TREND MICRO™

Trend Micro™
Deep Discovery™ Director
(Internal Network Analytics Version)

5.5

Administrator's Guide

Breakthrough Protection Against APTs and Targeted Attacks

Deep Discovery Director (Internal Network Analytics Version) Administrator's Guide

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

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

https://www.trendmicro.com/privacy

Table of Contents

Chapter 4: Detections

Chapter 5: Threat Intelligence

Chapter 6: Appliances

Chapter 7: Alerts

Chapter 8: Reports

Chapter 9: Administration

Chapter 10: Troubleshooting

Chapter 11: Technical support

Appendices

Appendix A: Service Addresses and Ports

Appendix B: Settings Replicated by Deep Discovery Director

Index

Preface

Preface

Welcome to the Trend Micro Deep Discovery Director (Internal Network Analytics Version) *Administrator's Guide*. This guide contains information about product settings.

Documentation

The documentation set for Deep Discovery Director (Internal Network Analytics Version) includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Director (Internal Network Analytics Version), and explanations on Deep Discovery Director (Internal Network Analytics Version) concepts and features.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Director.
Automation API Guide	A PDF document that explains how to use Deep Discovery Director Automation APIs.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Director (Internal Network Analytics Version) to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Director (Internal Network Analytics Version) management console. The Online Help contains explanations of Deep Discovery Director (Internal Network Analytics Version) components and features, as well as procedures needed to configure Deep Discovery Director (Internal Network Analytics Version).

Document	Description
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: https://success.trendmicro.com
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Director (Internal Network Analytics Version), and using the Preconfiguration Console to set initial configurations and perform system tasks.

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

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

Audience

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

- Network topologies

- Database management

- Antivirus and content security protection

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

Convention	Description
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

About Trend Micro

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to

automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

Trend Micro customers include 9 of the top 10 Fortune® Global 500 companies across automotive, banking, healthcare, telecommunications, and petroleum industries.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. https://www.trendmicro.com

Chapter 1

Introduction

This chapter introduces Trend Micro™ Deep Discovery™ Director (Internal Network Analytics Version) 5.5 and the features and benefits in this release.

About Deep Discovery Director (Internal Network Analytics Version)

Trend Micro Deep Discovery Director (Internal Network Analytics Version) is a management solution that enables the following for Deep Discovery Inspector, Deep Discovery Analyzer, and Deep Discovery Director (Standalone Network Analytics Mode) appliances:

- Centralized deployment of hotfixes, critical patches, firmware, and Virtual Analyzer images

- Configuration replication

- Log aggregation

- Realtime threat detection monitoring and correlation

- Threat intelligence management and sharing

What's New

TABLE 1-1. What's New in Deep Discovery Director (Internal Network Analytics Version) 5.5

FEATURE/ ENHANCEMENT	DETAILS
Migrate OS to Rocky Linux	Deep Discovery Director (Internal Network Analytics Version) migrates backend OS to Rocky Linux

Features and Benefits

Deep Discovery Director (Internal Network Analytics Version) includes the following features:

FEATURE OR BENEFIT	DETAILS
MITRE ATT&CK™ Framework Tactics and Techniques information	Deep Discovery Director (Internal Network Analytics Version) detection details and analysis reports include MITRE ATT&CK™ framework Tactics and Techniques information.

Feature or Benefit	Details
Advanced threat analysis	Deep Discovery Director (Internal Network Analytics Version) seamlessly combines the management capabilities of Deep Discovery Director and the data correlation capabilities of Deep Discovery Director - Network Analyticsinto one server.
Deep Discovery Inspector log aggregation	Deep Discovery Director (Internal Network Analytics Version) aggregates Deep Discovery Inspector detection logs. Using the same intuitive multi-level format, the Deep Discovery Director (Internal Network Analytics Version) management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.
Product intelligence	Deep Discovery Director (Internal Network Analytics Version) consolidates suspicious objects and C&C callback addresses from registered Deep Discovery appliances.
Custom intelligence	Deep Discovery Director (Internal Network Analytics Version) can distribute YARA rules to registered appliances and import threat intelligence using the Structured Threat Information eXpression (STIX 1.x, 2.0) format. You can also add user-defined suspicious objects that have not yet detected on your network, as well as exceptions that you consider harmless.
Feed management	Deep Discovery Director (Internal Network Analytics Version) allows you to subscribe to and monitor intelligence feeds for threat information that can be used to complement your product and custom intelligence.
Threat intelligence sharing	Deep Discovery Director (Internal Network Analytics Version) can share threat intelligence data with other products or services through TAXII (1.x, 2.0), OpenDXL, and HTTP or HTTPS web service.
Auxiliary products and services	To help provide effective detection and blocking at the perimeter, Deep Discovery Director (Internal Network Analytics Version) can distribute threat intelligence data to auxiliary products and services.
File passwords syncing	Deep Discovery Director (Internal Network Analytics Version) can configure and sync **File Passwords** settings with registered Deep Discovery Analyzer appliances.

FEATURE OR BENEFIT	DETAILS
Dashboard	The Dashboard screen and Deep Discovery appliance widgets allow administrators to view network integrity and system threat data.
Detections	The **Detections** screen provides access to real-time information about various detection categories.
Syslog	The **Syslog** screen allows Deep Discovery Director (Internal Network Analytics Version) to send suspicious objects lists and detection and appliance related logs in CEF and LEEF to up to three **Syslog** servers.
System alerts	Administrators can view the details of triggered alerts directly on the management console. Custom rules can be created to be alerted of specific threats.
Reports	Deep Discovery Director (Internal Network Analytics Version) can generate scheduled and on-demand **Network Security** reports.
Simple Network Management Protocol	Deep Discovery Director (Internal Network Analytics Version) supports Simple Network Management Protocol (SNMP) and can use it to send SNMP trap messages to notify administrators about events that require attention, and to listen to SNMP manager requests for system information and status updates.
Role-based access control	Built-in roles allow administrators to control which management console screens and features can be accessed. Custom roles can be created to control which appliances a role can see and manage, and which email message detections a role can see.
Storage configuration	Administrators can add extra available disk space to Deep Discovery Director (Internal Network Analytics Version) partitions to increase the number of logs or repository files that can be stored.
Directory	The **Directory** displays information about Deep Discovery appliances that are registered to Deep Discovery Director (Internal Network Analytics Version).
Plans	Plans define the scope and schedule of deployments to target appliances.
Repository	The **Repository** screen displays all update, upgrade, and **Virtual Analyzer** image files hosted by the server. Upload and delete files from here.

Feature or Benefit	Details
Component updates	Deep Discovery Director (Internal Network Analytics Version) uses components to display related information about detections.
Updates	The **Updates** screen enables you to install hotfixes, patches and firmware upgrades to Deep Discovery Director (Internal Network Analytics Version). After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.
LDAP server integration	Deep Discovery Director (Internal Network Analytics Version) allows **LDAP** accounts to access the management console.
SAML for single sign-on (SSO)	Deep Discovery Director (Internal Network Analytics Version) supports the Security Assertion Markup Language (SAML) authentication standard using Okta and Active Directory Federation Services (ADFS) identify providers to allow users to single sign-on to the Deep Discovery Director (Internal Network Analytics Version) console when they sign in to their organization's portal.
System Logs	Deep Discovery Director (Internal Network Analytics Version) maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.
Trend Micro Apex Central™ integration	Deep Discovery Director (Internal Network Analytics Version) integrates with Trend Micro Apex Central for the express purpose of retrieving endpoint analysis reports to provide Deep Discovery Director - Network Analytics as a Service with even more data for more thorough advanced threat analysis.
Web API access	Deep Discovery Director (Internal Network Analytics Version) now allows the creation of user accounts that are only allowed system access via web API. Web API can be used to automate certain threat intelligence related tasks.

Chapter 2

Deployment and Installation

This chapter contains information about the requirements and procedures for deploying and installing Deep Discovery Director (Internal Network Analytics Version).

Virtual Appliance System Requirements

Trend Micro recommends the following minimum specifications when installing Deep Discovery Director (Internal Network Analytics Version) on a virtual appliance.

> **Important**
>
> The minimum specifications are for a fresh installation. If you are upgrading from Deep Discovery Director 5.3 or later, you can use your current configuration with Deep Discovery Director 5.5.

TABLE 2-1. System Requirements

REQUIREMENT	MINIMUM SPECIFICATIONS

Hardware	• Network interface card: 1 with E1000 or VMXNET 3 adapter
	
	⚠️ **Important**
	    • Deep Discovery Director (Internal Network Analytics Version) does not support the VMXNET 2 (Enhanced) adapter type.
	    • For port binding, specify the same adapter type to use for all network interface cards.
	
	• SCSI Controller: LSI Logic Parallel
	• CPU: 1.8GHz (at least 8 cores)
	• Memory: 24GB
	• Hard disk: 300GB
	
	📝 **Note**
	    • The minimum specifications are calculated using 30 days of detection log storage for 1 Deep Discovery appliance as basis.
	    • The CPU, memory, and hard disk requirements increase with the expected throughput for Deep Discovery Director (Internal Network Analytics Version) and with the number of Deep Discovery appliances Deep Discovery Director (Internal Network Analytics Version) is expected to aggregate detection logs from.
	    For details, see *Recommend System Requirements on page 2-4*.

Software	• Hypervisor: VMware vSphere ESXi 7.0 or Microsoft Hyper-V in Windows Server 2016, 2019, 2022, 2025 • Guest operating system: Red Hat Enterprise Linux 7 (64-bit)

Requirement	Minimum Specifications
Ports	• TCP 443 (Deep Discovery Director connection) • UDP 123 (default NTP server connection)
Certificate	• Self-signed • PEM format • Certificate only or certificate and private key in the same file • Certificate chain supported Encryption methods: • Private key: RSA algorithm only • Certificate: Digest size of 256 (SHA-256) or higher Generation command example (CentOS): ``` # openssl genpkey -algorithm RSA -out key.pem -pkeyopt rsa_keygen_bits:2048 # openssl req -new -key key.pem -out csr.pem # openssl req -x509 -sha256 -days 365 -key key.pem -in csr.pem -out certificate.pem # cat key.pem >> certificate.pem ```

Recommend System Requirements

The CPU, memory, and hard disk requirements increase with the expected throughput for Deep Discovery Director (Internal Network Analytics Version) and with the number of Deep Discovery appliances Deep Discovery Director (Internal Network Analytics Version) is expected to aggregate detection logs from.

Note

The hard disk requirements below are calculated using 180 days of detection log storage as basis. The longer detection logs are to be stored, the more disk space is required.

Throughput (Gbps)	Virtual CPUs	Virtual Memory (GB)	Virtual Disk
1	8	28	800 GB
2	10	34	1.3 TB
3	12	40	1.8 TB
4	14	46	2.3 TB

Installing Deep Discovery Director (Internal Network Analytics Version) on a Virtual Appliance

Important

Deep Discovery Director (Internal Network Analytics Version) supports installation under legacy Basic Input/Output System (BIOS).

- Changing the setting after installation causes Deep Discovery Director (Internal Network Analytics Version) to be unable to boot.

- Deep Discovery Director (Internal Network Analytics Version) must be reinstalled to change the setting.

Procedure

1. Create a custom virtual machine with the following minimum specifications:

   - Virtual machine hardware version: 17

   - Guest operating system: Red Hat Enterprise Linux 7 (64-bit)

   - CPU: 1 virtual socket with 8 cores

   - Memory: 24GB

   - Network interface card: 1 with E1000 or VMXNET 3 adapter

> ⚠️ **Important**
>
> - Deep Discovery Director (Internal Network Analytics Version) does not support the VMXNET 2 (Enhanced) adapter type.
>
> - For port binding, specify the same adapter type to use for all network interface cards.

- SCSI Controller: LSI Logic Parallel

- Hard disk: 300GB

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

3. Connect the CD/DVD device of the virtual machine to the Deep Discovery Director (Internal Network Analytics Version) ISO image file, and then boot the virtual machine from the CD/DVD drive.

   The Deep Discovery Director (Internal Network Analytics Version) Installation screen appears.

```
            Deep Discovery Director Installation

Install base version
Install internal Network Analytics (NA) version
Install no internal NA, no log receiving capability version
Silently install internal Network Analytics version
Exit
```
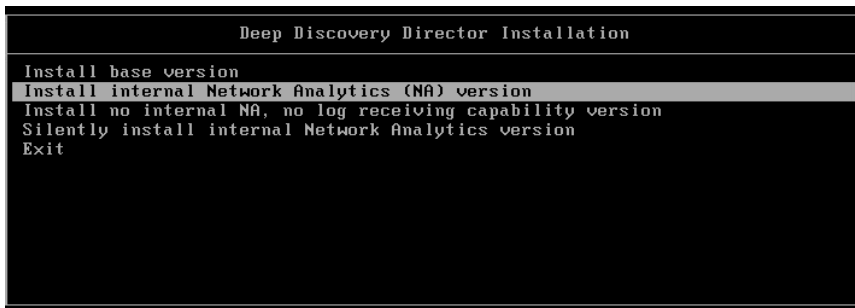
FIGURE 2-1. Deep Discovery Director Installation Screen

4. Select **Install internal Network Analytics (NA) version**.

The **Disk Selection** screen appears.
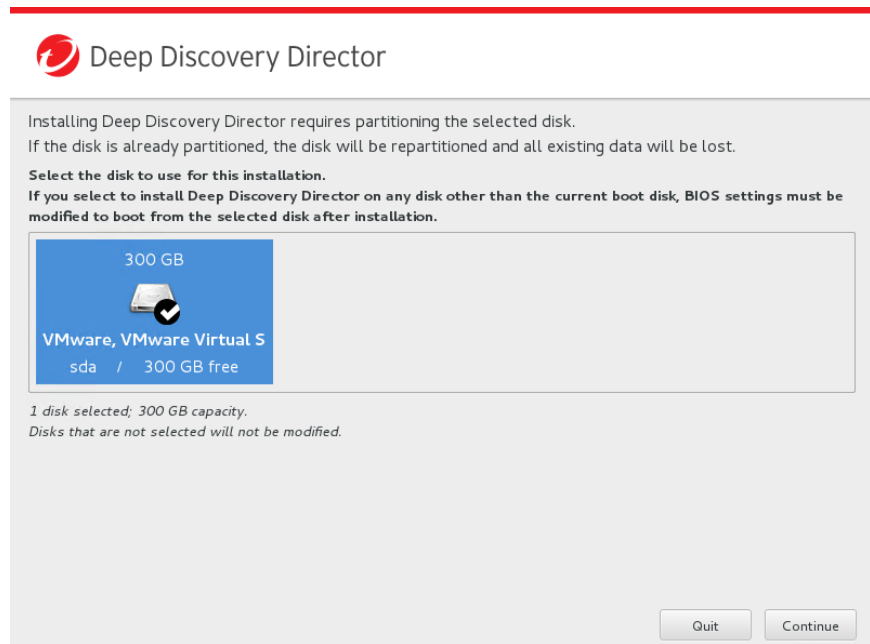
FIGURE 2-2. Disk Selection Screen

5. Click **Continue**.

The **Hardware Profile** screen appears.

