. Do one of the following:

   - For Network Detections saved searches, select the appliances to include as data source of this rule.
• For **Email Messages** saved searches, select domains from which email messages should be included in this rule.

7. Select the frequency at which the rule criteria are checked.

    **Note**
    • Shorter frequencies mean that the alert will be generated more often. Select longer frequencies to reduce the noise the alert generates.
    • Custom rules are configured to immediately generate alerts if rule criteria are met or exceeded. Only the **Check frequency** can be modified.

8. Specify the threshold.

9. (Optional) Type a description for this rule.

10. (Optional) Select or disable **Send to all accounts**.

    **Note**
    This setting can be used in combination with the additional recipients field.

11. (Optional) Select a contact, type to search, or type an email address and press ENTER.

    The contact or account is added to the recipients.

12. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

13. Click **Save**.

**Other Custom Rules Tasks**

You can also perform the following tasks:
### TABLE 7-4. Other Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a rule</td>
<td>Click on a rule name to open the <strong>Edit Rule</strong> screen and edit the rule.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The advanced search filter used as criteria cannot be modified.</td>
</tr>
<tr>
<td>Delete rules</td>
<td>Select one or more rules to delete and then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Toggle rule status</td>
<td>Click on the toggle in the <strong>Status</strong> column to enable or disable the rule.</td>
</tr>
</tbody>
</table>
Chapter 8

Administration

Learn how to administer Deep Discovery Director (Consolidated Mode) in the following sections:

- Updates on page 8-2
- Integrated Products/Services on page 8-7
- System Settings on page 8-11
- Account Management on page 8-19
- System Logs on page 8-28
- System Maintenance on page 8-32
- License on page 8-42
Updates

Use the Updates screen, in Administration > Updates, to update components and install hotfixes, patches, and firmware upgrades to Deep Discovery Director (Consolidated Mode).

Components

Deep Discovery Director (Consolidated Mode) uses components to display related information about detections. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest threats.

Deep Discovery Director (Consolidated Mode) automatically checks the availability of new components upon opening the Components screen.

Updating Components

Manually update components at any time.

Procedure

1. Go to Administration > Updates > Components.
   The Component screen appears.

2. Click Update All.

Configuring Component Update Settings

Configure Deep Discovery Director (Consolidated Mode) to automatically update components.

Procedure

1. Go to Administration > Updates > Components.
   The Components screen appears.
2. Click **Settings**.

   The **Component Update Settings** screen appears.

3. Select a source to download updates from:
   - **Trend Micro ActiveUpdate server**: The Trend Micro ActiveUpdate server is the default source for the latest components.
   - **Other update source**: Select this option to specify a different update source. The update source URL must begin with "http://" or "https://".

4. Select **Automatically check for updates**.

5. Select whether to update every few hours or daily at a specific time.

   **Tip**
   
   Trend Micro recommends setting the update frequency to every two hours.

6. Click **Save**.

---

**Hotfixes / Patches**

Use the **Hotfixes / Patches** screen, in **Administration > Updates > Hotfixes / Patches**, to install Deep Discovery Director (Consolidated Mode) hotfixes and patches. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.
### Table 8-1. Hotfixes / Patches

<table>
<thead>
<tr>
<th>SYSTEM UPDATE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotfix</td>
<td>A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.</td>
</tr>
</tbody>
</table>

**Note**
A new hotfix may include previous hotfixes until Trend Micro releases a patch.

| Patch         | A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Non-Windows patches commonly include a setup script. |

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


### Installing a Hotfix / Patch

**Procedure**

1. Obtain the product update file from Trend Micro.
   - If the file is an official patch, download it from the download center.
   - If the file is a hotfix, send a request to Trend Micro support.

2. Go to **Administration > Updates > Hotfixes / Patches**.
   The **Hotfixes / Patches** screen appears.

3. Click **Select** and select the product update file.

4. Click **Upload**.
5. Click **Install**.

---

**Important**

- Some updates cannot be rolled back once installed.
- Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.

Deep Discovery Director (Consolidated Mode) installs the update and will automatically restart if it is required to complete the update.

6. Log on to the management console.

7. Go back to the **Administration > Updates** screen.

8. Verify that the hotfix / patch displays in the **History** section as the latest update.

---

### Rolling Back a Hotfix / Patch

Deep Discovery Director (Consolidated Mode) has a rollback function to undo an update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular hotfix or patch is applied.

---

**Note**

Rolling back a hotfix or patch will automatically restart Deep Discovery Director (Consolidated Mode) if it is required to complete the rollback. Verify that all tasks on the management console have been completed before rollback.

---

**Procedure**

1. Go to **Administration > Updates > Hotfixes / Patches**.

2. In the **History** section, click **Roll Back**.

   Deep Discovery Director (Consolidated Mode) will automatically restart if it is required to complete the rollback.
3. Log on to the management console.

