



3.0 TREND MICRO™ Deep Discovery™ Director – Network Analytics

Service Pack 1
Installation and Deployment Guide



Network Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com/en-us/home.aspx/>

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, and Deep Discovery are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2018. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM38514/181030

Release Date: November 2018

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

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

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

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that Trend Micro Deep Discovery Director - Network Analytics collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

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

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Preface	v
Documentation	vi
Audience	vi
Document Conventions	vii
About Trend Micro	viii

Chapter 1: Introduction

Overview of Deep Discovery Director - Network Analytics	1-2
---	-----

Chapter 2: Deployment

Deployment Overview of Integrated Solution	2-2
Pre-deployment Checklist	2-2
System Requirements	2-4
Deep Discovery Director IP Address/API Key	2-5
Installation	2-6
Initial Setup Using the Preconfiguration Console	2-7
Registering to Deep Discovery Director	2-9
Moving the Appliance to a Managed Group	2-10

Chapter 3: Getting Started

Accessing the Settings Screen	3-3
Activating Your Product License	3-3
Registering to Deep Discovery Inspector	3-4
Adding as a Syslog Server	3-5

Configuring Settings	3-8
Configuring the Domain Exception List	3-9
Configuring the Priority Watch List	3-10
Configuring the Registered Services Lists	3-10
Configuring the Trusted Internal Networks List	3-12
Configuring SMTP Settings	3-12
(Optional) Modifying Network Settings	3-14
(Optional) Configuring Proxy Settings	3-15
Configuring Time Zone and NTP Settings	3-16
Configuring Alert Settings	3-17
Configuring Storage Retention Settings	3-19
(Optional) Configuring Disk Space	3-20
Configuring Automatic Backups	3-21
Performing Additional Tasks	3-22
Viewing Triggered Alerts	3-23
Viewing Your Product License	3-23

Chapter 4: Using Correlation Data for Advanced Threat Analysis

Viewing Correlation Data	4-2
Supported Protocols	4-2
Viewing Correlation Data from Correlated Events	4-3
Viewing Correlation Data for Suspicious Objects	4-4
Analyzing Correlation Data Information	4-6
Overview of the Correlation Data Screen	4-6
Reviewing the Correlation Data Summary	4-8
Analysis Using the Correlation Data Graph	4-10
Analysis Using Transaction Data	4-15
Configuring Incident Report Email Notifications	4-16

Chapter 5: Updating Deep Discovery Director - Network Analytics

Hotfixes and Patches Overview	5-2
Uploading a Hotfix / Critical Patch / Firmware File	5-2

Adding a Hotfix / Critical Patch / Firmware Deployment Plan	5-4
Synchronizing Modifications	5-5

Chapter 6: Backing Up or Restoring a Configuration

Settings That Are Backed Up or Restored	6-3
Manually Exporting a Backup	6-4
Configuring Automatic Backups	6-4
Restoring from Backup	6-5

Chapter 7: Technical Support

Troubleshooting Resources	7-2
Using the Support Portal	7-2
Threat Encyclopedia	7-2
Contacting Trend Micro	7-3
Speeding Up the Support Call	7-4
Sending Suspicious Content to Trend Micro	7-4
Email Reputation Services	7-4
File Reputation Services	7-5
Web Reputation Services	7-5
Other Resources	7-5
Download Center	7-5
Documentation Feedback	7-6

Index

Index	IN-1
-------------	------

Preface

Preface

Topics include:

- *Documentation on page vi*
- *Audience on page vi*
- *Document Conventions on page vii*
- *About Trend Micro on page viii*

Documentation

The documentation set for Deep Discovery Director - Network Analytics includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide discusses requirements and procedures for installing and deploying Deep Discovery Director - Network Analytics.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

Deep Discovery Director - Network Analytics provides an integrated solution that utilizes Deep Discovery Director and Deep Discovery Inspector. You can view and download documentation for all these products from the Trend Micro Documentation Center:

<http://docs.trendmicro.com/en-us/home.aspx/>

Audience

The Deep Discovery Director - Network Analytics documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:




- Network topologies
- Policy management and enforcement


The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations

CONVENTION	DESCRIPTION
 WARNING!	Critical actions and configuration options

About Trend Micro

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

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

<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

- *Overview of Deep Discovery Director - Network Analytics on page 1-2*

Overview of Deep Discovery Director - Network Analytics

Trend Micro Deep Discovery Director - Network Analytics provides advanced threat analysis on historical network data based on Deep Discovery Inspector network detections, and other related events as they occur over time. Designed to be integrated into your existing network topology, it is a transparent solution that integrates with Deep Discovery Director and Deep Discovery Inspector to provide advanced protection against cyber threats and attacks that could threaten your network.

Chapter 2

Deployment

This chapter contains information about the requirements and procedures for deploying Deep Discovery Director - Network Analytics.

- *Deployment Overview of Integrated Solution on page 2-2*
- *Pre-deployment Checklist on page 2-2*
- *System Requirements on page 2-4*
- *Deep Discovery Director IP Address/ API Key on page 2-5*
- *Installation on page 2-6*
- *Initial Setup Using the Preconfiguration Console on page 2-7*
- *Registering to Deep Discovery Director on page 2-9*
- *Moving the Appliance to a Managed Group on page 2-10*

Deployment Overview of Integrated Solution

Deep Discovery Director - Network Analytics is part of an integrated solution that provides advanced threat analysis by correlating threat events over time and identifying how the threat started and advanced in your network.

Three Trend Micro products are required in the integrated solution:

- Deep Discovery Director - Network Analytics (the appliance)
Provides correlation data and advanced threat analysis about threats detected by Deep Discovery Inspector.
- Deep Discovery Inspector
Provides network meta data and the detection logs that the appliance uses to make data correlations and advanced threat analysis.
- Deep Discovery Director
 - Provides management for the appliance.
 - Provides access to Deep Discovery Director - Network Analytics correlation data and to the appliance's configuration settings screen.

Pre-deployment Checklist

The Deep Discovery Director - Network Analytics advanced threat analysis solution is an integrated solution that utilizes Deep Discovery Director and Deep Discovery Inspector.

The following must be done before deploying Deep Discovery Director - Network Analytics (the appliance):


- Deep Discovery Director and Deep Discovery Inspector must be deployed.
- Deep Discovery Inspector must be registered to Deep Discovery Director.

TABLE 2-1. Pre-deployment Checklist

REQUIREMENT	DETAILS
Deep Discovery Director 3.0 or later	Provides management and access.
Deep Discovery Inspector 5.1 or later	Provides network meta data and syslogs used for correlation and advanced analysis.
Deep Discovery Director - Network Analytics Activation Code	Obtain from Trend Micro.
IP addresses	You must obtain one static IPv4 address for the network interface.
DNS server IP addresses	You must enter one DNS server IP address during initial deployment. You can enter up to three DNS server addresses.
NTP server IP addresses or FQDNs	You must use NTP to configure time on the Deep Discovery Director - Network Analytics appliance. You can enter up to four NTP server addresses.
Monitor and VGA cable	Connects to the VGA port of the appliance.
USB keyboard	Connects to a USB port of the appliance.
Ethernet cable	Connects to the management port.
Internet-enabled computer	<p>You can access the preconfiguration management console from a computer with one of the following supported web browsers:</p> <ul style="list-style-type: none"> • Mozilla® Firefox® latest version • Google Chrome™ latest version • Microsoft Internet Explorer™ latest version

System Requirements

TABLE 2-2. System Requirements

REQUIREMENT	RECOMMENDED SPECIFICATIONS
Hardware	<ul style="list-style-type: none"> • Network interface card: 1 Gbps port • SCSI Controller: LSI Logic Parallel • CPU: 1.8 GHz (8-12 cores) • Memory: 64 GB • Hard disk: 6 TB (thick provisioned) <hr/> <p> Note</p> <p>With this configuration and a typical enterprise level of network traffic, the Deep Discovery Director - Network Analytics appliance can service:</p> <ul style="list-style-type: none"> • Up to 4 DDI-1000 devices • Up to 1 DDI-4K device <p>With this storage capacity, the amount of time for which network data can be retained, and hence correlation will be available is:</p> <ul style="list-style-type: none"> • For 1 DDI-1000 device: 4-6 months • For 1 DDI-4K device: 40-45 days
Software	<ul style="list-style-type: none"> • Hypervisor: VMware vSphere ESXi 6.5 or Microsoft Hyper-V in Windows Server 2016 • Deep Discovery Director - Network Analytics is an appliance based on CentOS Linux 7 (64-bit)

REQUIREMENT	RECOMMENDED SPECIFICATIONS
Ports	<p>Inbound ports:</p> <ul style="list-style-type: none">• TCP 443 (Deep Discovery Director server and Deep Discovery Inspector connection)• TCP 514 (Deep Discovery Inspector detection logs) <p>Outbound ports:</p> <ul style="list-style-type: none">• TCP 443 and 80 (Deep Discovery Director server and Deep Discovery Inspector connection)• UDP 123 (default NTP server connection)

Deep Discovery Director IP Address/API Key

You must enter the Deep Discovery Director server's IP address and API Key on the Deep Discovery Director - Network Analytics appliance during the deployment procedure. You can use this procedure to record this information for later use.