6. Click **Continue**.

The installation starts.
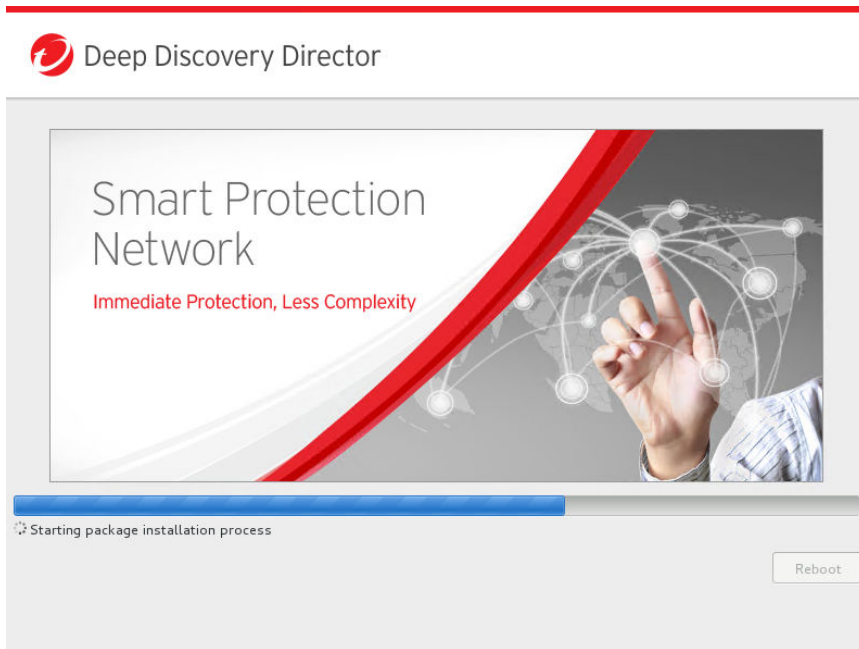
FIGURE 2-3. Installation Screen

Configuring Network Settings

Procedure

1. Log on to the preconfiguration console.

    The following are the default credentials:

    • User name: admin

    • Password: admin

    The **Main Menu** screen appears.

2. Select **Configure network settings** and then press **ENTER**.

   The **Configure Network Settings** screen appears.

3. Configure the following required settings:

   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - DNS server 1

   Note

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

   ---

4. Press **TAB** to navigate to **Save**, and then press **ENTER**.

   The **Main Menu** screen appears after the settings are successfully saved.

Logging on to the Management Console

Procedure

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

   The management console logon screen appears.

2. Type the following default credentials:

   - User name: admin
   - Password: admin

> **Important**
>
> - Trend Micro recommends changing the password after logging on to the management console for the first time.
>
> - Changing the password for the management console does not change the password for the preconfiguration console.

3. Click **Log on**.

    The management console appears.

Chapter 3

Dashboard

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

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Dashboard Overview

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

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

Tabs

Tabs provide a container for widgets.

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

Tab Tasks

Task	Steps
Add a tab	Click the plus icon at the top of the dashboard.
Rename a tab	1. Select the tab you wish to rename. 2. Click the menu icon beside the tab title and then select **Rename**. 3. Type a name with a maximum of 64 characters.
Move a tab	Drag a tab's title to change the tab's position.
Delete a tab	1. Select the tab you wish to delete. 2. Click the menu icon beside the tab title and then select **Delete**.

Widgets

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

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

Widget Tasks

Task	Steps
Add widgets to the dashboard	To add widgets to the dashboard, do any of the following: • Select the tab you wish to add widgets to, click the menu icon beside the tab title, and then select **Add Widgets**. • Select the tab you wish to add widgets to, click the gear icon in the top-right corner of the screen, and then select **Add Widgets**. • On newly created tabs, click **Add a widget.** The **Add Widgets** screen displays. For details, see *Adding Widgets to the Dashboard on page 3-4*.
Create a new widget	Create a new, customized widget to track and monitor information of interest to you. For details, see *Creating a Widget on page 3-5*.
Refresh a widget	Click the menu icon in the top-right corner of the widget, and then select the refresh icon. **Note** Widget views refresh automatically. Different widgets can have different refresh times.
Edit a widget	Click the menu icon in the top-right corner of the widget, and then select the edit icon. The **Edit Widget** dialog displays. For more details, see *Editing a Widget on page 3-6*. **Note** Different types of widgets have different settings to configure.

Task	Steps
Delete a widget	Click the menu icon in the top-right corner of the widget, and then select the delete icon.
	Note
	Widgets can also be deleted from the **Add Widgets** screen. Deleting a widget from the **Add Widgets** screen affects all instances that are already on the dashboard, and the deleted widgets cannot be restored.
Move a widget	Drag a widget's title change the widget's position.
Resize a widget	Drag the resize icon in the bottom-right corner of the widget to resize the widget.

Adding Widgets to the Dashboard

Procedure

1. Go to the **Dashboard** screen and do any of the following:

    • Select the tab you wish to add widgets to, click the menu icon beside the tab title, and then select **Add Widgets**.

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

    • On newly created tabs, click **Add a widget.**

    The **Add Widgets** screen displays.

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

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

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

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

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

4. Click **Add**.

   The selected widgets are added to the dashboard.

Creating a Widget

Procedure

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

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

   The **Create New Widget** screen displays.

3. Configure the following:

   a. Type a unique name for this widget.

   b. Select the filter to use for this widget. Only **Network Detections** and **Email Messages** saved searches can be selected.

   c. Type a description for this widget.

   d. Select the chart type and configure the data to display.

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

4. Click **Save**.

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

Editing a Widget

Procedure

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

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

The **Edit Widget** dialog displays.

3. Configure the widget.

> **Note**
>
> • Different types of widgets have different settings to configure.
>
> • No example charts are displayed in the dialog.

4. Click **OK**.

Deep Discovery Inspector Widgets

Deep Discovery Director (Internal Network Analytics Version) includes the following Deep Discovery Inspector widgets:

TABLE 3-1. Deep Discovery Inspector Widgets

WIDGET	DESCRIPTION
Threats at a Glance	This widget displays actionable information about six key metrics and links to the corresponding detection logs.
Top Affected Hosts	This widget displays hosts with the highest severity rating by severity in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

Widget	Description
Scanned Traffic by Protocol Type	This widget displays total traffic volume by protocol, in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.
Threat Geographic Map - C&C Communications	This widget displays a graphical representation of the affected hosts with C&C communication detections on a virtual world map within the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

Threats at a Glance

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

Table 3-2. Threats at a Glance

Metric	Source	Description
Targeted attact detections	Affected Hosts	• Counts Affected Hosts • Associated with the **Targeted Attack detections** preset search Click a value to drill down to the **Affected Hosts** screen.
C&C communication detections	Affected Hosts	• Counts Affected Hosts • Associated with the **C&C Communication detections** preset search Click a value to drill down to the **Affected Hosts** screen.
Lateral movement detections	Affected Hosts	• Counts Affected Hosts • Associated with the **Lateral Movement detections** preset search Click a value to drill down to the **Affected Hosts** screen.

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

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

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

Top Affected Hosts

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

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

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

Scanned Traffic by Protocol Type

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

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

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

Threat Geographic Map - C&C Communications

This widget displays a graphical representation of the affected hosts with C&C communication detections on a virtual world map within the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

The **Threat Geographic Map - C&C Communications** displays regions with affected hosts as a solid red circle.

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

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

Network Top YARA Rule Detections

This widget displays the YARA rule files with the highest detection counts in network detections in the last 1 hour/24 hours/7 days/14 days/30 days/90 days.

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

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

Deep Discovery Email Inspector Widgets

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Chapter 4

Detections

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

About the Detections Screens

The **Detections** screens provide access to realtime information about the following detection categories.

TABLE 4-1. Detections

DETECTION CATEGORIES	DESCRIPTION
Affected Hosts	Hosts that have been involved in one or more phases of a targeted attack. For details, see *Affected Hosts on page 4-7*. For details about the Host Severity scale, see *Host Severity on page 4-3*.
Network Detections	Hosts with detections from all event logs, including global intelligence, user-defined lists, and other sources. For details, see *Network Detections on page 4-47*.
Email Messages	**Note** Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances. This feature or screen will not contain any actual data or only display **No data to display.**
Quarantined Messages	**Note** Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances. This feature or screen will not contain any actual data or only display **No data to display.**

DETECTION CATEGORIES	DESCRIPTION
Correlated Events	Events that show one or more attack patterns derived from the correlated data of multiple detections in your network.
	For details, see *Correlated Events on page 4-75*.
	Note
	Review and understand for which protocols Deep Discovery Director - Network Analytics provides correlation data, and why it might not display any correlation data.
	• *Protocols That Support Advanced Analysis Using Correlation Data on page 4-6*
	• *Reasons Why No Correlations Are Found on page 4-6*

Host Severity

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

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

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

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

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

TABLE 4-2. Host Severity Scale

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

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

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

Protocols That Support Advanced Analysis Using Correlation Data

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

- HTTP
- HTTPS
- SSL
- FTP / FTP Data
- RDP
- SMB/SMB2
- KRB5
- SMTP

Reasons Why No Correlations Are Found

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

- Invalid data received causing fatal error. Please try again.
- Invalid session. Please re-login to Deep Discovery Director and try again.
- Invalid parameters found while attempting to find correlations. Try again later after errors are resolved.

- Client errors were encountered while attempting to find correlations. Try again later after errors are resolved.

- Invalid response while attempting to find correlations. Try again later after errors are resolved.

- Internal errors were encountered while attempting to find correlations. Try again later after errors are resolved.

- No correlation provided because the selected incident originated from a client in the safe server list.

- No correlation provided because the protocol for the selected event is not supported.

- Currently, no correlation has been found for the selected incident. The system is still attempting to find correlations.

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

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

- No correlation provided because the selected suspicious object is in the domain exception list.

- Invalid data received causing fatal error. Please try again.

- No correlation graph rendered due to no data.

Affected Hosts

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

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

Access different information about **Affected Hosts** on the following views:

1. **Affected Hosts** view:

- Displays a summary of affected hosts by attack phase

- Provides access to **Host Details** views

  By default, Deep Discovery Director (Internal Network Analytics Version) searches the **Affected Hosts** view by **IP Address** and **Host Name**.

2. **Host Details** view:

   - Displays host event details in chronological order

   - Provides access to **Detection Details** views

   - By default, Deep Discovery Director (Internal Network Analytics Version) searches the **Affected Hosts - Host Details** view by **Peer Host**.

3. **Detection Details** view:

   - Displays details of each detected threat

   - Provides access to different information panels, depending on search and other filter criteria and settings

Display Options and Search Filters

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

TABLE 4-3. Display Options and Search Filters: Affected Hosts

FILTER OPTION	DESCRIPTION	
Detection severity	Filter options include the following detection severity settings:	
	High	Displays high severity detections
	Medium	Displays medium severity detections
	Low	Displays low severity detections
	Information al	Displays informational detections

Filter Option	Description	
	All detection severity levels	Displays all detections
Period	**Last 24 hours**	
	Last 7 days	
	last 14 days	
	Last 30 days	
	Last 60 days	
	Custom range	
Data source	Select which appliances to include as data source.	
Customize Columns	Customize the display by hiding or displaying columns.	
Basic search	Search for an IP address or host name.	
	Note Type a case-insensitive keyword in the basic search field to search a partial host match.	

FILTER OPTION	DESCRIPTION

Saved Searches	Search by saved search criteria.
	
	• The **Affected Hosts** view includes the following built-in saved searches:
	
	    • **Targeted Attack detections**
	
	    • **C&C Communication detections**
	
	    • **Lateral Movement detections**
	
	• The **Host Details** view includes the following preset searches:
	
	    • **Threats**
	
	    • **Known Threats**
	
	    • **Potential Threats**
	
	    • **Ransomware**
	
	    • **YARA Rule Detections**

Advanced Search	Search by user-defined criteria sets. Each set includes one or more of the following: • Attributes • Operators • Associated values For details, see *Affected Hosts Advanced Search Filter on page 4-31*.

Viewing Affected Hosts

Procedure

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

    The **Affected Hosts** screen appears.

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

3. Select a time period.

4. Select which appliances to include as data source.

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

TABLE 4-4. Host Information Columns

COLUMN NAME	PRESELECTED	DESCRIPTION
IP Address	X	IP address of the affected host
Host Name	X	Computer name of the host
MAC Address		Media Access Control address of a network node
Network Group	X	Network group that an IP address/host is assigned
Host Severity	X	Highest impact on a host determined from aggregated detections by Trend Micro products and services For details about the **Host Severity**scale, see *Host Severity on page 4-3*.
Most Notable Threat	X	Threat description of the highest severity detection
Latest Detection	X	Most recent detection, based on timestamp

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

TABLE 4-5. Notable Statistics Columns

COLUMN NAME	PRESELECTED	DESCRIPTION
Targeted Attack		A threat that aims to exfiltrate data from a target system For details, see *APT Attack Sequence on page 4-14*.

TABLE 4-6. Attack Phase Columns

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

Column Name	Preselected	Description
Data Exfiltration	X	Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.
Unknown Attack Phase	X	Detection is triggered by a rule that is not associated with an attack phase.

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

    By default, Deep Discovery Director (Internal Network Analytics Version) searches **Affected Hosts** by **IP Address** and **Host Name**.

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

    Deep Discovery Director (Internal Network Analytics Version) provides the following built-in saved searches:

    TABLE 4-7. Built-in Saved Searches

Name	Filter Options
Targeted Attack detections	Notable events in targeted attack
C&C Communication detections	Notable events in C&C communication
Lateral Movement detections	Notable events in lateral movement

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

    For details, see *Affected Hosts Advanced Search Filter on page 4-31*.