4. Go back to the Administration > Updates > Hotfixes / Patches screen.

5. Verify that the hotfix or patch rollback is displayed as the most recent entry in the History section.

---

**Firmware**

Use the Firmware screen, in Administration > Updates > Firmware, to install a Deep Discovery Director (Consolidated Mode) upgrade. Trend Micro prepares a readme file for each upgrade. Read the accompanying readme file before installing an upgrade for feature information and for special installation instructions.

**Installing a Firmware Upgrade**

---

**Procedure**

1. Go to Administration > Updates > Firmware.

   The Firmware screen appears.

2. Click Select and select the firmware upgrade file.

3. Click Upload.

4. Click Install.

---

**Important**

- Firmware upgrades cannot be rolled back once installed.

- Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the server until upgrading is complete.

Deep Discovery Director (Consolidated Mode) will automatically restart after the upgrade is complete.
5. Log on to the management console.
6. Go back to the Administration > Updates > Firmware screen.
7. Verify that the firmware version is correct.

Integrated Products/Services

Deep Discovery Director (Consolidated Mode) integrates with other products and services:

- Microsoft Active Directory on page 8-7
- Syslog on page 8-9

Microsoft Active Directory

Use the Microsoft Active Directory screen to integrate a Microsoft Active Directory server with Deep Discovery Director (Consolidated Mode). Deep Discovery Director (Consolidated Mode) can then add Active Directory accounts to the list of accounts that can access the management console.

Configuring Microsoft Active Directory Settings

Procedure

1. Obtain the information required to configure Microsoft Active Directory integration from the server administrator.

2. Go to Administration > Integrated Products/Services > Microsoft Active Directory.

3. Select the server type that is integrating.
   - Microsoft Active Directory
4. Type the server address.

5. Select the encryption method.
   • SSL
   • STARTTLS

6. Type the port number.

---

**Note**

Trend Micro recommends using the following default ports:

- For Microsoft Active Directory:
  • SSL: 636
  • STARTTLS: 389

- For Microsoft AD Global Catalog:
  • SSL: 3269
  • STARTTLS: 3268

7. Type the base distinguished name.

8. Type the user name.

9. Type the password.

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

11. (Optional) If your organization uses a CA certificate, select **Use CA certificate** and click **Select** to locate the CA certificate file.

12. Click **Save**.
Syslog

Use the Syslog screen to configure Deep Discovery Director (Consolidated Mode) to send suspicious objects lists and Deep Discovery appliance logs to up to three syslog servers.

Adding a Syslog Server Profile

Procedure

1. Go to Administration > Integrated Products/Services > Syslog, and then click Add.
   
   The Add Syslog Server Profile dialog appears.

2. Select the status of this server profile.

3. Type a unique profile name for the syslog server.

4. Type the IP address or FQDN of the syslog server.

5. (Optional) Modify the port number.

6. Select the protocol to be used when transporting log content to the syslog server.

7. Select the scope of the data to send to the syslog server.

8. Click Save.

Note

Trend Micro recommends using the following default syslog ports:

- SSL/TLS: 6514
- TCP: 601
- UDP: 514
## Other Syslog Tasks

You can also perform the following tasks:

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a syslog server profile</td>
<td>Click on a server profile name to open the <strong>Edit Syslog Server Profile</strong> dialog and do the following:</td>
</tr>
<tr>
<td></td>
<td>• Toggle the status</td>
</tr>
<tr>
<td></td>
<td>• Modify the profile name</td>
</tr>
<tr>
<td></td>
<td>• Modify the server address</td>
</tr>
<tr>
<td></td>
<td>• Modify the port number</td>
</tr>
<tr>
<td></td>
<td>• Change the protocol</td>
</tr>
</tbody>
</table>
|                                   | **Note**  
Modifying the server address or changing the protocol resends all suspicious objects lists. |
| Delete syslog server profiles     | Select one or more syslog server profiles to delete and then click **Delete**. |
|                                   | **Note**  
Queued detection and appliance logs will be discarded and not sent to deleted syslog servers. |
| Toggle syslog server profile status | Click on the toggle in the **Status** column to enable or disable the syslog server profile. |
|                                   | **Note**  
Disabling a server profile causes queued detection and appliance logs to be discarded. |
System Settings

The System Settings screen, in Administration > System Settings, includes the following:

- **Network** on page 8-11
- **Proxy** on page 8-13
- **SMTP** on page 8-14
- **Bandwidth** on page 8-15
- **Time** on page 8-16
- **Certificate** on page 8-17
- **Session Timeout** on page 8-19

Network

Use this screen to configure the host name or fully qualified domain name, IP address, and other network settings of the Deep Discovery Director (Consolidated Mode) appliance.

Modify the IP address immediately after completing all deployment tasks.

**Note**

You can also use the Preconfiguration Console to modify the network settings.

For details, see [Configuring Network Addresses on the Preconfiguration Console on page 2-6](#).

Deep Discovery Director (Consolidated Mode) uses the specified IP address to connect to the Internet. The IP address also determines the URL used to access the management console.
Using Host Name as the Identity

Deep Discovery Director (Consolidated Mode) supports using the host name instead of the IP address as the identity of the server.