Procedure

1. Log on to the Deep Discovery Director console.
 2. Record the IPv4 address that you used to log on to the Deep Discovery Director console.
 3. Go to **Help**.
The API key is displayed under the **Product Information** section.
 4. Record the API key or leave this page open to use when performing the deployment.
-

Installation

To install Deep Discovery Director - Network Analytics (the appliance), you must first create a virtual machine with the specifications outlined below. You can then use the ISO image supplied by Trend Micro to install the appliance.

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)
 - CPU: 2-3 (8-12 cores)
 - Memory: 64 GB
 - Network interface card: 1 with 1 Gbps adapter
 - SCSI Controller: LSI Logic Parallel
 - Hard disk: 6 TB (Thick Provisioned Lazy Zeroed)
 - Configure the CD/DVD or Floppy drive device to connect at power on with the appliance's ISO image file selected.

The new virtual machine displays in the left-hand pane.

2. Select and then power on the new virtual machine.

The appliance's installation starts automatically with power on. The **INSTALLATION SUMMARY** screen appears where you will be asked to accept the EULA.

3. On the **INSTALLATION SUMMARY** screen, click on the **EULA** button.

The **EULA** screen opens.

4. Read the EULA, select **Accept license agreement terms** at the bottom of the screen, and then click **DONE** located at the top-left to exit the **EULA** screen.

5. Click **Begin Installation**.

After installation completes, you can log on to the appliance's preconfiguration console to continue deployment.

Initial Setup Using the Preconfiguration Console

From the Deep Discovery Director - Network Analytics (the appliance) preconfiguration console, you can use the following controls:

- Press **TAB** to navigate to menu items and fields.
 - Press **ENTER** to make a selection.
-

Procedure

1. Open the appliance's virtual machine console.
2. Log on to the preconfiguration console:
Default user name and password:
 - User name: admin
 - Password: adminThe **Main Menu** screen appears.
3. Go to **Network Configuration > Configure Management Interface**.
4. Configure and save the following required settings:
 - IPv4 address
 - Subnet mask
 - IPv4 gateway



Note

The eth0 interface is preselected. You can configure only IPv4 settings on this interface.

The **Network Configuration** screen appears after the settings are successfully saved.

5. Go to **Configure Hostname and DNS Settings**.

6. Configure and save the following settings:

- Hostname
Specify either as a host name or a FQDN.
- Primary DNS Server
- (Optional) Secondary DNS Server
- (Optional) Tertiary DNS Server
- (Optional) Search Order

The **Network Configuration** screen appears after the settings are successfully saved.

7. Use the **Back** button to navigate back to the main menu.

8. (Optional) From the main menu, go to **Change Admin Password** and then press **ENTER**.

Trend Micro recommends that you change the admin password.

The Linux **Change Password** prompt appears.

9. Change the admin password.

The **Main Menu** screen appears after the password is successfully changed.

After configuring network settings, you can use the preconfiguration console to register the appliance to Deep Discovery Director.

Registering to Deep Discovery Director on page 2-9

Registering to Deep Discovery Director

The Deep Discovery Director - Network Analytics appliance's correlation data and settings page are accessed through the Deep Discovery Director console. To access correlation data and the settings page, you must register the appliance to Deep Discovery Director.

You use the preconfiguration console to perform the registration.

From the preconfiguration console, you can use the following controls:

- Press **TAB** to navigate to menu items and fields.
- Press **ENTER** to make a selection.

Procedure

1. Open the appliance's preconfiguration console using the desired method.
 - Use the **Console** tab on the Virtual Machine Client.
 - Use a remote access application such as PuTTY.



Note

SSH is enabled by default, which enables you to remotely access the preconfiguration console. By using a remote access application, you can conveniently cut and paste registration information into the applicable fields.

2. Log on to the preconfiguration console:

Use the password that you configured during initial configuration. If you did not change the password, use the default password.

Default user name and password:

- User name: admin

- Password: admin

The **Main Menu** screen appears.

3. Go to **Register with Deep Discovery Director**.

The **DDD Registration and Unregistration** screen appears.

4. Enter the Deep Discovery Director IPv4 address and API key.



Note

For more about how to find this information, see [Deep Discovery Director IP Address/ API Key on page 2-5](#)

5. Navigate to **Register** and then press **ENTER**.

The **Status** changes to Connected.

6. Navigate to **Cancel** and then press **ENTER** to return to the **Main Menu**.

7. Navigate to **Logout** and then press **ENTER**.
-

Moving the Appliance to a Managed Group

When a Deep Discovery Director - Network Analytics appliance is first registered to Deep Discovery Director, it is placed in the **Unmanaged** folder of the Deep Discovery Director directory.

You must move the appliance to the **Managed** folder so that Deep Discovery Director can perform certain tasks for the appliance. For example, Deep Discovery Director can manage updates only for managed appliances.

Procedure

1. Log on to the Deep Discovery Director console.
2. Go to **Appliances > Directory**.

The **Directory** screen opens and displays the folder hierarchy of managed and unmanaged registered devices in the left pane.

The newly added appliance is displayed under the **Unmanaged** folder.

3. Hover over the appliance name and click the menu icon that appears on the right-hand side of the appliance name and then select **Move**.
4. In the window, select the **Managed** folder (or a subfolder within that folder) and then click **Move**.

For more information about managing appliances in the directory, see the *Deep Discovery Director Administrator's Guide*.

Chapter 3

Getting Started

After you complete the initial deployment, there are additional tasks you must perform to get the Deep Discovery Director - Network Analytics appliance up and running as quickly as possible.

You configure the appliance's settings by first logging in to Deep Discovery Director and then accessing the **Settings** screen for the appliance that you want to configure.

- *Accessing the Settings Screen on page 3-3*
- *Activating Your Product License on page 3-3*
- *Registering to Deep Discovery Inspector on page 3-4*
- *Adding as a Syslog Server on page 3-5*
- *Configuring Settings on page 3-8*
 - *Configuring the Domain Exception List on page 3-9*
 - *Configuring the Priority Watch List on page 3-10*
 - *Configuring the Registered Services Lists on page 3-10*
 - *Configuring the Trusted Internal Networks List on page 3-12*
 - *Configuring SMTP Settings on page 3-12*
 - *(Optional) Modifying Network Settings on page 3-14*

- *(Optional) Configuring Proxy Settings on page 3-15*
- *Configuring Time Zone and NTP Settings on page 3-16*
- *Configuring Alert Settings on page 3-17*
- *Configuring Storage Retention Settings on page 3-19*
- *(Optional) Configuring Disk Space on page 3-20*
- *Configuring Automatic Backups on page 3-21*
- *Performing Additional Tasks on page 3-22*
 - *Viewing Triggered Alerts on page 3-23*
 - *Viewing Your Product License on page 3-23*

Accessing the Settings Screen

You can configure the Deep Discovery Director - Network Analytics appliance through the **Settings** screen, which is accessed through the Deep Discovery Director console.

Procedure

1. Log on to the Deep Discovery Director console.
2. Go to **Appliances > Directory**.

In the left pane, the managed appliances are displayed under the **Managed** folder (or within a subfolder of the **Managed** folder).

3. Hover over the appliance name and click the menu icon to the right of the appliance name, then select **Management Console**.

The **Settings** screen opens.

4. In the **Settings** screen, configure settings as required and close the window when finished.
-

Activating Your Product License

After you have configured network access, you must activate your product license for full functionality.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **License**.
3. Click **New Activation code**.

The **Activation Code** screen opens.

4. Specify the new activation code.
5. Read the Trend Micro license agreement and then click **I have read and accept the terms of the Trend Micro License Agreement**.
6. Click **Save**.