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

APT Attack Sequence

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

In targeted attacks, the APT life cycle follows a continuous process of six key phases.

TABLE 4-8. APT Attack Sequence

PHASE	DESCRIPTION
Intelligence Gathering	Identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack
Point of Entry	An initial compromise typically from zero-day malware delivered via social engineering (email/IM or drive-by download)
	A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.
Command & Control (C&C) Communication	Communications used throughout an attack to instruct and control the malware used
	C&C communication allows the attacker to exploit compromised machines, move laterally within the network, and exfiltrate data.
Lateral Movement	An attack that compromises additional machines
	Once inside the network, an attacker can harvest credentials, escalate privilege levels, and maintain persistent control beyond the initial target.
Asset/Data Discovery	Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest
Data Exfiltration	Unauthorized data transmission to external locations
	Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.

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

Viewing Affected Hosts - Host Details

Procedure

1. Go to **Detections** > **Affected Hosts** and click any detection link.

   Details about the host are displayed.

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

3. Select a time period.

4. Select which appliances to include as data source.

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

TABLE 4-9. General Columns

COLUMN NAME	PRESELECTED
Timestamp	X
Details	X
Data Source	X
Source Host	
Destination Host	
Interested Host	
Interested Network Group	
Peer Host	X
Peer Network Group	

Column Name	Preselected
Peer IP Country/Region	
User Account	

> **Note**
>
> The default **Timestamp**, **Details**, and **Threat Description** columns cannot be removed.

Table 4-10. Email Columns

Column Name	Preselected
Sender	
Recipients	
Email Subject	

Table 4-11. Detection Information Columns

Column Name	Preselected
Threat Description	X
Detection Name	X
Threat (Virtual Analyzer)	
Reference	
Detection Type	
Protocol	X
Transport Layer Security (TLS)	
Detection Severity	X
Attack Phase	X
Tactics	X

Column Name	Preselected
URL Category	
Direction	X
Notable Object	X
YARA Rule File Name	

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

   By default, Deep Discovery Director (Internal Network Analytics Version) searches **Affected Hosts** - **Host Details** by **Peer Host**.

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

   Deep Discovery Director (Internal Network Analytics Version) provides the following built-in saved searches:

Table 4-12. Built-in Saved Searches

Name	Filter Options
Threats	Detection type options include the following: • Malicious Content • Malicious Behavior • Suspicious Behavior • Exploit • Grayware • Malicious URL
Known Threats	File Detection Types: Known Malware

Name	Filter Options

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

Ransomware	Detection name options include the following: • Ransomware-related detections
YARA Rule Detections	YARA Rule File Name: Has YARA rule file name

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

   For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-36*.

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

   The **Export** dialog appears.

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

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

Viewing Affected Hosts - Detection Details

Procedure

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

   Detection details about the event are displayed.

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

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

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

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

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

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

Important

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

The password for the zip archive is "virus".

---

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

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

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

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

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

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

> **Important**
>
> Suspicious files must always be handled with caution. Extract the detected file at your own risk.
>
> The password for the zip archive is "virus".

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

Affected Hosts - Detection Details

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

Affected Hosts - Detection Details - Connection Details

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

- *Affected Hosts - Detection Details - Detection Information on page 4-21*
- *Affected Hosts - Detection Details - Connection Summary on page 4-23*
- *Affected Hosts - Detection Details - Protocol Information on page 4-24*
- *Affected Hosts - Detection Details - File Information on page 4-25*
- *Affected Hosts - Detection Details - Additional Information on page 4-26*

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

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

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

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

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

Affected Hosts - Detection Details - Detection Information

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

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

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

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

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

> **Important**
>
> MITRE information displayed on Deep Discovery Director (Internal Network Analytics Version) is based on ATT&CK™ v6. The information may be different when displayed on products that use a different version of ATT&CK™.

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

- Notable Object
- Protocol
- Reference
- Targeted attack campaign
- Targeted attack related
- Threat
- Threat description
- Timestamp
- URL category
- Virtual Analyzer risk level

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

TABLE 4-13. Detection Types

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

Affected Hosts - Detection Details - Connection Summary

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

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

- Host details may include the following:

    - Host name

    - IP address and port

    - Last logon user

    - MAC address

    - Network group

    - Network zone

    - Operating system

Affected Hosts - Detection Details - Protocol Information

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

- BOT command

- BOT URL

- Certificate Information

    - Issued To

        - Common name

        - Organization

        - Organizational unit

    - Issued By

        - Common name

        - Organization

        - Organizational unit

- Domain name

- Host name

- HTTP referer

- ICMP code

- ICMP type

- IRC channel name

- IRC nick name

- Message ID

- Protocol

- Queried domain

- Recipients

- Sender

- SNI host name

- Subject

- Target share

- Transport Layer Security (TLS)

- URL

- User agent

- User name

Affected Hosts - Detection Details - File Information

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

- File name

- File SHA-1

- File SHA-256

- File size

Affected Hosts - Detection Details - Additional Information

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

- Attempted to disrupt connection

- Detected by

- Mitigation

- Fingerprinting

    - JA3 hash value

    - JA3S hash value

- VLAN ID

Affected Hosts - Detection Details - File Analysis Result

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

- *Affected Hosts - Detection Details - File Analysis Result - File Information on page 4-27*

- *Affected Hosts - Detection Details - File Analysis Result - YARA Detections on page 4-28*

- *Affected Hosts - Detection Details - File Analysis Result - Notable Characteristics on page 4-28*

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

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

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

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

> ⚠ **Important**
>
> Suspicious files must always be handled with caution. Extract the detected file at your own risk.
>
> The password for the zip archive is "virus".

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

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

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

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

- Child files
    - File name / URL
    - File size (bytes)
    - Type
    - File SHA-1
    - File SHA-256
- File name
- File size
- File type
- File MD5
- File SHA-1

- File SHA-256

- MITRE ATT&CK™ Framework

    - Tactics

    - Techniques

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

> **Important**
>
> MITRE information displayed on Deep Discovery Director (Internal Network Analytics Version) is based on ATT&CK™ v6. The information may be different when displayed on products that use a different version of ATT&CK™.

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

- Threat

- Virtual Analyzer risk level

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

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

- YARA Rule File

- YARA Rules

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

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

- Anti-security, self-preservation

- Autostart or other system reconfiguration

- Deception, social engineering

- File drop, download, sharing, or replication

- Hijack, redirection, or data theft

- Malformation or other known malware traits

- Process, service, or memory object change

- Rootkit, cloaking

- Suspicious network or messaging activity

- Other notable characteristic

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

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

Affected Hosts - Detection Details - Suspicious Object Information

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

- Related analyzed file

- Suspicious object

- Type

- Virtual Analyzer risk level

Affected Hosts - Detection Details - Related Analyzed File Information

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

- Child files

    - File name

- File size (bytes)

- File type

- File SHA-1

- File name

- File size

- File type

- File MD5

- File SHA-1

- File SHA-256

- MITRE ATT&CK™ Framework

    - Tactics

    - Techniques

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

> ⚠️ **Important**
>
> MITRE information displayed on Deep Discovery Director (Internal Network Analytics Version) is based on ATT&CK™ v6. The information may be different when displayed on products that use a different version of ATT&CK™.

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

- Threat

- Virtual Analyzer risk level

YARA Detections

- YARA Rule File

- YARA Rules

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

- Anti-security, self-preservation

- Autostart or other system reconfiguration

- Deception, social engineering

- File drop, download, sharing, or replication

- Hijack, redirection, or data theft

- Malformation or other known malware traits

- Process, service, or memory object change

- Rootkit, cloaking

- Suspicious network or messaging activity

- Other notable characteristic

Affected Hosts Advanced Search Filter

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

- **Affected Hosts**

  For details, see *About Affected Hosts Advanced Search Filter on page 4-31*.

- **Affected Hosts - Host Details**

  For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-36*.

About Affected Hosts Advanced Search Filter

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

TABLE 4-14. Search Filter Criteria: Affected Hosts

ATTRIBUTE	OPERATOR	ACTION
Host Name	**Contains**/**Does not contain**/**Starts with**/**Equals**	Type a value
IP Address	**Contains**/**Does not contain**/**Equals**	Type a value
	In range/**Not in range**	Type a range
MAC Address	**In**/**Not in**	Type a value
Network Group	**Contains**/**Does not contain**/**Equals**	Type a value
Notable Events	**In**	Select one or more of the following: • **Targeted Attack** • **C&C Communication** • **Lateral Movement**

For details, see the following:

Adding an Affected Hosts Advanced Search Filter

Procedure

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

2. Select an attribute and an associated operator.

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

   • Type a value in the text box.

   • Select a value from the drop-down list.

> **Tip**
>
> Type a keyword to search a partial match.
>
> For details, see *About Affected Hosts Advanced Search Filter on page 4-31*.

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

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

5. Click **Apply**.

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

6. To save the search, do the following:

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

      The **Save As** dialog appears.

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

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

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

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

Editing an Affected Hosts Saved Search

Procedure

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

2. Select a saved search to edit.

3. To edit the saved search, do one of the following:

- Click the edit icon on the right side of the screen.

- Click **Advanced**

4. Select an attribute and an associated operator.

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

- Type a value in the text box.

- Select a value from the drop-down list.

Tip

Type a keyword to search a partial match.

For details, see *About Affected Hosts Advanced Search Filter on page 4-31*.

Note

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

---

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

7. Click **Apply**.

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

8. To save the edited saved search, click the **Save** icon and do one of the following:

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

- To save the edited saved search with a new name, select **Save as** and do the following:

a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

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

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

Deleting an Affected Hosts Saved Searches

Procedure

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

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

> **Note**
>
> Built-in filters cannot be deleted.

Importing Affected Hosts Saved Searches

Procedure

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

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

    The **Import To Saved Searches** dialog appears.

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

    The file is uploaded and validated.

4. Click **Import**.

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

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

Exporting Affected Hosts Saved Searches

Procedure

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

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

   The **Export Saved Searches** dialog appears.

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

   > **Note**
   >
   > Built-in filters cannot be exported.

4. Click **Export**.

   The saved searches file download begins.

About Affected Hosts - Host Details Advanced Search Filter

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

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

ATTRIBUTE	OPERATOR	ACTION
Peer Host	Contains/Does not contain/Starts with/Equals	Type a value
Peer IP Address	Contains/Does not contain/Equals	Type a value
	In range/Not in range	Type a range
Peer MAC Address	In/Not in	Type a value
Peer Network Group	Contains/Does not contain/Equals	Type a value
Peer IP Country/Region	In/Not in	Select one or more peer IP countries
User Account	Has user account/No user account	
	Contains/Does not contain	Type a value
Protocol	In/Not in	Select one or more protocols
Transport Layer Security (TLS)	Equals	Select one of the following: • **Over SSL/TLS** • **Not over SSL/TLS**
Direction	Equals	Select one of the following: • **Internal** • **External**
Threat/ Detection/ Reference	Contains/Does not contain/Starts with/Equals	Type a value
Detection Rule ID	In/Not in	Type a value
YARA Rule File Name	Has YARA rule file name/No YARA rule file name	

Attribute	Operator	Action
	Contains/Does not contain/Equals	Type a value
Correlation Rule ID (ICID)	**In/Not in**	Type a value
Detection Type	**In/Not in**	Select one or more of the following: • **Malicious Content** • **Malicious Behavior** • **Suspicious Behavior** • **Exploit** • **Grayware** • **Malicious URL** • **Disruptive Application** • **Correlated Incident**
Attack Phase	**In/Not in**	Select one or more of the following: • **Intelligence Gathering** • **Point of Entry** • **C&C Communication** • **Lateral Movement** • **Asset/Data Discovery** • **Data Exfiltration** • **Unknown Attack Phase**
Tactics	**Has tactics/No tactics**	

Attribute	Operator	Action
	In/Not in	Select one or more of the following: • **Initial Access** • **Execution** • **Persistence** • **Privilege Escalation** • **Defense Evasion** • **Credential Access** • **Discovery** • **Lateral Movement** • **Collection** • **Exfiltration** • **Command and Control** • **Impact**
URL Category	In/Not in	Select one or more URL categories: • **Adware** • **C&C Server** • **Disease Vector** • **Coin Miners** • **Illegal or Prohibited Content** • **Malicious Domain** • **Malware Accomplice** • **Phishing** • **Proxy Avoidance and Anonymizers** • **Ransomware** • **Scam** • **Spyware**

Attribute	Operator	Action
C&C List Source	In/Not in	Select one or more of the following: • **Global Intelligence** • **Virtual Analyzer** • **User-defined** • **Relevance Rule**
C&C Callback Address	Contains/Does not contain/Equals	Type a value
C&C Risk Level	In/Not in	Select one or more of the following: • **Low** • **Medium** • **High**
Virtual Analyzer Result	Has analysis results/No analysis results	
PCAP File	Has PCAP file/No PCAP file	
Is Targeted Attack Related	Equals	Select one of the following: • **Yes** • **No**
File Detection Type	In	Select one or more of the following: • **Highly Suspicious File** • **Heuristic Detection** • **Known Malware**
File Path/File Name	Has file name/No file name	
	Contains/Does not contain/Equals	Type a value
File SHA-1	Has file SHA-1/No file SHA-1/	
	Contains/Does not contain	Type a value

Attribute	Operator	Action
File SHA-256	Has file SHA-256/No file SHA-256	
	Contains/Does not contain	Type a value
Domain/URL	Has network object/No network object	
	Contains/Does not contain/Equals	Type a value
Suspicious Object/Deny List Entity/ User-Defined SO	Contains/Does not contain/Stars with/Equals	Type a value
Sender (Email)	Has sender/No sender	
	Contains/Does not contain/Equals	Type a value
Recipient (Email)	Has recipient/No recipient	
	Contains/Does not contain/Equals	Type a value
Message ID (Email)	Has message ID/No message ID	
	Contains/Does not contain	Type a value
Subject (Email)	Has subject/No subject	
	Contains/Does not contain	Type a value

For details, see the following:

Adding an Affected Hosts - Host Details Advanced Search Filter

Procedure

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

2. To display **Affected Hosts - Host Details**, do one of the following:

   - Click any detection link associated with an affected host.