When this feature is selected, appliances connect to Deep Discovery Director (Consolidated Mode) using the host name to download files required to execute plans.

---

**Note**
The host name must be resolvable within your network.

---

**Procedure**

1. Select *Use host name instead of IP address as the identity of this server.*
2. Configure the IP address and other network settings.
3. Click *Save.*

---

Configuring Port Binding

Deep Discovery Director (Consolidated Mode) supports the binding of services to a second network port.

When this feature is selected, Deep Discovery Director (Consolidated Mode) directs all connections to the threat intelligence feeds, the license update server, and Active Update servers through eth1.

---

**Note**
This feature cannot be configured from the Preconfiguration Console.

---

**Procedure**

1. Select *eth0 (management) and eth1* to bind your services to.
**Important**

This feature requires at least two network interface cards to be installed and configured. The feature will be hidden from the **Network** screen otherwise.

A new eth1 section to configure network settings for the second network port displays under the existing eth0 (management) section.

2. Configure the IP address and other network settings of the second network port.

3. Click **Save**.

---

**Using IPv4 and IPv6 Dual Stack**

Deep Discovery Director (Consolidated Mode) supports IPv4 and IPv6 dual-stack configuration to function in network environments that communicate using the IPv6 protocol.

**Procedure**

1. Select **IPv4 and IPv6 (dual stack)** as **Type**.

   A new section to configure IPv6 settings displays between the existing IPv4 and DNS settings.

2. Configure the IPv6 settings.

3. Click **Save**.

---

**Proxy**

Deep Discovery Director (Consolidated Mode) can be configured to use a proxy server to connect to threat intelligence feeds, the license update server, and Active Update servers.
**Note**

When port binding is configured, only eth1 will use the proxy settings.

**Procedure**

1. Go to **Administration > System Settings > Proxy**.
   
The **Proxy** screen appears.

2. Select **Use a proxy server to connect to the Internet**.

3. Select the protocol to use for proxying.
   
   - **HTTP**
   - **SOCKS4**
   - **SOCKS5**

4. Type the IPv4 address or FQDN of the proxy server.

5. Type the port number. The default port number is **80**.

6. (Optional) If you selected **HTTP** or **SOCKS5** as protocol, and your proxy server requires authentication, select **Specify authentication credentials**, and then type the user name and password used for authentication.

7. (Optional) Click **Test Connection** to verify the connection to the proxy server.

8. Click **Save**.

---

**SMTP**

Use the **SMTP** screen, in **Administration > System Settings > SMTP**, to enable using a SMTP server to send alert notifications through email.

**Procedure**

1. Go to **Administration > System Settings > SMTP**.
The **SMTP** screen appears.

2. Select **Use a SMTP server**.

3. Type the IPv4 address or FQDN of the SMTP server.

4. Select the security protocol to use for connections to the SMTP server.

5. (Optional) Modify the port number.

6. Type a sender email address.

7. (Optional) If the SMTP server requires authentication, select **SMTP server requires authentication**, and then type the user name and password used for authentication.

---

**WARNING!**

Verify that the user name and password are valid. Connections made using an incorrect user name and password may cause some SMTP servers to reject all network request originating from Deep Discovery Director (Consolidated Mode).

---

8. (Optional) Verify that Deep Discovery Director (Consolidated Mode) can communicate with the specified SMTP server and send emails.

   a. Click **Send Test Message**.

      The **Send Test Message** dialog appears.

   b. Type at least one valid email address, and then click **Send**.

      If Deep Discovery Director (Consolidated Mode) can communicate with the specified SMTP server, an email with the predefined subject and message will be sent to the specified email addresses.

   c. Check your email account for receipt of the email.

---

**Bandwidth**

Use the **Bandwidth** screen, in **Administration > System Settings > Bandwidth**, to enable bandwidth usage throttling settings. Bandwidth usage throttling helps manage the
impact downloading and uploading of files may have on your network and internet connection.

For details, see *Configuring Bandwidth Usage Throttling on page 8-16*.

**Configuring Bandwidth Usage Throttling**

**Procedure**

1. Go to Administration > System Settings > Bandwidth.
   
   The Bandwidth screen appears.

2. Select Enable bandwidth usage throttling.

3. Type a speed limit value to limit the speed per connection for downloading files from Deep Discovery Director (Consolidated Mode) to the appliance. Each appliance establishes one connection.

4. Type a maximum value to limit the number of connections to.

5. Click Save.

**Time**

Configure date and time settings immediately after installation.

**Procedure**

1. Go to Administration > System Settings > Time.
   
   The Time screen appears.

2. Select one of the following methods and configure the applicable settings.
   
   - Select **Connect to an NTP server** and type the FQDN or IP address of the NTP server.
   
   - Select **Set manually** and configure the time.
3. Select the applicable time zone.

   **Note**
   Daylight Saving Time (DST) is used when applicable.

4. Select the preferred date and time format.

5. Click **Save**.

---

**Certificate**

Digital certificates are electronic documents that are used to create secure connections between clients and servers or websites. A valid and trusted certificate ensures clients that they are connecting to a trusted server or website, and helps protect against man-in-the-middle attacks.