The Deep Discovery Director - Network Analytics license activates.

Registering to Deep Discovery Inspector

As part of the integrated solution, you must register Deep Discovery Director - Network Analytics (the appliance) to Deep Discovery Inspector.

To perform this task, you must first access the appliance's **Settings** screen and record the appliance's IP address and API key.

You then log into Deep Discovery Inspector and use this information to register the appliance.



Important

Before performing this task, Deep Discovery Inspector must first be registered to Deep Discovery Director.

Procedure

Perform on Deep Discovery Director - Network Analytics.

1. Log on to Deep Discovery Director and access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Record the appliance's IP address and API key.
 - a. Go to **System Settings > Network** to find and record the IP address.

- b. Go to **About** to find and record the API key.
3. Close the **Settings** screen.
Perform on Deep Discovery Inspector.
4. Log on to the Deep Discovery Inspector console.
5. Go to **Administration > Integrated Products/Services > Deep Discovery Director > Network Analytics**.
6. Under **Connection Settings**, type the **Server address** and the **API key** for the appliance.
7. (Optional) If you have configured proxy settings for Deep Discovery Inspector and want to use these settings for connections to the appliance, select **Use the system proxy settings** and then configure the proxy server settings.
8. Click **Register**.

The **Status** changes to **Registered** and **Connected**.

**Note**

After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to the appliance.

9. Log out of the Deep Discovery Inspector console.
-

Adding as a Syslog Server

Deep Discovery Director - Network Analytics (the appliance) uses Deep Discovery Inspector's detection data for analysis and correlation. Therefore, you must configure Deep Discovery Inspector to send syslogs to the appliance.

To perform this task, you must first access the appliance's **Settings** screen and record the syslog IP address and port number, then log on to Deep Discovery Inspector and use the recorded information to add the appliance as a syslog server.

Procedure

Perform on Deep Discovery Director - Network Analytics

1. Log on to Deep Discovery Director and access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **Syslog Settings** and record the syslog IP address and port number.

You can change the syslog port number if desired.

3. Close the **Settings** screen.

Perform on Deep Discovery Inspector.

4. Log on to the Deep Discovery Inspector console.
5. Go to **Administration > Integrated Products/Services > Syslog**.
6. Click **Add**.

The **Add Syslog Server** screen appears.

Add Syslog Server

Enable syslog server

Server name or IP address: Port:

Protocol: UDP TCP SSL

Facility level:

Severity level:

Log format: CEF LEEF Trend Micro Event Format (TMEF)

Select all

Detection logs

<input checked="" type="checkbox"/> Malicious Content	<input checked="" type="checkbox"/> Malicious Behavior	<input checked="" type="checkbox"/> Suspicious Behavior	<input checked="" type="checkbox"/> Retro Scan
<input checked="" type="checkbox"/> Exploits	<input checked="" type="checkbox"/> Grayware	<input checked="" type="checkbox"/> Malicious URLs	
<input checked="" type="checkbox"/> Disruptive Applications	<input checked="" type="checkbox"/> Virtual Analyzer Detections	<input checked="" type="checkbox"/> Correlated Incidents	

System event logs

<input type="checkbox"/> System events	<input type="checkbox"/> Update events
--	--

Proxy Settings

Connect through a proxy server


FIGURE 3-1. Add Syslog Server

7. Select **Enable syslog server**.

8. In **Server name or IP address** and **Port**, type the IP address and port number identified in Step 2 above.

The default Deep Discovery Director - Network Analytics syslog port is 514.

9. Configure the following:

FIELD	VALUE
Protocol	TCP
Facility level	local3 The facility level specifies the source of a message.
Syslog severity level	Informational The syslog severity level specifies the type of messages to be sent to the syslog server. Deep Discovery Inspector will send informational and above messages.
Log format	Trend Micro Event Format (TMEF) Specifies the format with which to send event logs to the syslog server. Trend Micro Event Format (TMEF) is the format used by Trend Micro products for reporting event information.
Logs to send to the syslog server	<ul style="list-style-type: none"> • Select all logs in the Detection logs section. <hr/> <div style="border: 1px solid black; padding: 5px;">  Note Do not select logs in the System event logs section. </div>

10. Select **Connect through a proxy server** to use the settings configured on **Administration > System Settings > Proxy** to connect to a syslog server.

Select this option if Deep Discovery Inspector requires the use of proxy servers for intranet connections.

11. Click **Save**.
12. Log out of the Deep Discovery Inspector console.

Configuring Settings

Deep Discovery Director - Network Analytics settings are configured by first logging in to Deep Discovery Director and then accessing the **Settings** screen for the appliance that you want to configure.

Procedure

1. Open the **Settings** screen.
See *Accessing the Settings Screen on page 3-3*.
2. Configure the Domain Exception list.
See *Configuring the Domain Exception List on page 3-9*.
3. Configure the Priority Watch list.
See *Configuring the Priority Watch List on page 3-10*.
4. Configure the Registered Services lists.
See *Configuring the Registered Services Lists on page 3-10*.
5. Configure the Trusted Internal Networks list.
See *Configuring the Trusted Internal Networks List on page 3-12*.
6. Configure the SMTP server settings.
See *Configuring SMTP Settings on page 3-12*.
7. (Optional) Modifying the network settings.
See *(Optional) Modifying Network Settings on page 3-14*.
8. (Optional) Configure proxy settings.
See *(Optional) Configuring Proxy Settings on page 3-15*.
9. Configure time zone and NTP server settings.
See *Configuring Time Zone and NTP Settings on page 3-16*.

10. Configure alert settings.
See *Configuring Alert Settings on page 3-17*.
 11. Configure storage retention settings.
See *Configuring Storage Retention Settings on page 3-19*.
 12. (Optional) Configure additional disk space.
See *(Optional) Configuring Disk Space on page 3-20*.
 13. Configure automatic backups.
See *Configuring Automatic Backups on page 3-21*.
-

Configuring the Domain Exception List

Deep Discovery Director - Network Analytics uses the **Domain Exception List** to reduce the number of unnecessary correlations and false positives in the correlation data graphs.



Tip

Domains entered in this list and any interactions with them will not be included in the information displayed in the **Correlation Data** screen. By reducing false-positive correlations, you can more easily identify malicious event histories that require a response.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.
Accessing the Settings Screen on page 3-3
 2. In the left pane, select **Domain Exception List**.
 3. Enter domains that you consider safe as a comma delimited list.
 4. Click **Save**.
-

What to do next


You can later remove a domain from the list to include it and related interactions in past and future correlation graph histories.

Configuring the Priority Watch List

You can add servers from your environment that you consider high-priority for event tracking and incident reporting to the **Priority Watch List**.



Tip

Servers entered in this list are identified in the correlation graph with the priority list icon ()

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. In the left pane, select **Priority Watch List**.
3. Enter the IP addresses that you want to designate as high-priority servers as a comma-delimited list.

192.168.1.1,10.0.1.100

4. Click **Save**.
-

Configuring the Registered Services Lists

You can configure lists of registered services that help you manage analysis of Deep Discovery Director - Network Analytics correlation data.

**Tip**

Servers in the following registered lists and any interactions with them are not included in the information displayed in the **Correlation Data** screen.

- **HTTP Proxy - Transparent**
- **HTTP Proxy - Explicit**
- **High Traffic Server List**
- **High Traffic Client List**

Trend Micro recommends adding entries to these lists. By reducing false positive correlations, you can more easily identify malicious event histories that require a response.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. In the left pane, select **Registered Services**.
3. From the **Type** menu, select the desired registered service type and enter the IP address information for the server offering the service.

After you choose a type, you can click the info icon for a brief description of that service type.

- You can add one or more IPv4 or IPv6 addresses to each registered service list.
- You can add a server IP address to more than one registered service list.

For example, add a security audit server's IP address to the **High Traffic Client List** and a domain controller's IP address to the **High Traffic Server List** to reduce false-positive correlations.

4. Click **Add**.
-

Configuring the Trusted Internal Networks List

Deep Discovery Director - Network Analytics (the appliance) uses the **Trusted Internal Networks List** to determine which hosts are **Internal hosts** when creating correlation graphs and data.



Important

You must enter internal network information into the **Trusted Internal Networks List** list so that the appliance can create correlation information.

Any hosts that are not part of the **Trusted Internal Networks List** are designated as **External servers** in the **Correlation Data** screen. If information about your internal network is not accurately entered in this list, the appliance cannot accurately create correlations.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. In the left pane, select **Trusted Internal Networks List**.
3. Enter IPv4 or IPv6 networks that you consider safe and are trusted as a comma delimited list.