- Click the IP address of an affected host.

Details about the host are displayed.

3. Click **Advanced**.

4. Select an attribute and an associated operator.

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

  - Type a value in the text box.

  - Select a value from the drop-down list.

> 💡 **Tip**
>
> Type a keyword to search a partial match.
>
> For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-36*.

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

---

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

7. Click **Apply**.

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

8. To save the search, do the following:

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

    The **Save As** dialog appears.

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

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

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

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

Editing an Affected Hosts - Host Details Saved Search

Procedure

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

2. To display **Affected Hosts - Host Details**, do one of the following:

    - Click any detection link associated with an affected host.

    - Click the IP address of an affected host.

    Details about the host are displayed.

3. Click the **Saved Searches** icon.

4. Select a saved search to edit.

5. To edit the saved search, do one of the following:

    - Click the edit icon on the right side of the screen.

    - Click **Advanced**

6. Select an attribute and an associated operator.

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

    - Type a value in the text box.

    - Select a value from the drop-down list.

> **Tip**
>
> Type a keyword to search a partial match.
>
> For details, see *About Affected Hosts - Host Details Advanced Search Filter on page 4-36*.

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

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

9. Click **Apply**.

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

10. To save the edited saved search, click the **Save** icon and do one of the following:

    • To save the edited saved search with the same name, select **Save**.

    • To save the edited saved search with a new name, select **Save as** and do the following:

    a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

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

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

Deleting an Affected Hosts - Host Details Saved Search

Procedure

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

2. To display **Affected Hosts - Host Details**, do one of the following:

- Click any detection link associated with an affected host.

- Click the IP address of an affected host.

Details about the host are displayed.

3. Click the **Saved Searches** icon.

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

> **Note**
>
> Built-in filters cannot be deleted.

Importing Affected Hosts - Host Details Saved Searches

Procedure

1. Go to **Detections** > **Affected Hosts** and click any detection link.

2. Click the **Saved Searches** icon.

3. Click **Import**.

The **Import To Saved Searches** dialog appears.

4. Click **Select** to locate the file containing the saved searches.

The file is uploaded and validated.

5. Click **Import**.

> **Note**
>
> - Only saved searches that were created on the Deep Discovery Director (Internal Network Analytics Version) **Affected Hosts - Host Details** screen can be imported.
>
> - Importing overwrites existing saved searches with the same names.

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

Exporting Affected Hosts - Host Details Saved Searches

Procedure

1. Go to **Detections** > **Affected Hosts** and click any detection link.

2. Click the **Saved Searches** icon.

3. Click **Export**.

The **Export Saved Searches** dialog appears.

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

> **Note**
>
> Built-in filters cannot be exported.

5. Click **Export**.

The saved searches file download begins.

Network Detections

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

By default, Deep Discovery Director (Internal Network Analytics Version) searches **Network Detections** by **Source Host**, **Destination Host** and **Interested Host**.

Display Options and Search Filters

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

TABLE 4-16. Display Options and Search Filters: Network Detections

FILTER OPTION	DESCRIPTION	
Detection severity	Filter options include the following detection severity settings:	
	High	Displays high severity detections
	Medium	Displays medium severity detections
	Low	Displays low severity detections
	Information al	Displays informational detections
	All detection severity levels	Displays all detections
Period	**Last 24 hours**	
	Last 7 days	
	last 14 days	
	Last 30 days	
	Last 60 days	
	Custom range	

Filter Option	Description
Data source	Select which appliances to include as data source.
Customize Columns	Customize the display by hiding or displaying columns.
Basic search	Search for an IP address or host name.
	Note Type a case-insensitive keyword in the basic search field to search a partial host match.

Saved Searches	Search by saved search criteria.
	
	The **Network Detections** view includes the following preset searches:
	
	  • **Threats**
	
	  • **Known Threats**
	
	  • **Potential Threats**
	
	  • **Email Threats**
	
	  • **Ransomware**
	
	  • **YARA Rule Detections**

Advanced Search	Search by user-defined criteria sets.
	
	Each set includes one or more of the following:
	
	  • Attributes
	
	  • Operators
	
	  • Associated values
	
	For details, see *Network Detections Advanced Search Filter on page 4-65*.

Viewing Network Detections

Procedure

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

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

3. Select a time period.

4. Select which appliances to include as data source.

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

TABLE 4-17. General Columns

COLUMN NAME	PRESELECTED
Timestamp	X
Data Source	X
Details	X
Source Host	X
Destination Host	X
Interested Host	X
Interested Network Group	
Peer Host	
Peer Network Group	
Peer IP Country/Region	
User Account	

Note

The default **Timestamp** and **Details** columns cannot be removed.

TABLE 4-18. Email Columns

COLUMN NAME	PRESELECTED
Sender	
Recipients	
Email Subject	

TABLE 4-19. Detection Information Columns

COLUMN NAME	PRESELECTED
Threat Description	X
Detection Name	X
Threat (Virtual Analyzer)	
Reference	
Detection Type	
Protocol	X
Transport Layer Security (TLS)	
Detection Severity	X
Attack Phase	X
Tactics	X
URL Category	
Direction	
Notable Object	X
YARA Rule File Name	

> **Note**
>
> The default **Threat Description** column cannot be removed.

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

   By default, Deep Discovery Director (Internal Network Analytics Version) searches **Network Detections** by **Source Host**, **Destination Host**, and **Interested Host**.

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

   Deep Discovery Director (Internal Network Analytics Version) provides the following built-in saved searches:

TABLE 4-20. Built-in Saved Searches

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

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

Name	Filter Options
Email Threats	Protocol options include the following: • IMAP4 • POP3 • SMTP
Ransomware	Detection name options include the following: • Ransomware-related detections
YARA Rule Detections	YARA Rule File Name: Has YARA rule file name

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

   For details, see *Network Detections Advanced Search Filter on page 4-65*.

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

Viewing Network Detections - Detection Details

Procedure

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

   Detection details about the event are displayed.

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

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

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

   • If a packet capture has been enabled and the detection matched a packet capture rule, click **Download** and then select **PCAP File**

to download a password protected ZIP archive containing the pcap file.

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

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

⚠ **Important**

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

The password for the zip archive is "virus".

---

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

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

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

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

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

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

⚠ **Important**

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

The password for the zip archive is "virus".

---

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

Network Detections - Detection Details

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

Network Detections - Detection Details - Connection Details

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

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

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

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

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

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

Network Detections - Detection Details - Detection Information

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

- Activity detected
- Attack phase
- Correlation Rule ID (ICID)
- Detection name
- Detection rule ID
- Detection severity
- Detection type
- Event class
- MITRE ATT&CK™ Framework
    - Tactics
    - Techniques

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

> **Important**
>
> MITRE information displayed on Deep Discovery Director (Internal
> Network Analytics Version) is based on ATT&CK™ v6. The information
> may be different when displayed on products that use a different version
> of ATT&CK™.

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

- Notable Object

- Protocol

- Reference

- Targeted attack campaign

- Targeted attack related

- Threat

- Threat description

- Timestamp

- URL category

- Virtual Analyzer risk level

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

TABLE 4-21. Detection Types

DETECTION TYPES	DESCRIPTION
Correlated Incident	Events/detections that occur in a sequence or reach a threshold and define a pattern of activity

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

Network Detections - Detection Details - Connection Summary

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

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

- Host details may include the following:

    - Host name

- IP address and port

- Last logon user

- MAC address

- Network group

- Network zone

- Operating system

Network Detections - Detection Details - Protocol Information

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

- BOT command

- BOT URL

- Certificate Information

    - Issued To

        - Common name

        - Organization

        - Organizational unit

    - Issued By

        - Common name

        - Organization

        - Organizational unit

- Domain name

- Host name

- HTTP referer

- ICMP code

- ICMP type

- IRC channel name

- IRC nick name

- Message ID

- Protocol

- Queried domain

- Recipients

- Sender

- SNI host name

- Subject

- Target share

- Transport Layer Security (TLS)

- URL

- User agent

- User name

Network Detections - Detection Details - File Information

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

- File name

- File SHA-1

- File SHA-256

- File size

Network Detections - Detection Details - Additional Information

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

- Attempted to disrupt connection

- Detected by

- Mitigation

- Fingerprinting

    - JA3 hash value

    - JA3S hash value

- VLAN ID

Network Detections - Detection Details - File Analysis Result

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

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

- *Network Detections - Detection Details - File Analysis Result - YARA Rule Detections on page 4-62*

- *Network Detections - Detection Details - File Analysis Result - Notable Characteristics on page 4-62*

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

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

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

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

> ⚠ **Important**
>
> Suspicious files must always be handled with caution. Extract the detected file at your own risk.
>
> The password for the zip archive is "virus".

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

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

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

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

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

- Tactics

- Techniques

Tip

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

Important

MITRE information displayed on Deep Discovery Director (Internal Network Analytics Version) is based on ATT&CK™ v6. The information may be different when displayed on products that use a different version of ATT&CK™.

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

- Threat

- Virtual Analyzer risk level

Network Detections - Detection Details - File Analysis Result - YARA Rule Detections

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

- YARA Rule File

- YARA Rules

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

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

- Anti-security, self-preservation

- Autostart or other system reconfiguration

- Deception, social engineering

- File drop, download, sharing, or replication

- Hijack, redirection, or data theft

- Malformation or other known malware traits

- Process, service, or memory object change

- Rootkit, cloaking

- Suspicious network or messaging activity

- Other notable characteristic

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

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

Network Detections - Detection Details - Suspicious Object Information

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

- Related analyzed file

- Virtual Analyzer risk level

- Suspicious object

- Type

Network Detections - Detection Details - Related Analyzed File Information

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

- Child objects
    - File name
    - File size (bytes)
    - Type

- File SHA-1
- File SHA-256

- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- MITRE ATT&CK™ Framework

  - Tactics
  - Techniques

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

> ⚠️ **Important**
>
> MITRE information displayed on Deep Discovery Director (Internal Network Analytics Version) is based on ATT&CK™ v6. The information may be different when displayed on products that use a different version of ATT&CK™.

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

- Threat
- Virtual Analyzer risk level

YARA Detections

- YARA Rule File

- YARA Rules

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

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

Network Detections Advanced Search Filter

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

TABLE 4-22. Search Criteria: Network Detections

ATTRIBUTE	OPERATOR	ACTION
Host Name	**Contains**/**Does not contain**/**Starts with**/**Equals**	Type a value
Interested Host	**Contains**/**Does not contain**/**Starts with**/**Equals**	Type a value
Peer Host	**Contains**/**Does not contain**/**Starts with**/**Equals**	Type a value
IP Address	**Contains**/**Does not contain**/**Equals**	Type a value
	In range/**Not in range**	Type a range

ATTRIBUTE	OPERATOR	ACTION
Interested IP Address	Contains/Does not contain/Equals	Type a value
	In range/Not in range	Type a range
Peer IP Address	Contains/Does not contain/Equals	Type a value
	In range/Not in range	Type a range
Peer IP Country/Region	In/Not in	Select one or more peer IP countries
MAC Address	In/Not in	Type a value
Network Group	Contains/Does not contain/Equals	Type a value
User Account	Has user account/No user account	
	Contains/Does not contain	Type a value
Protocol	In/Not in	Select one or more protocols
Transport Layer Security (TLS)	Equals	Select one of the following: • **Over SSL/TLS** • **Not over SSL/TLS**
Direction	Equals	Select one of the following: • **Internal** • **External**
Threat/ Detection/ Reference	Contains/Does not contain/Equals	Type a value
Detection Rule ID	In/Not in	Type a range
YARA Rule File Name	Has YARA rule file name/No YARA rule file name	
	Contains/Does not contain/Equals	Type a value

ATTRIBUTE	OPERATOR	ACTION
Correlation Rule ID (ICID)	**In**/**Not in**	Type a value
Detection Type	**In**/**Not in**	Select one or more of the following: • **Malicious Content** • **Malicious Behavior** • **Suspicious Behavior** • **Exploit** • **Grayware** • **Malicious URL** • **Disruptive Application** • **Correlated Incident**
Attack Phase	**In**/**Not in**	Select one or more of the following: • **Intelligence Gathering** • **Point of Entry** • **C&C Communication** • **Lateral Movement** • **Asset/Data Discovery** • **Data Exfiltration** • **Unknown Attack Phase**
Tactics	**Has tactics**/**No tactics**	

ATTRIBUTE	OPERATOR	ACTION
	In/**Not in**	Select one or more of the following: • **Initial Access** • **Execution** • **Persistence** • **Privilege Escalation** • **Defense Evasion** • **Credential Access** • **Discovery** • **Lateral Movement** • **Collection** • **Exfiltration** • **Command and Control** • **Impact**
URL Category	**In**/**Not in**	Select one or more URL categories
C&C List Source	**In**/**Not in**	Select one or more of the following: • **Global Intelligence** • **Virtual Analyzer** • **User-defined** • **Relevance Rule**
C&C Callback Address	**Contains**/**Does not contain**	Type a value
C&C Risk Level	**In**/**Not in**	Select one or more of the following: • **Low** • **Medium** • **High** • **Unknown**

Attribute	Operator	Action
Virtual Analyzer Result	**Has analysis results**/**No analysis results**	
PCAP File	**Has PCAP file**/**No PCAP file**	
Is Targeted Attack Related	**Equals**	Select one of the following: • **Yes** • **No**
File Detection Type	**In**	Select one or more of the following: • **Highly Suspicious File** • **Heuristic Detection** • **Known Malware**
File Path/File Name	**Has file name**/**No file name**	
	Contains/**Does not contain**/**Equals**	Type a value
File SHA-1	**Has file SHA-1**/**No file SHA-1**/	
	Contains/**Does not contain**	Type a value
File SHA-256	**Has file SHA-256**/**No file SHA-256**	
	Contains/**Does not contain**	Type a value
Domain/URL	**Contains**/**Does not contain**/**Equals**	Type a value
Suspicious Object/Deny List Entity/ User-Defined SO	**Contains**/**Does not contain**/**Starts with**/**Equals**	Type a value
Sender (Email)	**Has sender**/**No sender**	
	Equals/**Contains**/**Does not contain**	Type a value
Recipient (Email)	**Has recipient**/**No recipient**	
	Equals/**Contains**/**Does not contain**	Type a value

Attribute	Operator	Action
Message ID (Email)	Has message ID/No message ID	
	Contains/Does not contain	Type a value
Subject (Email)	Has subject/No subject	
	Contains/Does not contain	Type a value

For details, see the following:

Adding a Network Detections Advanced Search Filter

Procedure

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

2. Select an attribute and an associated operator.

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

    • Type a value in the text box.