Certificates become trusted by going through a validation process of a Certificate Authority (CA). Certificate Authorities themselves are usually third-party companies that are trusted by both the client and server or website.

On first installation, Deep Discovery Director (Consolidated Mode) creates a self-signed SSL certificate that will be used to securely communicate with other Deep Discovery appliances and Local Repository. In doing so, Deep Discovery Director (Consolidated Mode) also acts as its own CA.

Users who wish to adopt their own organizations' CA can import a certificate signed by that CA to Deep Discovery Director (Consolidated Mode).
Important

Accessing the management console of a Deep Discovery Director (Consolidated Mode) server with an untrusted or expired certificate displays a security warning in the web browser.

An untrusted or expired certificate does not affect the communication between Deep Discovery Director (Consolidated Mode) servers and Deep Discovery appliances. Deep Discovery Director (Consolidated Mode) servers with untrusted or expired certificates can still deploy plans to Deep Discovery appliances, and appliances can still download the files required to execute the plans from those servers.

Importing a Certificate

Deep Discovery Director (Consolidated Mode) uses a certificate to create secure connections to clients. Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.

WARNING!

- Verify that your web browser accepts the new certificate before importing it. Importing a certificate that is not accepted by your web browser will leave you unable to access the management console.
- Importing the certificate will restart the service. Existing connections to repositories and Deep Discovery appliances will be interrupted, and clients will have to trust the new fingerprint to restore the connection.

Procedure

1. Go to Administration > System Settings > Certificate.

   The Certificate screen appears.

2. Click Import, select the certificate, and then click Open.

   The certificate will be imported immediately.
Session Timeout

Select the time period after which users are logged out due to inactivity. The default value is 15 minutes.

Account Management

Deep Discovery Director (Consolidated Mode) uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks.

Each account is assigned a specific role. A role defines the level of access to the management console.

Accounts

Use the Accounts screen, in Administration > Account Management > Accounts, to create and manage user accounts. Users can use these accounts, instead of the default administrator account, to access the management console.

Deep Discovery Director (Consolidated Mode) supports the creation of user accounts by using the following methods:

• Adding a Local User Account on page 8-20
• Adding an Active Directory User Account or Group on page 8-20

Note

This method is only available if Microsoft Active Directory settings have been configured.

For details, see Microsoft Active Directory on page 8-7.
Adding a Local User Account

Procedure

1. Go to Administration > Account Management > Accounts, and then click Add.
   The Add Account screen appears.
2. Toggle the Status of this account.
3. Select Local user as the Type of this account.
4. Type a valid user name.
5. Type a valid password.
6. Type the password again to confirm it.

   Tip
   Click the Show password icon to unmask the password and skip this step.

7. (Optional) Type a valid email address that can be used to receive alerts sent by Deep Discovery Director (Consolidated Mode).
8. Select a Role for this account. The role determines the level of access this account has.
   For details, see Roles on page 8-24.
9. (Optional) Type a description for this account.
10. Click Save.

Adding an Active Directory User Account or Group

If your company uses Microsoft Active Directory to manage user accounts and groups, you can enable those user accounts and groups access to Deep Discovery Director (Consolidated Mode).
Note

• Microsoft Active Directory settings have to be configured before an Active Directory user account or group can be added.

For details, see *Microsoft Active Directory on page 8-7.*

• Deep Discovery Director (Consolidated Mode) syncs Microsoft Active Directory user accounts and groups every 24 hours. User accounts or groups that are removed from the Active Directory server will be removed from Deep Discovery Director (Consolidated Mode) after syncing with the Active Directory server.

• If a Microsoft Active Directory user is a member of one or more groups, the user's level of access in Deep Discovery Director (Consolidated Mode) is determined by the highest level of access granted to the user's Deep Discovery Director (Consolidated Mode) account or any group the user is a member of.

Procedure

1. Go to **Administration > Account Management > Accounts**, and then click **Add**.

   The **Add Account** screen appears.

2. Toggle the **Status** of this account.

3. Select **Active Directory user or group** as the **Type** of this account.

4. Type a user or group name and click **Search** to search the Active Directory for matching user accounts or groups.

   Matching user accounts and groups are displayed in the results table.

5. Select the Active Directory user account or group to add.
6. Select a **Role** for this account. The role determines the level of access this account has.

   For details, see *Roles on page 8-24*.

7. (Optional) Type a description for this account.