Enter as single IP addresses or as CIDRs.

23.208.39.244,2001:0db8:85a3:0000:0000:8a2e:0370:7334

128.154.26.0/24,2001:DB8::0/120

4. Click **Save**.
-

Configuring SMTP Settings

You must configure an SMTP server to send the Deep Discovery Director - Network Analytics appliance's incident reports and alert notifications through email.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Settings > SMTP**.

The **SMTP** screen appears.

3. Select **Use a SMTP server**.

4. Type the IPv4 address or FQDN of the SMTP server.

5. Select the security protocol to use for connections to the SMTP server.

Options are None, SSL/TLS, or StartTLS.

6. (Optional) Modify the port number.

7. Type a sender email address.

8. (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 requests originating from the appliance.

9. (Optional) Verify that the appliance 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 - Network Analytics can communicate with the specified SMTP server, an email with the predefined subject and message will be sent to the specified email address.

- c. Check your email account for receipt of the email.
-

(Optional) Modifying Network Settings

You can modify the Deep Discovery Director - Network Analytics appliance's network interface settings after the initial deployment. You can modify the following settings:

- Specify to use a host name instead of an IP address as the identity of the appliance.
 - Modify the IPv4 address information
 - Modify DNS settings
-

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Settings > Network**.
3. (Optional) Select **Use host name instead of IP address as the identity of this server**.

The host name must be resolvable within your network.

4. (Optional) Modify IPv4 settings.
 - a. Unregister the appliance from Deep Discovery Inspector prior to making any changes to the appliance's IPv4 address by going to **Administration > Integrated Products/Services > Deep Discovery Director > Network Analytics** on the Deep Discovery Inspector console and clicking on **Unregister** under **Connection Settings**.

Be sure to record the API key information before unregistering.

- b. Modify the appliance's IPv4 address settings.
5. (Optional) Modify DNS settings or add additional DNS servers to the list.
6. Click **Save**.
7. If you unregistered the Deep Discovery Director - Network Analytics appliance in a previous step, go to Deep Discovery Inspector and reregister the appliance.
 - a. Go to **Administration > Integrated Products/Services > Deep Discovery Director > Network Analytics** on the Deep Discovery Inspector console.
 - b. Under **Connection Settings**, enter the appliance's new IP address and the appliance's API key and click **Register**.
8. On the Deep Discovery Director - Network Analytics appliance, use the preconfiguration console to update the network information on Deep Discovery Director.
 - a. On the preconfiguration console, go to **Main Menu** and select **Register with Deep Discovery Director**.
 - b. Select **Update Settings** and press **ENTER**.

Related information

↳ [Registering to Deep Discovery Inspector](#)

(Optional) Configuring Proxy Settings

You must specify proxy settings if Deep Discovery Director - Network Analytics connects to the license update server through a proxy server.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

[Accessing the Settings Screen on page 3-3](#)

2. Go to **System Settings > Proxy**.
 3. To enable proxy settings, select **Connect to the license update server using a proxy server**.
 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 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**.
-

Configuring Time Zone and NTP Settings

Configure time zone and NTP server settings immediately after initial deployment.



Note

You must use NTP for time synchronization. You cannot manually configure the date and time on the Deep Discovery Director - Network Analytics appliance.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.
Accessing the Settings Screen on page 3-3
2. Go to **System Settings > Time**.
3. In the **Date and time** section, enter up to four NTP server addresses as IP addresses or FQDN.

4. Select the applicable time zone.

**Note**

Daylight Saving Time (DST) is used when applicable.

5. Select the preferred date and time format.
 6. Click **Save**.
-

Configuring Alert Settings

Deep Discovery Director - Network Analytics has a set of built-in alert rules that are enabled by default.

A standard template is used when generating an alert. You cannot modify the subject or the message.

You can modify the following settings:

- Enable or disable any rule.
- Edit certain rules to modify the frequency at which alerts are generated.
- Enter alert recipients for any rule.

**Note**

You must configure the list of recipient email addresses that will receive alerts.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **Alerts > Built-in Rules**.

3. Click the name of the rule you want to edit in the **Rule** column.

The **Edit Rule** screen appears.

4. (Optional) Toggle the status of this rule to **Enabled**.
5. (Optional) Configure the appropriate frequency settings:
 - **Alert frequency:** Select the frequency at which the alert is generated when the rule criteria are met or exceeded
 - **Check frequency:** Select the frequency at which the rule criteria are checked

For each built-in rule, you can configure the following:

- **License Expiration:** Cannot modify frequency
- **Service Stopped:** Edit **Alert frequency**
- **Incident Report:** Edit **Check frequency**
- **High Root Disk Usage:** Edit **Alert frequency**
- **High Data Disk Usage:** Edit **Alert frequency**

 **Note**

- Shorter frequencies mean that the alert will be generated more often. Select longer frequencies to reduce the noise the alert generates.
 - System rules are configured to continuously check the rule criteria. Only the **Alert frequency** can be modified.
 - Security rules are configured to immediately generate alerts if rule criteria are met or exceeded. Only the **Check frequency** can be modified.
-

6. In the **Recipients** field, type an email address and press **ENTER**.

You can add one or more recipients. Press **ENTER** after each entry.

7. Click **Save**.

**Tip**

Click **Restore Defaults** to restore this rule to its default values.

Alerts

Alerts provide immediate intelligence about the state of Deep Discovery Director - Network Analytics.

Alerts are classified into two categories:

- Critical alerts are triggered by events that require immediate attention.
- Important alerts are triggered by events that require observation.

Alert notifications are triggered by a set of predefined built-in rules that cannot be deleted. However, you can make modifications to the alert built-in rules to meet your needs. The rules define what the conditions are for triggering an alert, the content of the notifications, and the list of email recipients to whom the alerts are sent.

Configuring Storage Retention Settings

Configure how long Deep Discovery Director - Network Analytics saves system logs and the database that contains detection logs received from Deep Discovery Inspector.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Storage**.
3. Under **Database Storage**, configure the following:
 - a. **Delete database entries older than x days:** Type the number of days to save database entries.

**Note**

A **database entry** in this context refers to a Deep Discovery Inspector detection entry.

- b. **Delete system logs older than x days:** Type the number of days to save system logs.
-

**Note**

System logs contain entries about account log on and log off activity, system events such as backups, and system updates such as firmware upgrades.

4. Click **Save**.
-

(Optional) Configuring Disk Space

You can add disk space to the Deep Discovery Director - Network Analytics appliance's partitions to increase the number of logs or detection data that you can store.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Storage**.
3. Click **Configure space**.

The **Disk Space Configuration** screen appears.

4. (Optional) To add more disks to the appliance, do the following:
 - a. Click **Add disks**.
The disk selection dialog displays.
 - b. Select at least one disk to add to the appliance's disk space configuration.

Only unformatted disks that are larger than 1024 MB in size are displayed.

**WARNING!**

Disks cannot be removed after they are added.

- c. Click **Add**.

The selected disks are formatted and available disk space is added to the **Disk Space Configuration** screen.

5. 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.
-

6. Click **Apply**.

Available space is added to the partitions as specified.

Configuring Automatic Backups

You can configure Deep Discovery Director - Network Analytics to back up configuration settings and the database of metadata information sent from Deep Discovery Inspector.

The time it takes to export a backup depends on the size of the data and might take some time.

**Important**

The specified folder to which backups are exported must already exist. If necessary, go to the SFTP server and create the folder in the specified path before configuring automatic backups.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Back Up**.
3. Select **Automatically back up to SFTP server**.
4. Specify the following information:

FIELD	DESCRIPTION
Server address	Type the IP address or FQDN of the SFTP server.
Port	Type the port number (default port is 22).
Folder path	Type the folder path to use on the SFTP server.
User name / Password	Type the user name and password used to log on to the SFTP server.
Backup frequency	Specify a backup frequency using the drop-down lists and the clock tool.

5. Click **Save**.
-

Performing Additional Tasks

You can perform additional tasks on the **Settings** screen to help manage your Deep Discovery Director - Network Analytics appliance:

- *Viewing Triggered Alerts on page 3-23*
- *Viewing Your Product License on page 3-23*

For information about how to perform additional tasks that you can perform using Deep Discovery Director, see the *Deep Discovery Director Administrator's Guide*.