    • Select a value from the drop-down list.

    > **Tip**
    >
    > Type a keyword to search a partial match.
    >
    > For details, see *Network Detections Advanced Search Filter on page 4-65*.

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

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

5. Click **Apply**.

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

6. To save the search, do the following:

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

      The **Save As** dialog appears.

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

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

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

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

Editing a Network Detections Saved Search

Procedure

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

2. Select a saved search to edit.

3. To edit the saved search, do one of the following:

   • Click the edit icon on the right side of the screen.

   • Click **Advanced**

4. Select an attribute and an associated operator.

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

- Type a value in the text box.

- Select a value from the drop-down list.

💡 **Tip**

Type a keyword to search a partial match.

For details, see *Network Detections Advanced Search Filter on page 4-65*.

📝 **Note**

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

---

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

7. Click **Apply**.

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

8. To save the edited saved search, click the **Save** icon and do one of the following:

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

   - To save the edited saved search with a new name, select **Save as** and do the following:

   a. In the **Save as** dialog that appears, type a name and an optional description, and then click **Save**.

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

📝 **Note**

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

---

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

Deleting a Network Detections Saved Search

Procedure

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

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

> **Note**
>
> Built-in filters cannot be deleted.

Importing Network Detections Saved Searches

Procedure

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

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

The **Import To Saved Searches** dialog appears.

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

The file is uploaded and validated.

4. Click **Import**.

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

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

Exporting Network Detections Saved Searches

Procedure

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

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

   The **Export Saved Searches** dialog appears.

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

   > **Note**
   >
   > Built-in filters cannot be exported.

4. Click **Export**.

   The saved searches file download begins.

Email Messages

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Quarantined Messages

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Correlated Events

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

Display Options and Search Filters

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

TABLE 4-23. Display Options and Search Filters: Correlated Events

FILTER OPTION	DESCRIPTION	
Severity	Filter options include the following severity settings:	
	High	Displays high severity events
	Medium	Displays medium severity events
	Low	Displays low severity events
	All	Displays all events
Period	**Last 24 hours**	
	Last 7 days	
	last 14 days	
	Last 30 days	

FILTER OPTION	DESCRIPTION		
	Last 60 days		
	Custom range		
Attack Pattern	Filter options include the following attack patterns:		
	All attack patterns	Displays all events	
	Brute Force Authenticati on	Displays events with brute force authentication attack patterns	
	C&C Callback	Displays events with C&C callback attack patterns	
	Data Exfiltration	Displays events with data exfiltration attack patterns	
	Lateral Movement	Displays events with lateral movement attack patterns	
	Malicious Transfer	Displays events with malicious transfer attack patterns	
	Other Malicious Activities	Displays events with malicious activity attack patterns	
	Vulnerabilit y Exploit	Displays events with vulnerability exploit attack patterns	
Basic search	Search for an interested IP address.		

Viewing Correlated Events

Procedure

1. Go to **Detections** > **Correlated Events**.

   The **Correlated Events** screen appears.

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

3. Select the attack patterns by using the drop-down control.

4. Select a time period.

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

Viewing Correlated Events - Correlation Data

Procedure

1. To view correlation data, click the **Correlation Data** icon (✂) under **Details** on the **Correlated Events** screen.

   > **Note**
   >
   > The **Correlation Data** icon is grayed out when correlation data is unavailable.

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

   - **Summary**

     Displays the severity, the number of detected internal hosts and Indicators of Compromise (IOCs), the assigned attack patterns, and provides a high-level overview of the malicious activity of the correlation data.

   - **Correlation Graph**

     Provides a visual representation of correlations made between the correlated event selected in Deep Discovery Director and other related events as they occurred over time.

   - **Transaction and IOC Details**

     Provides details about each transaction represented in the correlation graph, and each detected Indicator of Compromise (IOC). Transactions are listed from oldest transaction at the top to

the most recent transaction at the bottom. IOCs are listed from oldest first seen at the top to the most recent first seen at the bottom.

> **Tip**
>
> - Information displayed in the **Correlation Data** screen is created dynamically. The number of correlations and details about interactions and malicious activity between hosts presented in this screen can change over time. You can access the correlation data for a specific detection at a later time to see if additional analysis details are available.
>
> - When Deep Discovery Director (Internal Network Analytics Version) is integrated with more than one Deep Discovery Director (Internal Network Analytics Version) server operating in Deep Discovery Director (Standalone Network Analytics Mode), multiple sets of correlation data may exist for a single correlated event. Switch between the correlation data generated by each Deep Discovery Director (Standalone Network Analytics Mode) server by clicking on the **Network Analytics** server display name and IP address and selecting the desired server.

3. For details on how to use the information displayed in the **Correlation Data** screen to assist in advanced analysis, see *Analyzing Correlation Data Information on page 4-78*.

Analyzing Correlation Data Information

Learn how to use the information displayed in the **Correlation Data** screen to assist in advanced analysis in the following topics.

Overview of the Correlation Data Screen

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

- **Summary**

- **Correlation Graph**

- **Transaction and IOC Details**

Summary

The **Summary** section displays the severity, the number of detected internal hosts and Indicators of Compromise (IOCs), and the attack patterns, and provides a high-level overview of the malicious activity of the correlated event.

To export the correlation data of this correlated event, click **Export** and then select **Printer-friendly** or **CSV**.

Click on the help icon (ⓘ) and then select **Tutorial** to display an on-screen tutorial that describes each section of the **Correlation Data** screen step-by-step. Use **Next** and **Back** to navigate the tutorial, or click **Skip** to end it immediately.

The **Summary** section can be collapsed and expanded by clicking on the collapse (⌃) and expand icons (⌄).

See *Reviewing the Summary on page 4-80*.

Correlation Graph

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

Click on the filter icon (▼) located next to the **Playback Bar** to display or hide the advanced search filter.

See *Analysis Using the Correlation Graph on page 4-83*.

Transaction and IOC Details

The **Transaction and IOC Details** section provides details about each transaction represented in the correlation graph, and each detected Indicator of Compromise (IOC)

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. IOCs are listed from oldest first seen at the top to the most recent first seen at the bottom.

The **Transaction and IOC Details** section can be collapsed and expanded by clicking on the collapse (>) and expand icons (<).

See *Analysis Using the Transaction and IOC Details on page 4-98*.

Reviewing the Summary

The **Summary** section displays the severity, the number of detected internal hosts and Indicators of Compromise (IOCs), and the attack patterns, and provides a high-level overview of the malicious activity of the correlated event.

Procedure

1. Review the severity, detection counts, attack patterns, and activity summary.

Severity	The severity assigned by Deep Discovery Director - Network Analytics to the event and related correlations. Deep Discovery Director - Network Analytics uses a number of factors to assign severity, including proprietary analysis.
Internal Hosts and Indicators of Compromise detection count	The detection count numbers allow you to quickly determine the scope of the correlated event.
Attack patterns	The attack patterns for the correlated event or suspicious object selected in Deep Discovery Director.

Activity summary	The activity summary is broken up by attack pattern and provides the following information:
	• Protocols on which activities were detected.
	• Number of detected Suspicious Objects (SOs) and Indicators of Compromise (IOCs).
	• Hosts which were involved in suspicious or malicious activity. Activity might be between internal hosts and external servers or might include lateral activity between internal hosts. Internal hosts are defined by the **Network Groups** list. **Note** • To provide an accurate analysis of correlation data, it is important to specify your internal networks and hosts in the **Network Groups** list. • By default, private networks are considered trusted and are set internally as trusted. You only need to add non-private IP addresses to the **Network Groups** list.
	• The activity with the **Trigger Event** label is the focal point of this correlated event and contains the IP address found in the **Interested Host** field of the **Correlated Events** screen.
	• Additional hosts that participated in the suspicious activity.
	• Additional suspicious objects when viewing correlation data for suspicious objects.

2. (Optional) Perform one of the following actions on individual summary items:

ITEM	ACTION
Internal Hosts detection number	Click the detection number and then click on the **Copy to clipboard** icon (🗐) to copy the entire list to your clipboard, or click on the **Focus** icon (🔍) to focus on the item in the **Correlation Graph**.

ITEM	ACTION
Indicators of Compromise detection number	Click the detection number and then click on the **Copy to clipboard** icon (🗒) to copy the value to your clipboard.
Attack patterns	Hover over an attack pattern to highlight only activities related to that attack pattern in the summary.
IP addresses and domains	Hover over the triangle icon (▼) and select one of the following: • **Focus**: Focus on the item in the **Correlation Graph**. • **Copy to clipboard**: Copy the value to your clipboard. • **View network detection events**: Open the **Network Detections** screen in a new browser tab with filters matching this object applied. • **Threat Connect**: Open **Trend Micro Threat Connect** in a new browser tab with a query for this object. • **DomainTools (WHOIS)**: Open **DomainTools** in a new browser tab with a query for this IP address or domain. • **VirusTotal**: Open **VirusTotal** in a new browser tab with a query for this object.

3. (Optional) Click **Export** and then select one of the following options to export the correlation data of this correlated event.

   • **Printer-friendly**: Displays your system's printer dialog. Modify settings and then click **Print**.

   • **CSV**: Select a delimiter and then click **Export** to export and download the correlation data of this correlated event to a CSV file with the chosen delimiter.

   Note

   If any advanced search filter is applied, export is limited to the currently filtered correlation data.

Analysis Using the Correlation Graph

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

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

Procedure

- From the main screen, perform initial analysis:

ELEMENT IN CORRELATION GRAPH

FIGURE 4-1. Playback Bar / Time Slider
 	
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.
 	
Use the time line sliders to view correlated events over a selected time frame. The graph displays only the correlations within the selected time frame.
 	
  • Adjust the time frame by clicking on the left and right grab bars on the time line and dragging them to the desired location.
 	
  • To move the entire time frame, click inside the current time frame and drag the frame toward the left or the right.
 	
  • The correlations displayed in the graph (and resultant transaction details) change according to event data found within the selected time frame.

Click on the filter icon (▼) located next to the **Playback Bar** to display or hide the advanced search filter. Use the advanced search filter to create and apply customized searches. For details, see *Correlation Graph Advanced Search Filter on page 4-88*.

Element in Correlation Graph
Correlation Line Each correlation graph contains one or more correlation lines that correlate malicious or suspicious activity between a source and destination. • Each correlation line represents one or more transactions between two hosts. • The thickness of the line is proportional to the number of transactions occurring between the hosts. • Correlation lines can be between an internal host and external server or between two internal hosts (lateral movement). • Each correlation line is labeled with the protocols used in transactions between the hosts. An arrow within the correlation line indicates the direction of the transactions, from source to destination.   Correlation lines involving email senders are labeled as **Suspicious Email Activity**.

ELEMENT IN CORRELATION GRAPH

Internal hosts

- Internal hosts are identified by IP address; the host name and logged on user are also supplied if known.

  Icons representing relevant information might be displayed next to an internal host. For example, if the internal host is on the priority watch list or on a registered service list, the graph displays the appropriate icon.

- Hover over the downward triangle icon (▼) located next to each internal host and external server to view a list of additional actions you can perform for that host.

    - **Copy to clipboard**: Copy the value to your clipboard.

    - **View network detection events**: Open the **Network Detections** screen in a new browser tab with filters matching this object applied.

- Deep Discovery Director attempts to retrieve an endpoint analysis report for hosts on the priority watch list and for the host that is the Interested IP in the trigger event. If there is a report, the icon is located beneath the internal host. Click on the **Endpoint Analysis Report** icon (🔍 Endpoint Analysis Report) to open the report provided by Apex Central.

    > **Note**
    >
    > - Deep Discovery Director must be integrated with Apex Central before the **Endpoint Analysis Report** icon becomes available in the correlation graph.
    >
    >   For details, see *Configuring Apex Central Settings on page 9-11*.

ELEMENT IN CORRELATION GRAPH

External servers
 	
 • External servers are identified by IP address; the domain name is also supplied if known.
 	
   Email senders are identified by email address and are always displayed at the top of the **External Servers** side.
 	
   Other relevant information might be displayed for external hosts.
 	
 • Hover over the downward triangle icon () located next to each external server to view a list of additional actions you can perform for that host.
 	
      • **Copy to clipboard**: Copy the value to your clipboard.
 	
      • **View network detection events**: Open the **Network Detections** screen in a new browser tab with filters matching this object applied.
 	
      • **Threat Connect**: Open **Trend Micro Threat Connect** in a new browser tab with a query for this object.
 	
      • **DomainTools (WHOIS)**: Open **DomainTools** in a new browser tab with a query for this IP address or domain.
 	
      • **VirusTotal**: Open **VirusTotal** in a new browser tab with a query for this object.

Special Icons
 	
 Additional icons provide information about elements in the correlation graph.
 	
 • **Priority Watch List** icon:
 	
 • **Endpoint Analysis Report** icon: Endpoint Analysis Report
 	
   Deep Discovery Director attempts to retrieve an endpoint analysis report for hosts on the priority watch list and for the host that is the Interested IP in the trigger event. If there is a report, the icon is located beneath the internal host.
 	
   Deep Discovery Director (Consolidated Mode) retrieves the report from Apex Central, which is integrated with Apex One. Apex One provides the endpoint sensor feature.
 	
   There are several statuses for retrieving the report:

Element in Correlation Graph

Legend

Provides a list of icons used in the correlation graph, including the following:

- The color of the correlation line for the interested host

- Whether the graph contains hosts on the priority watch list

- Registered services icons indicating that the hosts in the graphs are members of that list
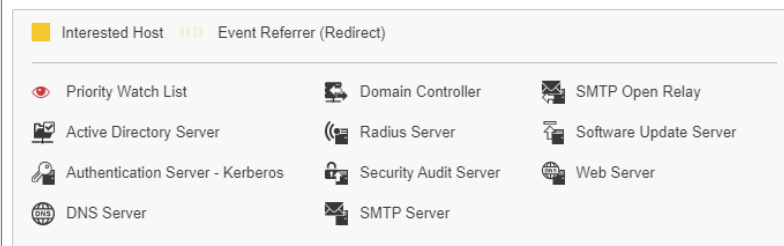
Figure 4-2. Legend

Interested Host

Represents the focal point of this correlated event.