8. Click **Save**.

---

**Other Accounts Tasks**

You can also perform the following tasks:
### TABLE 8-2. Other Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit account</td>
<td>Click on a user name to open the <strong>Edit Account</strong> screen and do the following:</td>
</tr>
<tr>
<td></td>
<td>• Toggle the account status</td>
</tr>
<tr>
<td></td>
<td>• Change the password</td>
</tr>
<tr>
<td></td>
<td>• Change the email address</td>
</tr>
<tr>
<td></td>
<td>• Change the role</td>
</tr>
<tr>
<td></td>
<td>• Modify the description</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• The passwords and email addresses of Microsoft Active Directory accounts cannot be changed from the management console.</td>
</tr>
<tr>
<td></td>
<td>• Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.</td>
</tr>
<tr>
<td></td>
<td>• Users who are currently logged on to the management console and whose roles are changed will be logged off automatically.</td>
</tr>
<tr>
<td>Delete account</td>
<td>Select one or more user accounts to delete and then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• There must be at least one local user account using the built-in administrator role.</td>
</tr>
<tr>
<td></td>
<td>• You cannot delete the logged-on account.</td>
</tr>
<tr>
<td></td>
<td>• Users who are currently logged on to the management console will be logged off automatically.</td>
</tr>
</tbody>
</table>
Deep Discovery Director (Consolidated Mode) includes a security feature that locks an account in case the user typed an incorrect password three times in a row. This feature cannot be disabled. Accounts locked this way, even administrator accounts, unlock automatically after ten minutes.

**Note**

Microsoft Active Directory accounts are never locked.

**View account lock status**

Click on the toggle in the **Status** column to enable or disable the user account.

**Note**

- At least one local user account using the built-in administrator role must be enabled.
- Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.

### Roles

Use the **Roles** screen, in **Administration > Account Management > Roles**, to create and manage user roles. Assign each user a role that will restrict their activities to all but those necessary for the completion of their duties.

Deep Discovery Director (Consolidated Mode) comes with a set of built-in user roles that you cannot delete:

<table>
<thead>
<tr>
<th>ROLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Built-in Administrator role with full access to all management console features</td>
</tr>
<tr>
<td>ROLE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Investigator</td>
<td>Built-in Investigator role with read-only access to all management console features, but download access to investigation package and pcap data</td>
</tr>
<tr>
<td>Operator</td>
<td>Built-in Operator role with read-only access to all management console features</td>
</tr>
</tbody>
</table>

Deep Discovery Director (Consolidated Mode) also supports custom user roles. Create new roles to limit access to the management console, and to restrict users from seeing and managing specific appliances.

**Adding a Role**

**Procedure**

1. Go to Administration > Account Management > Roles, and then click Add.
   
   The Add Role screen appears.

2. Type a role name.

3. Select a **Permission** for this role.

4. Select the appliances this role can see and manage.

5. Select the domains from which email message detections should be displayed.

   **Note**
   
   To specify domains, you have to add them first. For details, see *Managing Domains on page 8-26*.

6. Select an account, or type to search and press ENTER, and then click **Add** to add the selected account to this rule.

   **Note**
   
   Added accounts will be removed from all other roles.
7. (Optional) Type a description for this role.
8. Click Save.

Managing Domains

In addition to finely controlling which appliances a role can see and manage, the integration with Deep Discovery Email Inspector calls for control over which email messages a role can see. To address this requirement, Deep Discovery Director (Consolidated Mode) provides users with the control to separate email messages by using domains.

Procedure

1. Go to Administration > Account Management > Roles.

   The Roles screen appears.

2. Do one of the following:
   • Click Add to open the Add Role screen.
   • Click on a role name to open the Edit Role screen.

3. In the Domain access section, click on Domain management.

   The Domain Management dialog appears.

4. Type a domain in the left text box and click Add to add the domain to the list.

   Note
   One wildcard (*) connected with a "." in the domain prefix is supported.

5. Select one or more domains from the list and click Delete to delete the selected domains.

6. (Optional) To search for a domain, type a keyword in the right search text box, and then press ENTER or click the magnifying glass icon.
7. Click Close.

Other Roles Tasks

You can also perform the following tasks:

**TABLE 8-3. Other Tasks**

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Edit role  | Click on a role name to open the *Edit Role* screen and do the following:  
  • Modify the role name  
  • Change the permission  
  • Modify the appliances this role can see and manage  
  • Add accounts to this role  
  • Modify the description |

**Note**

- You cannot modify the role name, permission, appliance access rights, and description of built-in roles.
- Users who are currently logged on to the management console and whose appliance access rights are modified will be logged off automatically.
- Users who are currently logged on to the management console and whose roles are changed will be logged off automatically.
### Task Description

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete role</td>
<td>Select one or more user roles to delete and then click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

**Note**
- You cannot delete built-in roles.
- You cannot delete roles that are in use by at least one account.

### System Logs

Use the **System Logs** screen, under **Administration > System Logs**, to view, query and export system logs.

Deep Discovery Director (Consolidated Mode) maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.

Deep Discovery Director (Consolidated Mode) stores system logs in the appliance hard drive.

Query system logs to gather information from the database. The queried system logs can be exported in CSV format for offline viewing.

For details, see *Querying System Logs on page 8-30*.