Viewing Triggered Alerts

You can use the **Settings** screen to quickly view a historical list of triggered alerts.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **Alerts > Triggered Alerts**.

The **Triggered Alerts** screen appears with a list of triggered alerts that have been sent.

3. Click on the details icon (📄) in the **Details** column to view more information for the selected triggered alert.

Viewing Your Product License

You can use the **Settings** screen to view information about your product license.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **License**.
3. Under **License Details**, view licensing details.
4. If your license has expired, you can enter a new activation code by clicking on **New Activation Code**.

If your license has expired, events continue to be correlated and correlation data graphs are available. However, your Deep Discovery Director - Network Analytics

appliance cannot be updated with ActiveUpdate and certain other features such as URL rating queries are not available. You should update the license at the earliest possible time.

Chapter 4

Using Correlation Data for Advanced Threat Analysis

- *Viewing Correlation Data on page 4-2*
- *Analyzing Correlation Data Information on page 4-6*

Viewing Correlation Data

You can view Deep Discovery Director - Network Analytics correlation data by clicking on the **Correlation Data** icon displayed on the Deep Discovery Director console. After you click on the icon, the **Correlation Data** screen opens to display the dynamically generated correlation data.



Note

The appliance provides correlation data only for certain protocols.

See *Supported Protocols on page 4-2*.

Procedure

- View correlation data for correlated events.

Viewing Correlation Data from Correlated Events on page 4-3

- View correlation data for suspicious objects.

Viewing Correlation Data for Suspicious Objects on page 4-4

Supported Protocols

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

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

- SMTP

Viewing Correlation Data from Correlated Events

You can use the **Correlation Data** icon on the **Correlated Events** screen to view correlation data for the selected event.



Note

Not all events detected by Deep Discovery Inspector are listed on the **Correlated Events** screen. Deep Discovery Director - Network Analytics (the appliance) creates correlated data only for detection events it determines are high risk where advanced analytics are of special interest to administrators and can help with advanced analysis of threats.


There are several reason why an event might be listed on the **Affected Hosts** screen or the **Network Detections** screen, but is not listed on the **Correlated Events** screen:

- The appliance determined that the detected event was not high risk.
- There are no correlations for that particular event.
- There are correlations for a particular event, but the appliance is still processing and correlating the event.

There is a certain delay between when Deep Discovery Director lists a detection in the **Network Detections** or **Affected Hosts** screens and when the **Correlation Data** icon is visible on the **Correlated Events** screen (if it is determined high risk). Generally the delay is 10-15 minutes, but can be up to 30 minutes under heavy load.













Procedure

1. Log on to the Deep Discovery Director console.
2. Go to **Detections > Correlated Events**.

The **Correlated Events** screen opens, which displays the list of detections with correlated events for the specified time period. The **Correlation Data** icon () is displayed on the left-hand side of the **Details** column.

Correlated Events 2018-07-01 00:00:00 to 2018-07-07 19:19:19

Search an interested IP address

Details	Correlated ↓	Attack Pattern	Severity	Interested IP	Data Source
 	2018-07-07 00:44:02	Malicious Download, CnC Callback	 High	10.52.198.72	ddd-na-sanjose (10.202.243.48)
 	2018-07-07 00:43:03	Lateral Probing, CnC Callback	 High	10.52.198.72	ddd-na-sanjose (10.202.243.48)
 	2018-07-03 15:30:02	Lateral Probing	 High	10.1.116.22	ddd-na-sanjose (10.202.243.48)
 	2018-07-03 12:00:02	Vulnerability Exploit, Lateral Probing	 High	209.58.129.98	ddd-na-sanjose (10.202.243.48)

- (Optional) Change the time period to see more or less correlated events.

If no events are displayed for the selected time period, increase the time period until you can see correlated events.



Note

You can use additional filters to filter the results displayed in the **Correlated Events** screen to make selection of the desired correlation data easier. See the *Deep Discovery Director Administrator's Guide* for more information.

- Click on the **Correlation Data** icon ()

The **Correlation Data** screen opens.

What to do next

Use the **Correlation Data** screen for advanced analysis and to view threat histories for detected threats.

See [Analyzing Correlation Data Information on page 4-6](#)

Viewing Correlation Data for Suspicious Objects


You can view correlation data for suspicious objects from the **Threat Intelligence** location.

**Note**

You can use additional filters to filter the results displayed in the specified **Threat Intelligence** screens to make selection of the desired correlation data easier. See the *Deep Discovery Director Administrator's Guide* for more information.

Procedure

1. Log on to the Deep Discovery Director console.
2. Go to the appropriate location:
 - Go to **Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects** to see correlation data from product intelligence suspicious objects.
 - Go to **Threat Intelligence > Custom Intelligence > User-Defined Suspicious Objects** to see correlation data from custom intelligence suspicious objects.

A screen opens that displays the list of suspicious objects for the selected suspicious object type. If correlation data exists for a suspicious object in the list, the **Correlation Data** icon () is displayed to the right of the suspicious object name.



Product Intelligence		
Synchronized Suspicious Objects		C&C Callback Addresses
<input type="button" value="Export"/>		
Type: All	<input type="text" value="Search an IP address, domain, URL, or SHA-1 hash value"/> <input type="button" value="Q"/>	
Object	Type	Risk Level
<input type="checkbox"/> 69AD1A8E8F6037FB34461FC8489F1D1A97619094	 File SHA-1	 High

FIGURE 4-1. Synchronized Suspicious Objects

Custom Intelligence

YARA Rules STIX **User-Defined Suspicious Objects** Exceptions

+ Add Import

Type: All Search an IP address, domain, URL, or SHA-1 hash value, or description. Q


Object	Type	Source	Description
<input type="checkbox"/> *.wagng.com	 Domain	Custom	malicious domain

FIGURE 4-2. User-Defined Suspicious Objects

3. Click on the **Correlation Data** icon ()

The **Correlation Data** screen opens.

What to do next

Use the **Correlation Data** screen for advanced analysis and to view threat histories for detected threats.

See *Analyzing Correlation Data Information on page 4-6*

Analyzing Correlation Data Information

- *Overview of the Correlation Data Screen on page 4-6*
- *Reviewing the Correlation Data Summary on page 4-8*
- *Analysis Using the Correlation Data Graph on page 4-10*
- *Analysis Using Transaction Data on page 4-15*
- *Dynamic Correlation Data Analysis on page 4-8*

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  for more summary details.

See [Reviewing the Correlation Data Summary on page 4-8](#).

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 4-10](#).

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 4-15](#).



Note

Deep Discovery Director - Network Analytics limits the displayed results to 1000 transactions. If there is too much correlation data, displayed results are truncated and do not contain all correlations.



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM38514/181030

Dynamic Correlation Data Analysis

The **Correlation Data** screen depicts correlation results at the point in time when you access the data. The results displayed are dynamic over time. Each time that you access the **Correlation Data** screen for a particular correlated event or suspicious object, the correlation results are dynamically created for that point in time. Therefore, initial results can display a limited set of correlations, but when the results are accessed on a later date, Deep Discovery Director - Network Analytics might display additional correlated events.

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. Open the **Correlation Data** screen from Deep Discovery Director.

[Viewing Correlation Data on page 4-2](#)

2. Review the risk and activity summary.

The summary provides the following information:

Risk summary	<ul style="list-style-type: none">• The attack pattern for the correlated event or suspicious object selected in Deep Discovery Director.• Risk assigned by Deep Discovery Director - Network Analytics to the event and related correlations. <p>Deep Discovery Director - Network Analytics uses a number of factors to assign risk, including proprietary risk analysis.</p>
--------------	--

Activity summary	<ul style="list-style-type: none"> • Identifies which hosts are involved in the suspicious or malicious activity. <p>Activity might be between internal hosts and external servers or might include lateral activity between internal hosts.</p> <p>Internal hosts are defined by the Trusted Internal Networks list that you configured during setup. For Deep Discovery Director - Network Analytics to provide an accurate analysis of correlation data, it is important to enter your internal networks and hosts in the Trusted Internal Networks list.</p> <ul style="list-style-type: none"> • Identifies the malicious activities found in the correlation data. • Identifies protocols involved in the transactions that are part of the correlation data. • Can include information about additional hosts that participated in the suspicious activity. • Can include information about suspicious objects when viewing correlation data for suspicious objects. • Each unique summary is generated from the dynamically created data in the Correlation Data screen.
------------------	---

3. Review more detailed summary data by clicking on **Show detection history**.

The detection history provides the following information:

Start IP address	<ul style="list-style-type: none"> • Displays the IP address found in the Interested IP field of the correlated event selected in Deep Discovery Director • The detection history for suspicious objects does not contain a start IP address entry.
------------------	--

Summary details	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">• Intelligence Gathering• Point of Entry• Command and Control Communications• Asset and Data Discovery• Lateral Movement• Data Exfiltration
-----------------	---

4. 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:

ELEMENT IN CORRELATION DATA GRAPH



FIGURE 4-3. Playback Bar

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.