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

> **Note**
>
> Suspicious Object detections selected from Deep Discovery Director generally do not generate a **Interested Host** correlation.

Element in Correlation Graph
Activity Legend   Identifies key activities for the internal host and external server participants in the graph.   • Activities vary for each specific correlation graph.   • Can include activities similar to the following: Brute Force Authentication, C&C Callback, Data Exfiltration, Lateral Movement, Malicious Transfer, Other Malicious Activities, and Vulnerability Exploit.   • Some activities correspond to "Reason" in Deep Discovery Inspector logs.
Participant Icons   You can determine the activities in which each internal host or external server participated by checking the presence of an icon in the corresponding activity column.   Hover over an internal host or external server to see the activities in which they are participants highlighted in blue.

Correlation Graph Advanced Search Filter

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

The following table outlines the actions available for the advanced search filter.

Action	Description
Toggle panel visibility	Click on the filter icon (▼) located next to the **Playback Bar** to display or hide the advanced search filter.
Apply a saved search filter	With the advanced search filter panel displayed, click on the **Saved Search** drop-down list (☰) and then select a saved advanced search filter to apply to the **Correlation Graph**.
Add an advanced search filter	With the advanced search filter panel displayed, add an advanced search filter to apply to the **Correlation Graph**. For details, see *Adding a Correlation Graph Advanced Search Filter on page 4-89*.

Action	Description
Save an advanced search filter	With any filter applied and the advanced search filter panel hidden, click the **Save** icon (■), and then select **Save** or **Save as** to save the advanced search filter.
Edit an advanced search filter	With any filter applied and the advanced search filter panel hidden, click the **Edit** icon (✎) to display the advanced search filter panel, and then edit the search criteria. Click the **Save** button (■) and select **Save** to save the advanced search filter.
Clear filter	With any advanced search filter applied, click the **Clear** icon (✕) to clear the advanced search filter.

Adding a Correlation Graph Advanced Search Filter

Procedure

1. To create an **Correlation Graph** advanced search filter, go to **Detections** > **Correlated Events**, and then click on the **Correlation Data** icon (⚛) under **Details**.

2. Click on the filter icon (▼) located next to the **Playback Bar** to display the advanced search filter.

3. Select an attribute and an associated operator.

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

    - Type a value in the text box.

    - Select a value from the drop-down list.

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

For details, see *Network Detections Advanced Search Filter on page 4-65*.

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

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

6. Click **Apply**.

    The **Correlation Graph** is updated and displays data filtered by the search criteria. All search criteria sets are displayed above the **Correlation Graph**.

7. Click the **Save** button (🖪) and select **Save as**.

    The **Save As** dialog appears.

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

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

Endpoint Analysis Reports - Status Details

The **Endpoint Analysis Report** icon can display the following statuses:

TABLE 4-24. Endpoint Analysis Report - Status Details

Icon	Message	Description
Endpoint Analysis Report	Report retrieved on <date + time>.	The report was retrieved with new data and is ready to open.
		The report was retrieved with existing data and is ready to open.
		The retrieval of existing data is pending.

Icon	Message	Description
(i) Endpoint Analysis Report	There is no correlational report for this host.	There is no correlation report with new data for this host. Additionally, an existing report does not exist.
⚠ Endpoint Analysis Report	Cannot retrieve latest correlational report. [Error code]	You can click to open existing report.
⚠ Endpoint Analysis Report	Cannot retrieve correlational report. [Error code]	There is no data to retrieve.
(i) Retrieving Endpoint...	Retrieving Endpoint Analysis Report. Please wait.	There is a report to retrieve.
	Report retrieval failed. Trying to retrieve report again. [Error code]	Deep Discovery Director is trying to retrieve the report again.

The following table describes the error codes that can appear and how to resolve the issues.

TABLE 4-25. Error Code Descriptions and Solutions

Error Code	Description	Solution
4	Retrieval of the Endpoint Analysis Report has timed out.	Verify that there are no connection issues between Deep Discovery Director (Internal Network Analytics Version), Deep Discovery Director - Network Analytics as a Service, and Trend Micro Apex Central.
11352		
11356		
11351	Trend Micro Apex Central encountered an unexpected error.	Verify that Trend Micro Apex Central works normally.
11353	The Endpoint Sensor license is invalid.	Verify that the Endpoint Sensor license status is normal on Trend Micro Apex Central.

Error Code	Description	Solution
11354	Trend Micro Apex Central could not find the target endpoint.	Verify that Endpoint Sensor and installation of security agents are enabled in Trend Micro Apex Central.
11355	The operating system of the endpoint is not supported.	None. Endpoint Analysis Reports can only be generated on endpoints running Windows operating systems.

Endpoint Analysis Report

The criteria that were used to generate the endpoint analysis report are displayed at the top of the screen.

> **Tip**
> Click the down-arrow icon in the title bar to hide or display the criteria.

The endpoint analysis report includes the following tabs:

Analysis Chains

The **Analysis Chains** tab displays the root cause analysis and also highlights additional information which might be beneficial to the investigation.

Information	Description
Target Endpoint	Displays details about the endpoint where the root cause chain occurred.
First Observed Object	Object that most likely created the matched object. This is often the entry point of a targeted attack. Hover over an object and click 🔍 to locate the object in the root cause analysis.

INFORMATION	DESCRIPTION
Matched Objects	Displays the object or a list of objects matching the investigation criteria.
	Hover over an object and click $\mathbb{Q}$ to locate the object in the root cause analysis.
Noteworthy Objects	Highlights objects in the chain that are possibly malicious, based on existing Trend Micro intelligence.
	The value counts the number of unique noteworthy objects in the chain.
	Hover over the value to view the list of noteworthy objects.
	Hover over an object and click $\mathbb{Q}$ to locate the object in the root cause analysis.
Root cause analysis area	Displays the root cause analysis map.

The root cause analysis area displays a visual analysis of the objects involved in an event.

Note

If the number of nodes in the root cause chain exceeds the presentation limit, only the main root cause chains are displayed.

To move around, click and drag the area to your preferred direction. This area also provides the following navigation options.

2 matched chains : Chain 1: 2018/08/06 13:24:09 ▾	A root cause analysis can contain one or more matched root cause chains.
	Click the drop down to view other root cause chains for the selected endpoint.

⬈ symbol	Click to enter full screen mode. Click again to exit full screen mode.
+ − symbol	Click to zoom in or zoom out.
i symbol	Hover to view an explanation of the symbols appearing in the root cause chain.

Hover over an object in the root cause analysis area to view additional details. Click an object to display a side panel with the following tabs:

- The **Profile** tab shows the details applicable for the selected object type.

  Some objects may show only a limited set of details, or may not have any details available at the time of execution.

  The tab also displays additional options for **Matched Objects** and **Noteworthy Objects**:

  - **Add to Suspicious Objects List**: Adds the object to the **User-Defined Suspicious Object** list. The following object types can be added to the list:

    - IP addresses

    - URLs

    - File SHA-1

- Domains

- The **Related Objects** tab displays all the dependencies of the matched object.

  These are the objects required to run the matched object. This tab displays the following details:

PROPERTY	DESCRIPTION
Action	Action done by the object.
Logged	Date and time of the recorded action.
Rating	Rating assigned to the object based on Trend Micro intelligence.
Destination path	Target destination of the object.

The following options are available to manage the **Related Objects** tab:

- The tab provides a drop down that can filter objects based on the specified action. Click the drop down to view all available actions.

- Click **Show detail** to view more details about the object.

Root Cause Analysis Icons

The analysis chain shows object types using the following icons:

ICON	NAME	DESCRIPTION
	First Observed Object	Marks an object that most likely created the matched object
	Matched Criteria	Marks objects matching the investigation criteria
	Normal Object	Marks objects that have been verified to not pose a threat These are usually common system files.
	Unrated Object	Marks objects that have not yet been rated

ICON	NAME	DESCRIPTION
●	Suspicious Object	Marks objects that exhibit behaviors that are similar to known threats
●	Malicious Object	Marks objects that match a known threat
⏻	Boot	Objects that launch during system startup
▣	Browser	Objects that are capable of displaying web pages, usually a web browser
✉	Email client	Objects that can send and receive email messages, usually an email client or server
⊛	Email message	Objects identified through use of the Cloud App Security integration email correlation feature
📄	File	Objects that are files on the disk
🌐	Network	Objects related to network connections or the Internet
⚙	Process	Objects that are processes running during the time of execution
▦	Registry	Objects that are registry keys, entries or data
→	Event	Indicates actions done by the object
---	Association	Indicates relationships between two objects

Object Details

The **Object Details** tab presents information as a table. It also organizes the objects into the following tabs:

- **Objects**: Objects involved in the execution of the matched object, grouped by their parent processes. Click ▶ to expand the list.

- **Noteworthy objects**: Objects in the chain that are possibly malicious, based on existing Trend Micro intelligence

- **File events**: Objects in the chain that are files

- **Registry events**: Objects in the chain that are registry keys, data and entries

- **IP address / DNS events**: Objects that are IP addresses or DNS events

The table provides the following details:

Column	Description
Recorded Object	Name of the recorded object. Click the object name to view more details.
PID	Process ID of the recorded object.
Recorded	Date and time when the object became involved in the chain.
Activity	Action done by the object. Click the object name to view more details.
Object Reputation	Rating assigned to the object based on Trend Micro intelligence.

Use the following options to manage the table:

- On the **Objects** tab, click the filter icon (▼) to filter the table according to the specified criteria.

- On the **Noteworthy Objects**, **File events**, **Registry Events**, and **IP Address / DNS events** tabs, sort the table by clicking on the **Recorded** and **Object Reputation** columns.

Analysis Using the Transaction and IOC Details

The **Transaction and IOC Details** section provides information about transactions and IOCs from the **Correlation Graph** section.

The oldest transactions are listed first. IOCs are listed by highest risk level first and then by first seen time.

Procedure

- Scroll through the **Transactions** and **IOCs** lists to identify information useful for analysis.

- Click on a correlation line in the **Correlation Graph** section to display a summary and to filter and limit the transactions and IOCs that are displayed in the **Transaction and IOC Details** section to ones that are directly related to the selected correlation line.

   > **Tip**
   >
   > Click on an empty space in the **Correlation Graph** section to remove the filter.

- Click on an internal host, external server, or email sender in the **Correlation Graph** section to display details about the selected internal host, external server, or email sender in the **Transaction and IOC Details** section.

   > **Tip**
   >
   > Click on an empty space in the **Correlation Graph** section to revert the **Transaction and IOC Details** section back to normal.

- Perform one of the following actions on **Transaction and IOC Details** section items:

Item	Action
IP addresses, domains, URLs, and hash values	Hover over the triangle icon (▼) and select one of the following:
	Note Depending on the location of the item on the screen, not all actions may be available.
	• **Focus**: Focus on the item in the **Correlation Graph**. • **Copy to clipboard**: Copy the value to your clipboard. • **View network detection events**: Open the **Network Detections** screen in a new browser tab with filters matching this object applied. • **Threat Connect**: Open **Trend Micro Threat Connect** in a new browser tab with a query for this object. • **DomainTools (WHOIS)**: Open **DomainTools** in a new browser tab with a query for this IP address or domain. • **VirusTotal**: Open **VirusTotal** in a new browser tab with a query for this object.
Deep Discovery Inspector rules	Click on a rule with a hyperlink to open the **Trend Micro Threat Encyclopedia** page for that rule in a new browser tab.

Viewing Correlated Events - Detection Details

Procedure

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

> **Note**
>
> The **Details** icon may not appear because:
>
> - The related detection logs have been purged
> - The current user account's role cannot see and manage appliances with related detections
> - Appliances with related detections have been moved to the **Unmanaged** group
> - Appliances with related detections have been unregistered from Deep Discovery Director (Internal Network Analytics Version)

Detection details about the event are displayed.

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

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

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

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

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

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

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

> **!** **Important**
>
> Suspicious files must always be handled with caution. Extract the detected file and pcap file at your own risk.
>
> The password for the zip archive is "virus".

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

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

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

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

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

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

> **!** **Important**
>
> Suspicious files must always be handled with caution. Extract the detected file at your own risk.
>
> The password for the zip archive is "virus".

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

Correlated Events - Detection Details

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

Correlated Events - Detection Details - Connection Details

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

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

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

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

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

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

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

Correlated Events - Detection Details - Detection Information

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

- Activity detected

- Attack phase

- Correlation Rule ID (ICID)

- Detection name

- Detection rule ID

- Detection severity

- Event class

- Notable Object

- Protocol

- Reference

- Targeted attack campaign

- Targeted attack related

- Threat

- Threat description

- Detection type

- Timestamp

- URL category

- Virtual Analyzer risk level

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

TABLE 4-26. Detection Types

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

Correlated Events - Detection Details - Connection Summary

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

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

- Host details may include the following:

    - Host name

    - IP address and port

    - Last logon user

    - MAC address

    - Network group

    - Network zone

    - Operating system

Correlated Events - Detection Details - Protocol Information

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

- BOT command

- BOT URL

- Domain name

- Host name

- HTTP referer

- ICMP code

- ICMP type

- IRC channel name

- IRC nick name

- Message ID

- Protocol

- Queried domain

- Recipients

- Sender

- Subject

- Target share

- Transport Layer Security (TLS)

- URL

- User agent

- User name

Correlated Events - Detection Details - File Information

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

- File name

- File SHA-1

- File SHA-256

- File size

Correlated Events - Detection Details - Additional Information

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

- Attempted to disrupt connection

- Detected by

- Mitigation

- VLAN ID

Correlated Events - Detection Details - File Analysis Result

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

- *Correlated Events - Detection Details - File Analysis Result - File Information on page 4-108*

- *Correlated Events - Detection Details - File Analysis Result - Notable Characteristics on page 4-108*

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

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

💡 **Tip**

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

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

⚠ **Important**

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

The password for the zip archive is "virus".