The following table lists all system-log-related information:

**TABLE 8-4. System Log Information**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged</td>
<td>Event date and time</td>
</tr>
<tr>
<td><strong>COLUMN</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event identifier&lt;br&gt;Each specific action has its own event ID. Examples:&lt;br&gt;• 20001&lt;br&gt;<strong>Description:</strong> User logged on&lt;br&gt;• 20002&lt;br&gt;<strong>Description:</strong> User logged off</td>
</tr>
<tr>
<td>Type</td>
<td>One of the following types displays:&lt;br&gt;• Account Logon/Logoff&lt;br&gt;• External Web Services&lt;br&gt;• System&lt;br&gt;• TMCM Integration&lt;br&gt;• Update</td>
</tr>
<tr>
<td>Level</td>
<td>One of the following levels displays:&lt;br&gt;• Informational&lt;br&gt;• Warning&lt;br&gt;• Error</td>
</tr>
<tr>
<td>Result</td>
<td>One of the following results displays:&lt;br&gt;• Successful&lt;br&gt;• Unsuccessful</td>
</tr>
<tr>
<td>Source</td>
<td>Activity by source&lt;br&gt;Information about the following sources may display:&lt;br&gt;• user name&lt;br&gt;<strong>Example:</strong> johnadmin&lt;br&gt;• system&lt;br&gt;<strong>Example:</strong> SYSTEM</td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>IP Address</td>
<td>Event IP address</td>
</tr>
<tr>
<td>Description</td>
<td>Event details</td>
</tr>
</tbody>
</table>

**Querying System Logs**

The task of finding a specific system log entry can be difficult when there may be hundreds or thousands to go through. Use the filters and search box to lower the number of entries shown.

**Procedure**

1. Go to **Administration > System Logs**.
   
   The **System Logs** screen appears.

2. Click the **Filters** button.
   
   Filter drop-down lists and a search box appear.

3. Select a log type.
   
   - All types
   - Account Logon/Logoff
   - System
   - Update
   
   The screen is updated immediately.

4. Select a log level.
   
   - All levels
   - Error
   - Warning
• **Informational**

  The screen is updated immediately.

5. Select a log result.

  • **All results**
  
  • **Successful**
  
  • **Unsuccessful**

  The screen is updated immediately.

6. Select a period or specify a custom period using the calendar and clock.

  The screen is updated immediately.

7. Type a event ID, source, or description keyword in the search box and press ENTER to only display system logs whose event ID, source, or description contain the keyword.

8. Click **Export** to export the currently filtered system logs.

  The **Export** dialog displays.

9. Confirm the system log filters and select a delimiter to use.

  • **Comma**
  
  • **Semicolon**
  
  • **Space**
  
  • **Tab**

10. Click **OK** to export and download the currently filtered system logs to a CSV file with the chosen delimiter.

---

**Note**

The exported system logs are ordered by **Log ID**, a consecutive number that coincides with the **Logged** date and time.
System Maintenance

The System Maintenance screen, in Administration > System Maintenance, includes the following tabs:

- System Status on page 8-32
- Storage on page 8-32
- Back Up on page 8-34
- Restore on page 8-37
- Power Off / Restart on page 8-42

System Status

The System Status screen displays the utilization of key hardware components.

Storage

Use the Storage screen, in Administration > System Maintenance > Storage, to configure how long Deep Discovery Director (Consolidated Mode) saves database entries, system logs, and detection logs, and to configure disk usage.

Under Database Storage, configure the following:

- **Delete database entries older than X days**: Type the number of days to save database entries. Entries older than the specified value are automatically deleted.

  Tip
  A database entry in this context refers to a Deep Discovery Director (Consolidated Mode) plan.

- **Delete system logs older than X days**: Type the number of days to save system logs. Logs older than the specified value are automatically deleted.
• **Delete detection and appliance related logs older than X days:** Type the number of days to save detection logs. Logs older than the specified value are automatically deleted.

---

**Tip**

- **Detection logs** in this context refers to Deep Discovery Inspector and Deep Discovery Email Inspector related detection details.
- **Appliance logs** in this context refers to Deep Discovery appliance logs such as Email Message Tracking and MTA logs.

---

**Note**

In addition to the settings above, Deep Discovery Director (Consolidated Mode) automatically purges system logs until there is 200 MB free database disk space. This threshold cannot be modified.

The **Disk Usage** section displays information about the usage and total size of partitions. Any available space can be added to the any of the partitions. New disks can be added to further increase partition size.

### Configuring Disk Space

Add extra available disk space to Deep Discovery Director (Consolidated Mode) partitions to increase the number of logs or repository files that can be stored.

#### Procedure

1. Go to **Administration > System Maintenance > Storage**, and click **Configure space**.

   The **Disk Space Configuration** dialog appears.

2. (Optional) To add more disks to Deep Discovery Director (Consolidated Mode), do the following:
   a. Click **Add disks**.

   The disk selection dialog displays.
b. Select at least one disk to add to the Deep Discovery Director (Consolidated Mode) disk space configuration.

---

**Important**

Only unformatted disks that are larger than 1024 MB in size are displayed.

---

c. Click **Add**.

---

**WARNING!**

Disks cannot be removed after they are added.

The selected disks are formatted and available disk space is added to the **Disk Space Configuration** dialog.

3. To add available space to a partition, do one of the following:

   • Select **Add all available space to this partition**

   • Type values into the **Add** fields.