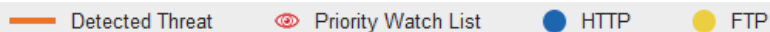


FIGURE 4-4. Example: Legend

ELEMENT IN CORRELATION DATA GRAPH**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.



Activity Legend

Identifies key activities for the internal host and external server participants in the graph.

- Activities vary for each specific correlation data graph.
- Can include activities similar to the following: Lateral Activity, Detected Event, C&C Activity, and Malicious Download
- Actions correspond to "Reason" in Deep Discovery Inspector logs.

Participant Icons

You can determine the activities in which each internal host or external server participated.



- Participant icons indicate if an internal host or external server is a participant in a specific activity.
- Hover over a internal host or external server to see the activities in which they are participants.
- Also determine which internal hosts or external servers were the source or endpoint for an activity.
- Participant: 
- Non-participant: 

ELEMENT IN CORRELATION DATA GRAPH**Correlation - Details Window**

- Hover over a correlation line to see more details about that correlation.
- Details include:
 - Source IP, user name, and host name
 - Destination IP
 - Severity
 - Detected URLs and SHA1s (if any)
 - Protocols and number of transactions
 - Reason
The listed reason corresponds to an activity in the **Activity Legend**.
 - Earliest date and latest date

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 end point is specified within the transaction number icon (color-coded for the protocol used for those transactions).
Examples of transaction number icons: , 
- 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 time line 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

Special Icons

Additional icons provide information about elements in the correlation graph.

- Member of **Priority Server List**: 
- Correlation event originated from an email: 

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 Data 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

- View the Deep Discovery Director - Network Analytics version number and build information located at the bottom of the **Transaction Data** section.
-

Configuring Incident Report Email Notifications

You can configure email notifications to receive incident reports for correlation events.

A standard template is used when generating an **Incident Report** message. You cannot modify the subject or the message.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **Alerts > Built-in Rules**.
3. Click on the **Incident Report** rule in the **Rule** column.

The **Edit Rule** screen opens.

4. If necessary, toggle the status of this rule to **Enabled**.
 5. Select the frequency at which the rule criteria is checked (1 hour, 3 hours, 8 hours, or 24 hours).
-



- Shorter frequencies mean that the alert will be generated more often. Select longer frequencies to reduce the noise the alert generates.
 - The **Incident Report** rule is configured to immediately generate alerts if rule criteria is met or exceeded.
-

6. In the **Recipients** field, type an email address and press **ENTER**.

You can add one or more recipients who should receive alert reports. Press **ENTER** after each entry.

7. Click **Save**.
-

Chapter 5

Updating Deep Discovery Director - Network Analytics

Updates to Deep Discovery Director - Network Analytics appliances are managed by Deep Discovery Director. To perform an update or to apply a hotfix or patch, you must upload the firmware or patch/hotfix on Deep Discovery Director, create a plan, and execute the plan with the appliance as a target.

Ensure that you have finished all management console tasks before executing upgrades. The upgrade process may take some time to complete. Trend Micro recommends starting the update during off-peak office hours. Installing the update restarts the appliance.


In addition, when you make modifications to certain settings on the appliance, you must synchronize those modifications to Deep Discovery Director using the Deep Discovery Director - Network Analytics preconfiguration console.

- *[Hotfixes and Patches Overview on page 5-2](#)*
- *[Uploading a Hotfix / Critical Patch / Firmware File on page 5-2](#)*
- *[Adding a Hotfix / Critical Patch / Firmware Deployment Plan on page 5-4](#)*
- *[Synchronizing Modifications on page 5-5](#)*

Hotfixes and Patches Overview

After an official product release, Trend Micro releases hotfixes, security patches, and patches to address issues, enhance product performance, or add new features.

TABLE 5-1. Hotfixes and Patches

HOTFIXES AND PATCHES	DESCRIPTION
Hotfix	<p>A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.</p> <hr/> <p> Note A new hotfix might include previous hotfixes until Trend Micro releases a patch.</p>
Security patch	A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.
Patch	A patch is a group of hotfixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.

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

<http://downloadcenter.trendmicro.com>

Uploading a Hotfix / Critical Patch / Firmware File

Updates to Deep Discovery Director - Network Analytics appliances are managed by Deep Discovery Director.

Before you can perform the update, you must upload the update files to the Deep Discovery Director repository.

Procedure

1. Obtain the hotfix / critical patch / firmware file.
 - Download the update from the Trend Micro Download Center at:
<http://downloadcenter.trendmicro.com>
 - Obtain the update from your Trend Micro reseller or support provider.
2. Log on the Deep Discovery Director console.
3. Go to **Appliances > Repository > Hotfix / Critical Patch / Firmware**.
4. Click **Upload**.
5. Click **Select** and then select a valid file.
6. (Optional) Type or paste the 64-character SHA-256 hash value of the selected file for verification.
7. (Optional) Type a description.
8. Click **Upload**.



Important

Closing the browser or tab that contains the management console cancels all uploads in progress.

9. Verify that the uploaded file is displayed in the **Hotfix / Critical Patch / Firmware** list.

For more information about uploading files to the repository, see the *Deep Discovery Director Administrator's Guide*.

Adding a Hotfix / Critical Patch / Firmware Deployment Plan

Updates to Deep Discovery Director - Network Analytics appliances are managed by Deep Discovery Director.

After you have uploaded the update files to the Deep Discovery Director repository, you can create a plan to deploy product updates and upgrades to an appliance.



Note

Only managed appliances can be updated by Deep Discovery Director.

Procedure

1. Log on the Deep Discovery Director console.
2. Go to **Appliances > Plans** and click on **Add**.
The **Add Plan** screen appears.
3. Type a plan name with a maximum of 256 characters.
4. Select **Hotfix / Critical Patch / Firmware** as type.
5. (Optional) Type a description.
6. Select a hotfix, critical patch, or firmware file from the list.



Note

Deep Discovery Director displays the list of files that are available on the repository server. Verify that the file matches the product and language of the target appliances.

7. Select target appliances.
Deep Discovery Director only displays compatible appliances.
8. Specify the schedule.

- **Custom:** Deploys the plan, downloads the files, and executes the plan according to the specified schedule.
- **Immediate:** Starts immediately after the plan is saved.

**Note**

Installing updates automatically restarts the target appliances.

9. Click **Save**.
10. After the plan is executed, verify that the update was applied successfully.
 - Go to the **Appliances > Plans** page and verify that the status is **Completed**.
 - Go to the **Appliances > Directory** page and click on the appliance name in the **Display Name** column.

For more information about using plans, see the *Deep Discovery Director Administrator's Guide*.

Synchronizing Modifications

After you make modifications to the Deep Discovery Director - Network Analytics appliance's configuration, you must synchronize those changes with Deep Discovery Director. For example, you must synchronize changes if you make changes to the network settings.

You use the preconfiguration console to perform the synchronization.

**Note**

Only modifications to managed appliances can be synchronized with Deep Discovery Director.

Procedure

1. Open the appliance's virtual machine console.



Note

If SSH is enabled, you can open the appliance's preconfiguration console using a remote access application such as PuTTY.

2. Log on to the preconfiguration console.

The **Main Menu** screen opens.

3. Select **Register with Deep Discovery Director** and then press **ENTER**.

The **DDD Registration and Unregistration** screen appears.

4. Press **TAB** to navigate to **Update Settings** and then press **ENTER**.

Updated settings are synchronized with Deep Discovery Director.

5. Press **TAB** to navigate to **Cancel** and then press **ENTER** to return to the main menu.

6. On the **Main Menu**, press **TAB** to navigate to **Logout** and then press **ENTER**.
-

Chapter 6

Backing Up or Restoring a Configuration

You can back up or restore certain of the Deep Discovery Director - Network Analytics appliance's configuration settings.

Trend Micro recommends exporting your settings to keep a backup.