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

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

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

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

- Child objects
    - File name / URL
    - File size (bytes)
    - Type
    - File SHA-1
    - File SHA-256
- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- Threat
- Virtual Analyzer risk level

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

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

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- Deception, social engineering
- File drop, download, sharing, or replication

- Hijack, redirection, or data theft

- Malformation or other known malware traits

- Process, service, or memory object change

- Rootkit, cloaking

- Suspicious network or messaging activity

- Other notable characteristic

Correlated Events - Detection Details - Suspicious Object and Related File Analysis Result

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

- *Correlated Events - Detection Details - Suspicious Object Information on page 4-109*

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

Correlated Events - Detection Details - Suspicious Object Information

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

- Related analyzed file

- Virtual Analyzer risk level

- Suspicious object

- Type

Correlated Events - Detection Details - Related Analyzed File Information

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

- Child objects

- File name
- File size (bytes)
- Type
- File SHA-1
- File SHA-256

- File name
- File size
- File type
- File MD5
- File SHA-1
- File SHA-256
- Threat
- Virtual Analyzer risk level

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

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

Ignore Rules

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

Ignore Rules Tasks

Task	Steps
Create an ignore rule	Ignore rules are created using the **Network Detections** or **Email Messages Advanced Search** filter. For details, see *Creating an Ignore Rule on page 4-111*.
View rule details	Hover on any text in the **Criteria** or **Description** columns to view the details of the ignore rule.
Delete rule	Select one or more ignore rules to delete and then click **Delete**.
Toggle rule status	Click on the toggle in the **Status** column to enable or disable the ignore rule. **Important** By default, ignore rules are disabled. Enabling a rule causes matching detection logs to be hidden from the management console, and to be ignored when displaying information.

Creating an Ignore Rule

Procedure

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

2. Select an attribute and an associated operator.

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

   - Type a value in the text box.

- Select a value from the drop-down list.

Tip

Type a keyword to search a partial match.

Note

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

---

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

5. Click **Create Ignore Rule**.

   The **Create Ignore Rule** dialog appears.

6. Type a name for this rule.

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

8. Click **Save**.

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

Chapter 5

Threat Intelligence

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

Product Intelligence

Deep Discovery Director (Internal Network Analytics Version) consolidates threat intelligence from managed appliances.

Note

This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Synchronized Suspicious Objects

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

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

Viewing Synchronized Suspicious Objects

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

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. Click the drop-down for detection type and then select one of the following detection types:

    - **All** (default)

    - **IP addresses**

    - **URLs**

    - **File SHA-1**

- **Domains**

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

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

> **Note**
>
> The **Network Detections** number only includes detections from Deep Discovery Inspector appliances. The **Email Messages** number only includes email messages from Deep Discovery Email Inspector appliances.

5. (Optional) To configure detections-related display settings, hover over the **Network Detections** or **Email Messages** icon in the column title and select **Display Settings**.

   a. Select a time period.

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

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

   c. Click **Apply**.

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

Exporting Synchronized Suspicious Objects

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

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. (Optional) Apply filters and search keywords as required.

    For details, see *Viewing Synchronized Suspicious Objects on page 5-2*.

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

    The **Export** dialog appears.

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

    - **Comma**
    - **Semicolon**
    - **Space**
    - **Tab**

5. Click **Export** to export and download the currently filtered list of synchronized suspicious objects to a CSV file with the chosen delimiter.

Moving Synchronized Suspicious Objects to Exceptions

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

Note

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

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. (Optional) Apply filters and search keywords as required.

    For details, see *Viewing Synchronized Suspicious Objects on page 5-2*.

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

    The **Move To Exceptions** dialog appears.

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

Expiring Synchronized Suspicious Objects

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

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. (Optional) Apply filters and search keywords as required.

    For details, see *Viewing Synchronized Suspicious Objects on page 5-2*.

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

    The **Expire Now** dialog appears.

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

Setting Synchronized Suspicious Objects to Never Expire

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

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. (Optional) Apply filters and search keywords as required.

    For details, see *Viewing Synchronized Suspicious Objects on page 5-2*.

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

    The **Never Expire** dialog appears.

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

Configuring Expiration Settings

By default, synchronized suspicious objects expire in 21 days. Newly synced suspicious objects can be configured to expire earlier.

Procedure

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

    The **Synchronized Suspicious Objects** screen appears.

2. Click the gear icon above the **Expiration** column.

    The **Expiration Settings** dialog appears.

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

4. Click **Save**.

C&C Callback Addresses

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

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

Viewing C&C Callback Addresses

Procedure

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

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

2. Click the drop-down for detection type and then select one of the following detection types:

- **All** (default)
- **IP addresses**
- **URLs**
- **Domains**

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

The **Display Settings** dialog appears.

4. Select a time period.

5. Select which appliances to include as data source.

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

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

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

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

Exporting C&C Callback Addresses

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

Procedure

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

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

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-7*.

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

    The **Export** appears.

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

    - **Comma**

    - **Semicolon**

    - **Space**

- **Tab**

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

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

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

Procedure

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

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

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-7*.

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

   The **Copy to User-Defined Suspicious Objects** dialog appears.

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

Copying C&C Callback Addresses to Exceptions

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

Procedure

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

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

2. (Optional) Apply filters and search keywords as required. For details, see *Viewing C&C Callback Addresses on page 5-7*.

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

    The **Copy to Exceptions** dialog appears.

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

Custom Intelligence

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

- *YARA Rules on page 5-10*
- *STIX on page 5-16*
- *User-Defined Suspicious Objects on page 5-19*

Deep Discovery Director (Internal Network Analytics Version) allow you to exclude objects from the **Synchronized Suspicious Objects** list based on the file SHA-1 hash value, IP address, domain or URL:

- *Exceptions on page 5-27*

YARA Rules

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

Deep Discovery Director (Internal Network Analytics Version) supports a maximum of 5,000 YARA rules regardless of the number of YARA rule files.

The following table shows information about YARA rule files.

TABLE 5-1. YARA Rules

COLUMN	DESCRIPTION
File Name	Name of the YARA rule file.
Rules	Number of YARA rules contained in the YARA rule file.
Files To Analyze	File types to analyze using the YARA rules in the YARA rule file.
Risk Level	Risk level of the YARA rules. **Note** Only Deep Discovery Email Inspector utilizes these risk levels.
Description	Description of the YARA rule file.
Last Updated	Date and time the YARA rule file was last updated.
Updated By	The account that last updated the YARA rule file.
Network Detections	Click a number to drill-down to the **Network Detections** screen with filters applied. The number only includes detections from Deep Discovery Inspector appliances.
Email Messages	Click a number to drill-down to the **Email Messages** screen with filters applied. The number only includes email messages from Deep Discovery Email Inspector appliances.

Note

This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Creating a YARA Rule File

Deep Discovery Director (Internal Network Analytics Version) supports YARA rules that follow version 4.1.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

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

https://yara.readthedocs.io/en/v4.1.0/writingrules.html

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

- File name must be unique

- File content cannot be empty

The following example shows a simple YARA rule:

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

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

TABLE 5-2. YARA Rule Parts and Usage

PART	USAGE
rule	The YARA rule name. Must be unique and cannot contain spaces.
meta:	Indicates that the "meta" section begins. Parts in the meta section do not affect detection.
desc	Optional part that can be used to describe the rule.

Part	Usage
weight	Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met: • 1 to 9 = Low risk • 10 = High risk **Note** • The weight value does not correspond to the risk level assigned by Deep Discovery products. • The weight value is ignored by Deep Discovery Email Inspector.
strings:	Indicates that the "strings" section begins. Strings are the main means of detecting malware.
$a / $b / $c	Strings used to detect malware. Must begin with a $ character followed by one of more alphanumeric characters and underscores.
condition:	Indicates that the "condition" section begins. Conditions determine how your strings are used to detect malware.
$a or $b or $c	Conditions are Boolean expressions that define the logic of the rule. They tell the condition under which a submitted object satisfies the rule or not. Conditions can range from the typical Boolean operators and, or and not, to relational operators >=, <=, <, >, == and !=. Arithmetic operators (+, −, *, \, %) and bitwise operators (&, |, <<, >>, ~, ^) can be used on numerical expressions.

Adding a YARA Rule File

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

Procedure

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

    The **YARA Rules** screen appears.

2. Click **Add**.

    The **Add YARA Rule File** dialog appears.

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

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

    > **Note**
    >
    > - Trend Micro recommends only specifying the file types targeted
    >   by the YARA rules. The **All file types** option includes additional
    >   file types that are not supported by Virtual Analyzer. Only Deep
    >   Discovery Email Inspector utilizes those additional file types.
    >
    > - File types that are not supported by Virtual Analyzer can be added
    >   as custom file types. Only Deep Discovery Email Inspector utilizes
    >   custom file types.

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

    > **Note**
    >
    > Only Deep Discovery Email Inspector utilizes these risk levels.

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

7. Click **Add**.

    The YARA rule file appears in the **YARA Rules** list. Registered appliances
    receive the updated **YARA Rules** list during the next synchronization.

Editing a YARA Rule File

Procedure

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

    The **YARA Rules** screen appears.

2. Click the file name of the YARA rule file you want to edit.

    The **Edit YARA Rule File** dialog appears.

3. Modify the settings.

4. Click **Save**.

Exporting YARA Rule Files

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

Procedure

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

    The **YARA Rules** screen appears.

2. Do one of the following to export the YARA rule files:

    -   To export all YARA rule files, click **Export** without selecting any YARA rule files.

    -   To export specific YARA rule files, select the YARA rule files to export and click **Export Selected**.

    Deep Discovery Director (Internal Network Analytics Version) creates a ZIP archive with the YARA rule files.

    Note

    Regardless of the original encoding used when the YARA rule files were imported, exported YARA rule files will always use UTF-8 encoding.

3.   Download and save the ZIP archive.

Deleting YARA Rule Files

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

Procedure

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

The **YARA Rules** screen appears.

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

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

STIX

Deep Discovery Director (Internal Network Analytics Version) enables you to import objects to the **User-Defined Suspicious Objects** list using the **Structured Threat Information eXpression (STIX)** format.

The following table shows information about STIX files.

TABLE 5-3. STIX

COLUMN	DESCRIPTION
File Name	Name of the STIX file.
Description	Description of the STIX file.
Version	Version of the STIX file.
Imported	Date and time the STIX file was imported.
Imported By	The Deep Discovery Director (Internal Network Analytics Version) account or TAXII client IP address that imported the STIX file.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Importing Objects From STIX

Procedure

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

    The **STIX** screen appears.

2. Click **Import**.

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

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

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

5. Click **Import**.

> **Note**
>
> - Only IP addresses, domains, URLs, file SHA-1 hash values, and file SHA-256 hash values will be added to the **User-Defined Suspicious Objects** list.
>
> - When using STIX 1.x, only `Indicators` whose `Confidence` is not `Medium`, `Low`, `None`, or `Unknown` will be added to the **User-Defined Suspicious Objects** list.
>
> - When using STIX 2.0, only `"indicator"` type objects that are not labeled as `"anomalous-activity"`, `"anonymization"`, `"benign"`, or `"compromised"`, and that are not revoked will be added to the **User-Defined Suspicious Objects** list.
>
> - When using STIX 2.1, only `"indicator"` type objects that are not labeled as `"anomalous-activity"`, `"anonymization"`, `"benign"`, `"compromised"`, or `"unknown"`, and that are not revoked will be added to the **User-Defined Suspicious Objects** list.
>
> - The STIX file and object information can be shared as part of threat intelligence.

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

Exporting STIX Files

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

Procedure

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

   The **STIX** screen appears.

2. Do one of the following to export the STIX files:

    • To export all STIX files, click **Export** without selecting any STIX files.

    • To export specific STIX files, select the STIX files to export and click **Export Selected**.

    Deep Discovery Director (Internal Network Analytics Version) creates a ZIP archive with the STIX files.

Deleting STIX Files

Procedure

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

    The **STIX** screen appears.

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

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

> **Note**
>
> Deleting the STIX files does not affect already imported objects.

User-Defined Suspicious Objects

The **User-Defined Suspicious Objects** list allows you to define suspicious file SHA-1 hash value, suspicious file SHA-256 hash value, IP address, URL, and domain objects that Deep Discovery products with Virtual Analyzer have not yet detected on your network. Supported Deep Discovery products can take action on the objects found in the list to prevent the spread of unknown threats.

Viewing User-Defined Suspicious Objects

Procedure

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

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

2. Click the drop-down for detection type and then select one of the following detection types:

    - **All** (default)

    - **IP addresses**

    - **URLs**

    - **File SHA-1**

    - **File SHA-256**

    - **Domains**

3. To run a search, type an IP address, domain, URL, SHA-1 hash value, SHA-256 hash value, or description keyword in the search text box, and then press ENTER or click the magnifying glass icon.

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

    > **Note**
    >
    > The **Network Detections** number only includes detections from Deep Discovery Inspector appliances. The **Email Messages** number only includes email messages from Deep Discovery Email Inspector appliances.

5. (Optional) To configure display settings, hover over the **Network Detections** or **Email Messages** icon in the column title and select **Display Settings**.

     a. Select a time period.

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

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

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

Viewing User-Defined Suspicious Objects - Correlation Data

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

Procedure

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

2. To view correlation data, click the **Correlation Data** icon (⚒) under **Details**.

> **Note**
>
> • The **Correlation Data** icon is grayed out when correlation data is unavailable.
>
> • Deep Discovery Director - Network Analytics only stores correlation data for suspicious objects for a limited time, even if the suspicious objects are set to never expire.
>
> • Deep Discovery Inspector appliances from which you want to collect correlated data must enabled as connected sources.

The **Correlation Data** screen appears.

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

   - **Summary**

     Displays the severity, the number of detected internal hosts and Indicators of Compromise (IOCs), the assigned attack patterns, and provides a high-level overview of the malicious activity of the correlation data.

   - **Correlation Graph**

     Provides a visual representation of correlations made between the correlated event selected in Deep Discovery Director and other related events as they occurred over time.

   - **Transaction and IOC Details**

     Provides details about each transaction represented in the correlation graph, and each detected Indicator of Compromise (IOC). Transactions are listed from oldest transaction at the top to the most recent transaction at the bottom. IOCs are listed from oldest first seen at the top to the most recent first seen at the bottom.

Tip

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

---

4. For details on how to use the information displayed in the **Correlation Data** screen to assist in advanced analysis, see *Analyzing Correlation Data Information on page 4-78*.

Adding a User-Defined Suspicious Object

Procedure

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

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

2. Click **Add**.

    The **Add Object** dialog appears.

3. Select the object type:

    -   **IP address**: type an IP address or a hyphenated range.

        > **Note**
        >
        > IPv4 and IPv6 addresses and subnet mask bits are supported.