---

**Note**

   • The **Available space** and **Total** values are automatically updated.

   • It is not required to distribute all available space among the partitions.

---

4. Click **Apply**.

   Available space is added to the partitions as specified.

---

**Back Up**

Use the **Back Up** screen, in **Administration > System Maintenance > Back Up**, to export a backup file of most of the configuration settings and the database, and to configure automatic backups of those.

---

• **Exporting a Configuration Settings and Database Backup on page 8-36**
- **Configuring Automatic Backups on page 8-37**

The following table shows the screens and elements with backed up configuration settings.

**TABLE 8-5. Backed Up Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intelligence &gt; Product Intelligence</td>
<td>Synchronized Suspicious Objects</td>
</tr>
<tr>
<td></td>
<td>C&amp;C Callback Addresses</td>
</tr>
<tr>
<td>Threat Intelligence &gt; Custom Intelligence</td>
<td>YARA Rules</td>
</tr>
<tr>
<td></td>
<td>STIX</td>
</tr>
<tr>
<td></td>
<td>User-Defined Suspicious Objects</td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
</tr>
<tr>
<td>Threat Intelligence &gt; Feed Management</td>
<td>All settings</td>
</tr>
<tr>
<td>Threat Intelligence &gt; Sharing Settings</td>
<td>TAXII</td>
</tr>
<tr>
<td></td>
<td>Web Service</td>
</tr>
<tr>
<td></td>
<td>Auxiliary Products/ Services</td>
</tr>
<tr>
<td>Appliances &gt; Directory</td>
<td>Appliance tree with group structure</td>
</tr>
<tr>
<td></td>
<td>Registered appliances and appliance details</td>
</tr>
<tr>
<td>Appliances &gt; Plans</td>
<td>All plans</td>
</tr>
<tr>
<td>Alerts</td>
<td>Triggered Alerts</td>
</tr>
<tr>
<td></td>
<td>Built-in Rules</td>
</tr>
<tr>
<td></td>
<td>Custom Rules</td>
</tr>
</tbody>
</table>
Exporting a Configuration Settings and Database Backup

Deep Discovery Director (Consolidated Mode) can export a backup file of most configuration settings and the database. Use the backup file to restore Deep Discovery Director (Consolidated Mode) to a previous point in time. Use the backup file on another server, when the active server is unresponsive and cannot be restored, to restore operation and minimize downtime.

Procedure

1. Go to Administration > System Maintenance > Back Up.

   The Back Up screen appears.
2. Under **Configuration Settings and Database Backup**, click **Export**.
   The active server exports a backup file with the configuration settings and database. For details, see *Back Up on page 8-34*.
3. Download and save the backup file.

---

**Configuring Automatic Backups**

Deep Discovery Director (Consolidated Mode) can be configured to create and upload automatic backups of its configuration settings and database to a SFTP server of your choice. Deep Discovery Director (Consolidated Mode) creates up to five backup files, after which the oldest one is deleted in order to keep the number of backup files at five.

**Procedure**

1. Go to **Administration > System Maintenance > Back Up**.
   The **Back Up** screen appears.
2. Under **Automatic Backups**, select **Automatically back up to SFTP server**.
3. Type the IP address or FQDN of the SFTP server.
4. Type the port number. The default port number is 22.
5. Type the folder path to use on the SFTP server.
6. Type the user name and password used to log on to the SFTP server.
7. Specify a backup frequency using the drop-down lists and the clock tool.
8. Click **Save**.

---

**Restore**

Use the **Restore** screen, in **Administration > System Maintenance > Restore**, to restore configuration settings and database from a backup file. If the active Deep Discovery Director (Consolidated Mode) server is unresponsive or cannot be restored, a
configuration settings and database backup can also be used on another server to restore operation and minimize downtime.

- Restoring a Configuration Settings and Database Backup on page 8-38
- Replacing the Active Server with Another Server on page 8-39

---

**Note**

For more information on exporting a configuration settings and database backup, see Exporting a Configuration Settings and Database Backup on page 8-36.

---

**Restoring a Configuration Settings and Database Backup**

A configuration settings and database backup can be used to restore Deep Discovery Director (Consolidated Mode) to a previous point in time.

If the active Deep Discovery Director (Consolidated Mode) is unresponsive or cannot be restored, a configuration settings and database backup can also be used on another server to restore operation and minimize downtime.

For details, see Replacing the Active Server with Another Server on page 8-39.

---

**Procedure**

1. Go to Administration > System Maintenance > Restore.

   The Restore screen appears.

2. Click Select File... and select the backup file.

3. Click Upload.

   The backup file is uploaded, and Deep Discovery Director (Consolidated Mode) displays information about the backup file.

4. Click Restore.

   Deep Discovery Director (Consolidated Mode) displays a confirmation message.

5. Click OK.
Deep Discovery Director (Consolidated Mode) restores configuration settings and database from the backup file, and then restarts the server.

6. (Optional) Restore the repository by re-uploading all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

**Important**

Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.

7. (Optional) Configure the network addresses. For details, see Network on page 8-11.