- If the appliance cannot recover from a critical problem, import your configuration backup after restoring the device to automatically implement the pre-failure configuration.
- Or you can create a backup on a running appliance before making changes to the configuration. Having a backup allows you to quickly and conveniently revert to the original settings saved in the backup.



Important

When exporting/importing your settings, the database is locked. Therefore, all Deep Discovery Director - Network Analytics actions that depend on database access will not function.

Trend Micro recommends:

- Backing up the current configuration before each import operation.

- Performing the operation when the appliance is idle. Importing and exporting affects the appliance's performance.

Settings That Are Backed Up or Restored

You can back up the Deep Discovery Director - Network Analytics appliance's settings that are listed in the following table as well as the database of metadata sent from Deep Discovery Inspector.

SETTINGS MENUS AND METADATA DATABASE		DESCRIPTION
Metadata database used to create correlation data		Database of metadata sent from Deep Discovery Inspector
Domain Exception List		All entries on the domain exception list
Priority Watch List		All entries on the priority watch list
Registered Services		All entries on the registered servers list
Trusted Internal Networks List		All entries on the trusted internal networks list
System Logs		All system logs
License		The appliance's Activation code
About		The appliance's API key
Alerts	Triggered Alerts	All triggered alert records
	Built-in Rules	All rule settings
System Settings	Network	All network settings
	Proxy	Proxy settings
	SMTP	SMTP server settings
	Time	Time and NTP settings

SETTINGS MENUS AND METADATA DATABASE		DESCRIPTION
System Maintenance	Storage	Database and storage log retention settings and disk configuration
	Backup	Automatic backup settings

Manually Exporting a Backup

You can manually export a backup file of most of the Deep Discovery Director - Network Analytics appliance's configuration settings and the metadata database sent from Deep Discovery Inspector.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Back Up**.

The **Back Up** screen appears.

3. Under **Configuration Settings and Database Backup**, click **Export**.

The appliance exports a backup file with the configuration settings and database.

4. Download and save the backup file.
-

Configuring Automatic Backups

You can configure the Deep Discovery Director - Network Analytics appliance to create and upload automatic backups of its configuration settings and metadata database to an SFTP server of your choice.

The appliance 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. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Back Up**.

The **Back Up** screen appears.

3. Under **Automatic Backups**, select **Automatically back up to SFTP server**.

4. Type the IP address or FQDN of the SFTP server.

5. Type the port number.

Default is port 22.

6. Type the folder path to use on the SFTP server.

The folder specified in this step must already exist. If it does not exist, you must first create it on the SFTP server.

7. Type the user name and password used to log on to the SFTP server.

8. Specify a backup frequency using the drop-down lists and the clock tool.

9. Click **Save**.
-

Restoring from Backup

You can use a configuration settings and database backup to restore the Deep Discovery Director - Network Analytics appliance to a previous point in time.

Procedure

1. From the Deep Discovery Director management console, access the **Settings** screen.

Accessing the Settings Screen on page 3-3

2. Go to **System Maintenance > Restore**.

The **Restore** screen appears.

3. Click **Select File...** and select the backup file.

4. Click **Upload**.

The backup file is uploaded, then the appliance displays information about the backup file.

5. Click **Restore**.

The appliance displays a confirmation message.

6. Click **OK**.

The appliance restores the configuration settings and database from the backup file, and then restarts the server.

The server is now ready to resume operation.

Chapter 7

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 7-2*
- *Contacting Trend Micro on page 7-3*
- *Sending Suspicious Content to Trend Micro on page 7-4*
- *Other Resources on page 7-5*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

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

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

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

Threat Encyclopedia

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

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> to learn more about:

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

<https://ers.trendmicro.com/>

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

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File Reputation Services

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

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

Web Reputation Services

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

<http://global.sitesafety.trendmicro.com/>

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

Other Resources

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

Download Center

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

<http://www.trendmicro.com/download/>

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

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Index

A

- accessing
 - the settings screen, 3-3
- activating
 - product licenses, 3-3
- activation code
 - requirements, 2-3
- adding
 - appliance as syslog server, 3-5
 - hotfix, critical patch, or firmware to a deployment plan, 5-4
- additional tasks
 - performing, 3-22
- administration
 - product updates, hotfixes and patches overview, 5-2
- advanced threat analysis
 - correlation data, using for, 4-1
- alert rules
 - overview, 3-19
- alerts
 - configuring settings for, 3-17
 - critical alerts, 3-19
 - important alerts, 3-19
 - overview, 3-19
 - viewing triggered, 3-23
- alert settings
 - configuring, 3-17
- analysis
 - overview of, 4-6
 - using Correlation Data screen, 4-6
 - using the correlation data graph, 4-10
 - using transaction data, 4-15
- API key

- recording Deep Discovery Director, 2-5
- automatic backups
 - configuring, 3-21, 6-4

B

- backup
 - creating a, 6-1
- backups
 - configuring automatic, 6-4
 - manually exporting, 6-4
 - restoring settings from, 6-5
 - settings that are backed up or restored, 6-3
- browsers
 - supported, 2-3

C

- cables
 - requirements, 2-3
- configuration
 - additional tasks, 3-22
- configuration settings
 - configuring automatic backups of, 6-4
 - manual backup of, 6-4
 - restoring from, 6-5
- configuring
 - alert settings, 3-17
 - automatic backups, 6-4
 - disk space, 3-20
 - domain exception list, 3-9
 - incident report notifications for correlation events, 4-16
 - network settings, 3-14
 - notification SMTP servers, 3-12
 - priority watch list, 3-10

- proxy settings, 3-15
 - registered services lists, 3-10
 - settings, 3-8
 - storage retention settings, 3-19
 - time zone and NTP settings, 3-16
 - trusted internal networks list, 3-12
- Correlated Events screen
- selecting correlated data icon from, 4-3
- correlation
- analysis using Correlation Data screen, 4-6
 - analysis using details from correlation data graph, 4-10
 - dynamic analysis using Correlation Data screen, 4-8
 - reviewing the correlation data summary, 4-8
- correlation data
- analysis using, 4-6
 - analysis using transaction data, 4-15
 - analysis using using the correlation data graph, 4-10
 - dynamic analysis, 4-8
 - protocols supported, 4-2
 - selecting icon from Correlated Events screen, 4-3
 - using for advanced threat analysis, 4-1
 - viewing, 4-2
 - viewing for suspicious objects, 4-4
- correlation data graph
- analysis using details from the, 4-10
- Correlation Data screen
- analysis using correlation data information, 4-6
 - analysis using transaction data, 4-15
 - analysis using using the correlation data graph, 4-10
 - dynamic analysis of correlation data, 4-8
 - overview, 4-6
 - protocols supported for analysis using, 4-2
 - reviewing the correlation data summary, 4-8
 - selecting suspicious objects to view on the, 4-4
 - viewing correlation data on the, 4-2
- correlation data summary
- reviewing the, 4-8
- correlation events
- configuring incident report notification, 4-16
- critical alerts
- overview, 3-19
- ## D
- database
- configuring automatic backups of, 6-4
 - manual backups of, 6-4
 - restoring from, 6-5
- Data Correlation
- screen, overview of, 4-6
- Deep Discovery Director
- accessing the settings screen from, 3-3
 - adding a hotfix, critical patch, or firmware to a deployment plan, 5-4
 - moving Deep Discovery Director - Network Analytics appliance to a managed group, 2-10
 - opening Correlation Data screen from, 4-2
 - recording IP address and API key, 2-5
 - registering to, 2-9

- synchronizing modifications to, 5-5
 - updating using deployment plans from, 5-1
 - uploading a hotfix, critical patch, or firmware to, 5-2
 - version requirements, 2-3
 - viewing correlation data for suspicious object using, 4-4
 - viewing correlation data from Correlated Events screen, 4-3
- Deep Discovery Director - Network Analytics
- accessing the settings screen, 3-3
 - activating the product license, 3-3
 - adding a hotfix, critical patch, or firmware to a deployment plan, 5-4
 - analysis using correlation data information, 4-6
 - analysis using the correlation data graph, 4-10
 - analysis using transaction data, 4-15
 - backing up or restoring a configuration, 6-1
 - configuring alert settings, 3-17
 - configuring automatic backups, 3-21, 6-4
 - configuring disk space, 3-20
 - configuring domain exception list, 3-9
 - configuring incident report notifications for correlation events, 4-16
 - configuring priority watch list, 3-10
 - configuring proxy settings, 3-15
 - configuring registered services lists, 3-10
 - configuring settings for, 3-8
 - configuring SMTP settings, 3-12
 - configuring storage retention settings, 3-19
 - configuring the trusted internal networks list, 3-12
 - configuring time zone and NTP settings, 3-16
 - deployment, 2-1
 - dynamic analysis of correlation data, 4-8
 - initial setup using the preconfiguration console, 2-7
 - installing, 2-6
 - introduction, 1-1
 - making modifications to network settings, 3-14
 - manually exporting a backup, 6-4
 - moving the appliance to a managed group, 2-10
 - overview of the Correlation Data screen, 4-6
 - performing additional tasks, 3-22
 - protocols supported for correlation data analysis, 4-2
 - registering to Deep Discovery Director, 2-9
 - restoring from backup, 6-5
 - reviewing the correlation data summary, 4-8
 - settings that are backed up or restored, 6-3
 - synchronizing modifications to Deep Discovery Director, 5-5
 - updating, 5-1
 - uploading a hotfix, critical patch, or firmware, 5-2
 - using correlation data for advanced threat analysis, 4-1
 - viewing correlation data, 4-2

- viewing correlation data for suspicious objects, 4-4
- viewing correlation data from Correlated Events screen, 4-3
- viewing triggered alerts, 3-23
- Deep Discovery Director - Network Analyzer
 - adding as a syslog server, 3-5
 - registering to Deep Discovery Inspector, 3-4
 - viewing product license, 3-23
- Deep Discovery Inspector
 - adding Deep Discovery Director - Network Analyzer as a syslog server on, 3-5
 - registering Deep Discovery Director - Network Analyzer to, 3-4
 - version requirements, 2-3
- default user name and password
 - Deep Discovery Director - Network Analytics, 2-7
- deployment
 - checklist, 2-3
 - Deep Discovery Director - Network Analytics, 2-1
- deployment plan
 - adding hotfix, critical patch, or firmware to a, 5-4
- disk space
 - configuring, 3-20
- DNS server
 - IP addresses requirements, 2-3
- documentation feedback, 7-6
- domain exception list
 - configuring, 3-9
- Download Center
 - URL, 5-2
- dynamic analysis
 - using Correlation Data screen, 4-8
- E**
 - email notifications
 - configuring for correlation events, 4-16
 - Ethernet cables
 - requirements, 2-3
 - exporting
 - a manual backup, 6-4
- F**
 - firmware
 - adding to a deployment plan, 5-4
 - uploading to Deep Discovery Director, 5-2
- G**
 - getting started
 - tasks, 3-1
- H**
 - hardware
 - system requirements, 2-4
 - High Traffic Client List
 - use registered services lists to configure, 3-10
 - High Traffic Server List
 - use registered services lists to configure, 3-10
 - hotfix
 - adding to a deployment plan, 5-4
 - hotfixes
 - uploading to Deep Discovery Director, 5-2
 - hot fixes
 - overview, 5-2

- HTTP Proxy - Explicit
 - use registered services lists to configure, 3-10
- HTTP Proxy - Transparent
 - use registered services lists to configure, 3-10
- I**
- important alerts
 - overview, 3-19
- incident report notifications
 - configuring for correlation events, 4-16
- initial setup
 - using the preconfiguration console for, 2-7
- installing
 - Deep Discovery Director - Network Analytics, 2-6
- introduction
 - Deep Discovery Director - Network Analytics, 1-1, 1-2
- IP address
 - recording Deep Discovery Director, 2-5
- IP addresses
 - requirements, 2-3
- iso image
 - using to install Deep Discovery Director - Network Analytics, 2-6
- L**
- license
 - activating the Deep Discovery Director - Network Analytics, 3-3
 - viewing information about product, 3-23
- M**
- managed group
 - moving Deep Discovery Director - Network Analytics appliance to a, 2-10
 - managing
 - product licenses, 3-3
 - manual backups
 - exporting, 6-4
 - modifying
 - network settings, 3-14
 - moving
 - Deep Discovery Director - Network Analytics appliance to a managed group, 2-10
- N**
- network settings
 - modifying, 3-14
- notifications
 - configuring email for incident reports, 4-16
 - configuring SMTP server for, 3-12
- NTP
 - configuring settings for, 3-16
- NTP server
 - IP addresses requirements, 2-3
- O**
- overview
 - Deep Discovery Director - Network Analytics, 1-2
 - Deep Discovery Director - Network Analytics solution, 2-2
 - hotfixes and patches, 5-2
- P**
- patch
 - adding to a deployment plan, 5-4
- patches

- overview, 5-2
- uploading to Deep Discovery Director, 5-2
- performing
 - additional tasks, 3-22
- ports
 - system requirements, 2-5
- pre-configuration console
 - using for initial setup, 2-7
 - using to register to Deep Discovery Director, 2-9
 - using to synchronize changes to Deep Discovery Director, 5-5
- pre-deployment
 - checklist, 2-3
- priority watch list
 - configuring, 3-10
- product updates
 - hotfixes and patches overview, 5-2
- product upgrades
 - uploading hotfixes, patches, firmware, 5-2
- protocols
 - supported for correlation data, 4-2
- proxy
 - configuring settings, 3-15
- proxy settings
 - configuring, 3-15
- R**
- recording
 - Deep Discovery Director IP address and API key, 2-5
- registered services lists
 - configuring, 3-10
- registering

- Deep Discovery Director - Network Analyzer to Deep Discovery Inspector, 3-4
- to Deep Discovery Director, 2-9
- requirements
 - hardware, software, and port system, 2-4
 - pre-deployment, 2-3
- restores
 - settings that are backed up or restored, 6-3
- restoring
 - configuration from a backup, 6-1
 - settings from backup, 6-5
- retention settings
 - configuring storage, 3-19
- reviewing
 - correlation data summary, 4-8
- S**
- security patches
 - overview, 5-2
- selecting
 - correlation data icon from Correlated Events screen, 4-3
- services lists
 - configuring registered, 3-10
- settings
 - configuring, 3-8
 - that are backed up or restored, 6-3
- settings screen
 - accessing the, 3-3
 - activating the product license from the, 3-3
 - configuring alert settings from the, 3-17
 - configuring automatic backups from the, 3-21

- configuring disk space from the, 3-20
 - configuring domain exception list from the, 3-9
 - configuring priority watch list from the, 3-10
 - configuring proxy settings from the, 3-15
 - configuring registered services lists from the, 3-10
 - configuring SMTP settings from the, 3-12
 - configuring storage retention settings from the, 3-19
 - configuring the trusted internal networks list from the, 3-12
 - configuring time zone and NTP settings from the, 3-16
 - modifying network settings from the, 3-14
 - performing additional tasks from the, 3-22
 - viewing product license information from the, 3-23
 - viewing triggered alerts from the, 3-23
- SMTP
- configuring settings, 3-12
 - notification server, configuring, 3-12
- SMTP settings
- configuring, 3-12
- software
- system requirements, 2-4
- solution overview
- Deep Discovery Director - Network Analytics, 2-2
- storage
- configuring retention settings for, 3-19
 - storage retention settings
 - configuring, 3-19
- support
- resolve issues faster, 7-4
- synchronizing
- modifications to Deep Discovery Director, 5-5
- syslog server
- adding appliance as syslog server on Deep Discovery Inspector, 3-5
- system maintenance
- backing up or restoring a configuration, 6-1
- system requirements
- hardware, software, and port, 2-4
 - pre-deployment, 2-3
- system settings
- configuring network settings, 3-14
 - configuring notification SMTP server, 3-12
 - configuring proxy settings, 3-15
 - configuring time zone and NTP settings, 3-16

T

- tasks
- getting started, 3-1
 - performing additional, 3-22
 - to configure settings, 3-8
 - to perform after getting started, 3-22
- time zone
- configuring settings for, 3-16
- transaction data
- analysis using, 4-15
- transactions
- analysis using details from, 4-15
- triggered alerts

- overview, 3-19

- viewing, 3-23

- trusted internal networks list

- configuring, 3-12

U

- updating

- using deployment plans from Deep Discovery Director, 5-1

- uploading

- hotfixes, critical patches, or firmware to Deep Discovery Director, 5-2

V

- version requirements

- Deep Discovery Director, 2-3

- Deep Discovery Inspector, 2-3

- viewing

- correlation data, 4-2

- correlation data for suspicious objects, 4-4

- product license information, 3-23

- triggered alerts, 3-23

- virtual machine

- creating when installing Deep Discovery Director - Network Analytics, 2-6