8. (Optional) Activate Deep Discovery Director (Consolidated Mode). For details, see License on page 8-42.

The server is now ready to resume operation.

---

### Replacing the Active Server with Another Server

If the Deep Discovery Director (Consolidated Mode) server is unresponsive or cannot be restored, it can be replaced by another server.

The following table lists requirements that need to be fulfilled by the replacement server. For details, see System Requirements on page 2-2.

**TABLE 8-6. Replacement Server Requirements**

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host machine hardware</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>Host machine software</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>Deep Discovery Director (Consolidated Mode)</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>deployment type</td>
<td></td>
</tr>
<tr>
<td>Deep Discovery Director (Consolidated Mode)</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>version and build</td>
<td></td>
</tr>
</tbody>
</table>
Procedure

1. Back up the configuration settings and database of the active server.
   a. On the management console of the active server, go to Administration > System Maintenance > Back Up.
   b. Under Configuration Settings and Database Backup, click Export.
      The active server exports a backup file with the configuration settings and database. For details, see Back Up on page 8-34.
   c. Download and save the backup file.

2. Install Deep Discovery Director (Consolidated Mode) on the replacement server.
   For details, see Installing Deep Discovery Director on page 2-4.

3. Configure temporary network addresses for the replacement server.
   For details, see Configuring Network Addresses on the Preconfiguration Console on page 2-6.

   **Important**
   Verify that the temporary network addresses are different from the network addresses of the active server to avoid IP addressing conflicts.

4. Log on to the management console of the replacement server.

5. Restore the configuration settings and database on the replacement server.
   a. On the management console of the replacement server, go to Administration > System Maintenance > Restore.
   b. Click Select File... and select the backup file.
   c. Click Upload.
      The backup file is uploaded, and Deep Discovery Director (Consolidated Mode) displays information about the backup file.
   d. Click Restore.
Deep Discovery Director (Consolidated Mode) displays a confirmation message.

e. Click **OK**.

Deep Discovery Director (Consolidated Mode) restores configuration settings and database from the backup file, and then restarts the server.

6. Restore the repository by re-uploading all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

---

**Important**

Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.

---

7. Power off the active server.

   a. On the management console of the active server, go to **Administration > System Maintenance > Power Off / Restart**.

   b. Click **Power Off**.

   The active server stops all services and gracefully shuts down.

---

**WARNING!**

The replacement server will be configured to use the network addresses of the active server. Leaving the active server powered on will cause IP addressing conflicts.

---

8. Configure the replacement server to use the network addresses of the active server. For details, see **Network on page 8-11**.

9. Activate Deep Discovery Director (Consolidated Mode). For details, see **License on page 8-42**.

   The replacement server is now ready to resume operation as the new active server.
Power Off / Restart

Use the Power Off / Restart screen, in Administration > Power Off / Restart, to power off or restart the server.

- **Power Off**: All active tasks are stopped, and then the server gracefully shuts down.
- **Restart**: All active tasks are stopped, and then the server is restarted.

Integrated products may queue data while the server is unavailable.

License

Use the License screen, in Administration > License, to view, activate, and renew the Deep Discovery Director (Consolidated Mode) license.

The License screen includes the following information and options.
### Table 8-7. License Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays either <strong>Activated</strong>, <strong>Not Activated</strong>, or <strong>Expired</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director (Consolidated Mode) does not allow the creation of new plans when the license status is <strong>Not Activated</strong> or <strong>Expired</strong>. Existing plans will deploy and execute as usual.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>View details</strong> to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated in the screen, click <strong>Refresh</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If proxy settings are enabled, Deep Discovery Director (Consolidated Mode) connects to the license update server using the proxy server.</td>
</tr>
<tr>
<td>Type</td>
<td>• <strong>Full</strong>: Provides access to all product features</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trial</strong>: Provides access to all product features</td>
</tr>
<tr>
<td>Expiration date</td>
<td>View the expiration date of the license. Renew the license before it expires. Click <strong>View renewal instructions</strong> to view instructions from the Trend Micro website.</td>
</tr>
</tbody>
</table>
### Field Details

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click <strong>New Activation Code</strong>, and type the new Activation Code. The <strong>License</strong> screen reappears displaying the number of days left before the product expires.</td>
</tr>
</tbody>
</table>

**Tip**

Deep Discovery Director (Consolidated Mode) can be activated with the Activation Code of any Deep Discovery product.
Technical Support

Learn about the following topics:

• Troubleshooting Resources on page 9-2
• Contacting Trend Micro on page 9-3
• Sending Suspicious Content to Trend Micro on page 9-4
• Other Resources on page 9-5
Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

Tip

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


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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia
provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

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

Contacting Trend Micro

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

| Address | Trend Micro, Incorporated  
225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A. |
|---------|--------------------------|
| Phone   | Phone: +1 (817) 569-8900  
Toll-free: (888) 762-8736 |
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

• Worldwide support offices:


• Trend Micro product documentation:

  http://docs.trendmicro.com
Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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 stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

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

http://www.trendmicro.com/download/

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

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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