    -   **URL**: type a URL.

        > **Note**
        >
        > HTTP and HTTPS URLs are supported.

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

    -   **File SHA-256**: type the SHA-256 hash value of a file.

    -   **Domain**: type a domain name.

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

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

5. Click **Add**.

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

> **Tip**
>
> Objects can also be added from product intelligence.
>
> For details, see *Copying C&C Callback Addresses to User-Defined Suspicious Objects on page 5-9*.

Editing a User-Defined Suspicious Object

Procedure

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

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

2. Click the object you want to edit.

    The **Edit Object** dialog appears.

3. Modify the settings.

    > **Note**
    >
    > The object type cannot be modified.

4. Click **Save**.

Importing User-Defined Suspicious Objects

Deep Discovery Director (Internal Network Analytics Version) supports importing objects from a CSV file.

Procedure

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

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

2. Click **Import**.

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

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

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

4. Select the delimiter that is used in the CSV file.

5. Click **Import**.

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

Exporting User-Defined Suspicious Objects

The **User-Defined Suspicious Objects** list can be exported in CSV format for offline viewing.

Procedure

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

2. (Optional) Apply filters and search keywords as required.

   For details, see *Viewing User-Defined Suspicious Objects on page 5-20*.

3. Click **Export** to export the currently filtered list of user-defined suspicious objects.

   The **Export** dialog appears.

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

   - **Comma**
   - **Semicolon**
   - **Space**
   - **Tab**

5. Click **Export** to export and download the currently filtered list of user-defined suspicious objects to a CSV file with the chosen delimiter.

Deleting User-Defined Suspicious Objects

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

Procedure

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

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

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

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

Configuring Expiration Settings

By default, user-defined suspicious objects never expire. Existing and newly added user-defined suspicious objects can be configured to automatically expire.

Procedure

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

2. Click the gear icon above the detections columns.

    The **Expiration Settings** dialog appears.

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

4. Click **Save**.

    The expiration settings immediately apply to existing objects, and are applied to newly added objects as they are added.

> **Note**
>
> • Objects that have not been updated in the specified number of days will be deleted immediately. Deleted objects cannot be restored.
>
> • Disabling expiration settings sets all existing objects to never expire.

Exceptions

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

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

Viewing Exceptions

Procedure

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

    The **Exceptions** screen appears.

2. Click the drop-down for detection type and then select one of the
    following detection types:

    -   **All** (default)

    -   **IP addresses**

    -   **URLs**

    -   **File SHA-1**

    -   **Domains**

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

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

Adding an Exception

Procedure

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

    The **Exceptions** screen appears.

2. Click **Add**.

    The **Add Exception** dialog appears.

3. Select the object type:

    -   **IP address**: type an IP address or a hyphenated range.

> **Note**
>
> IPv4 and IPv6 addresses and subnet mask bits are supported.

- **URL**: type a URL.

> **Note**
>
> HTTP and HTTPS URLs are supported.

- **File SHA-1**: type the SHA-1 hash value of a file.
- **Domain**: type a domain name.

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

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

5. Click **Add**.

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

> **Tip**
>
> Exceptions can also be added from product intelligence. For details, see the following topics:
>
> - *Moving Synchronized Suspicious Objects to Exceptions on page 5-4*
> - *Copying C&C Callback Addresses to Exceptions on page 5-9*

Importing Exceptions

Procedure

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

The **Exceptions** screen appears.

2. Click **Import**.

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

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

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

4. Click **Import**.

   The objects appear in the **Exceptions** list. Registered appliances receive the new object information during the next synchronization.

Deleting Exceptions

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

Procedure

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

   The **Exceptions** screen appears.

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

   The object is deleted from the **Exceptions** list. Registered appliances receive the updated **Exceptions** list during the next synchronization.

Feed Management

Deep Discovery Director (Internal Network Analytics Version) allows you to subscribe to and monitor intelligence feeds for threat information that can be used to complement your product and custom intelligence.

The following table shows information about intelligence feeds.

TABLE 5-4. Intelligence Feeds

COLUMN	DESCRIPTION
Feed Name	Name of the intelligence feed.
TAXII Version	TAXII version of the intelligence feed.
API Root	API root of the intelligence feed.
Collection	Collection that is selected from the intelligence feed.
Polling Interval	Frequency at which the intelligence feed is polled for information.
Last Polled	Date and time the intelligence feed was last polled for information.
Status	Click the toggle to enable or disable polling the intelligence feed for information.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Adding an Intelligence Feed

Procedure

1. Go to **Threat Intelligence** > **Feed Management**.

    The **Feed Management** screen appears.

2. Click **Add**.

The **Add Intelligence Feed** screen appears.

3. Enable the intelligence feed.

4. Type a name for this intelligence feed.

5. Select the server version for this intelligence feed.

> **Note**
>
> The server version cannot be modified once the intelligence feed has been added.

---

6. Type the discovery URL for this intelligence feed.

7. (Optional) Select **Use server certificate** if the server uses it, and then click **Select** to locate the server certificate file.

8. (Optional) Select **Specify authentication credentials** if the server requires it, and then type the user name and password used for authentication.

9. (Optional) Select **Server requires client authentication** if the server requires it, and then click **Select** to locate the client certificate file.

10. (Optional) Type the client certificate passphrase.

11. Click **Discover** to find and then select an available collection.

12. Select the frequency at which the intelligence feed is polled for information.

13. Select how far in the past you want to begin polling information from.

14. Click **Add**.

   The intelligence feed appears in the **Feed Management** list. Polled information that contains IP addresses, domains, URLs, SHA-1 hash values, and SHA-256 hash values will be added to the **User-Defined Suspicious Objects** list. Registered appliances receive the updated **User-Defined Suspicious Objects** list during the next synchronization.

> **Note**
>
> - When using TAXII 1.x, only `Indicators` whose `Confidence` is not `Medium`, `Low`, `None`, or `Unknown` will be added to the **User-Defined Suspicious Objects** list.
>
> - When using TAXII 2.0, only `"indicator"` type objects that are not labeled as `"anomalous-activity"`, `"anonymization"`, `"benign"`, or `"compromised"`, and that are not revoked will be added to the **User-Defined Suspicious Objects** list.
>
> - When using TAXII 2.0, there are certain specifications to ensure server compatibility. For more information visit the following site:
>
>   http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html
>
> - When using TAXII 2.1, only `"indicator"` type objects that are not labeled as `"anomalous-activity"`, `"anonymization"`, `"benign"`, `"compromised"`, or `"unknown"`, and that are not revoked will be added to the **User-Defined Suspicious Objects** list.
>
> - When using TAXII 2.1, there are certain specifications to ensure server compatibility. For more information visit the following site:
>
>   https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html

Editing an Intelligence Feed

Procedure

1. Go to **Threat Intelligence** > **Feed Management**.

    The **Feed Management** screen appears.

2. Click the feed name of the intelligence feed you want to edit.

    The **Edit Intelligence Feed** screen appears.

3. Modify the settings.

> **Note**
>
> The server version cannot be modified once the intelligence feed has been added.

4. Click **Save**.

Deleting Intelligence Feeds

Procedure

1. Go to **Threat Intelligence** > **Feed Management**.

   The **Feed Management** screen appears.

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

   The intelligence feeds are deleted from the **Feed Management** list. STIX files that were obtained from the intelligence feeds and that were added to the **STIX** list will be deleted. Deleting the STIX files does not affect already imported objects.

Sharing Settings

Deep Discovery Director (Internal Network Analytics Version) provides various methods to share threat intelligence data with other products or services.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

TAXII 1.x

Deep Discovery Director (Internal Network Analytics Version) can share threat intelligence data with other products or services through TAXII 1.x.

Configuring TAXII 1.x Settings

Procedure

1. Go to **Threat Intelligence** > **Sharing Settings** > **TAXII 1.x**.

   The **TAXII 1.x** screen appears.

2. Select **Enable TAXII 1.x server to allow exchange of threat intelligence with integrated products/services**.

3. Type the user name and password used for authentication.

4. Select the risk level of the objects to be included in the threat intelligence data file.

5. Click **Save**.

6. (Optional) Click **Generate Now**.

7. Deep Discovery Director (Internal Network Analytics Version) automatically generates threat information every 10 minutes. Configure an integrated product/service to subscribe to and monitor the Deep Discovery Director (Internal Network Analytics Version) discovery URL for threat information. For more information, see the documentation for the integrated product/service.

TAXII 2.0/2.1

Deep Discovery Director (Internal Network Analytics Version) can share threat intelligence data with other products or services through TAXII 2.0 and 2.1.

Configuring TAXII 2.0/2.1 Settings

Procedure

1. Go to **Threat Intelligence** > **Sharing Settings** > **TAXII 2.0/2.1**.

   The **TAXII 2.0/2.1** screen appears.

2. Select **Enable TAXII 2.0/2.1 server to allow exchange of threat intelligence with integrated products/services**.

3. Type the user name and password used for authentication.

4. Select the risk level of the objects to be included in the threat intelligence data file.

5. Click **Save**.

6. (Optional) Click **Generate Now**.

7. Deep Discovery Director (Internal Network Analytics Version) automatically generates threat information every 10 minutes. Configure an integrated product/service to subscribe to and monitor the Deep Discovery Director (Internal Network Analytics Version) discovery URL for threat information. For more information, see the documentation for the integrated product/service.

OpenDXL

Deep Discovery Director (Internal Network Analytics Version) can distribute threat intelligence data to OpenDXL clients, services, and brokers.

Configuring OpenDXL Settings

Procedure

1. Go to **Threat Intelligence** > **Sharing Settings** > **OpenDXL**.

   The **OpenDXL** screen appears.

2. Select **Distribute objects to OpenDXL client/service/broker**.

3. Type the server address.

4. Type the port.

5. Click **Select** to locate the server certificate, client certificate, and key files used for authentication.

6. (Optional) Click **Test Connection**.

7. Select which objects to include in the threat intelligence data.

8. Select the risk level of the objects to be included in the threat intelligence data.

9. Select the frequency at which objects should be distributed.

10. Click **Save**.

11. (Optional) Click **Distribute Now** to distribute suspicious objects and C&C callback addresses to this OpenDXL client/service/broker.

Web Service

Deep Discovery Director (Internal Network Analytics Version) can share threat intelligence data with other products or services (for example, a Blue Coat ProxySG device) through HTTP or HTTPS web service.

Configuring Web Service Settings

Procedure

1. Go to **Threat Intelligence** > **Sharing Settings** > **Web Service**.

   The **Web Service** screen appears.

2. Select **Enable web service to allow integrated products/services to obtain information from Deep Discovery Director**.

3. (Optional) By default, Deep Discovery Director (Internal Network Analytics Version) shares threat intelligence data only through HTTPS web service. To additionally enable threat intelligence data through HTTP, select **Share information using HTTP (in addition to HTTPS)** and specify the HTTP server port number.

4. Select which objects to include in the threat intelligence data file.

5. Select the risk level of the objects to be included in the threat intelligence data file.

   The objects appear in the generated file under the following categories.

TABLE 5-5. Object Categories in Generated File

OBJECT	CATEGORY IN GENERATED FILE
Synchronized Suspicious Objects	DDD_so_list
User-Defined Suspicious Objects	DDD_so_list
C&C Callback Addresses	DDD_cnc_callback_addresses_list
Malicious URL detected by Web Reputation Service from integrated product	DDD_wrs_list

6. Select the frequency at which objects should be shared.

7. Click **Save**.

8. (Optional) Click **Generate Now**.

> **Note**
>
> After the file generation is successful, you can click the URL to download the threat intelligence data file to view the content.

9. Configure an integrated product/service (for example, Blue Coat ProxySG device) to obtain threat intelligence data from Deep Discovery Director (Internal Network Analytics Version). For more information, see the documentation for the integrated product/service.

Auxiliary Products/Services

To help provide effective detection and blocking at the perimeter, Deep Discovery Director (Internal Network Analytics Version) can distribute threat intelligence data to auxiliary products and services.

Deep Discovery Director (Internal Network Analytics Version) integrates with the following solutions:

TABLE 5-6. Supported Solutions

NAME	VERSIONS
Trend Micro TippingPoint Security Management System (SMS)	SMS 4.6.0 or later
Check Point Open Platform for Security (OPSEC)	Check Point R80.10 or later
IBM Security Network Protection (XGS)	XGS 5.2 or later
Palo Alto Panorama	PAN-OS 7.0.1 or later
Palo Alto Firewalls	PAN-OS 4.1.0 or later

Trend Micro TippingPoint Security Management System (SMS)

Deep Discovery Director (Internal Network Analytics Version) can send synchronized suspicious objects, user-defined suspicious objects and C&C callback addresses to Trend Micro TippingPoint Security Management System (SMS).

Note

The following actions will remove suspicious objects from Trend Micro TippingPoint Security Management System (SMS):

- Moving synchronized suspicious objects to Exceptions
- Expiring synchronized suspicious objects
- Deleting user-defined suspicious objects

Deep Discovery Director (Internal Network Analytics Version) sends each C&C callback address and suspicious object with the following optional information:

- Trend Micro Severity: Severity of each suspicious object or C&C callback attempt
- Trend Micro Publisher: Trend Micro Deep Discovery Director (Internal Network Analytics Version)

- Trend Micro Source: Deep Discovery Director (Internal Network Analytics Version) host name

- Trend Micro Detection Category: Suspicious object or C&C callback attempt

- Reputation Entries TTL: The time to live (TTL) of the C&C callback address or suspicious object.

> **Note**
>
> Only supported by SMS 5.1 or higher.

Configuring Trend Micro TippingPoint Security Management System (SMS)

Procedure

1. On the Deep Discovery Director (Internal Network Analytics Version) management console, go to **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

   The **Auxiliary Products/Services** screen appears.

2. Select **Distribute objects to auxiliary products/services**.

3. Select **Trend Micro TippingPoint Security Management System (SMS)**.

4. Type the server address.

   > **Note**
   >
   > The server address must be the IPv4 address or FQDN of the auxiliary product/service.

5. Type the user name and password used for authentication.

6. (Optional) Click **Test Connection**.

7. To send object information from Deep Discovery Director (Internal Network Analytics Version) to this auxiliary product/service, configure the following criteria:

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

    > **Note**
    >
    > Only supported by SMS 5.0 or higher.

    - Suspicious Object
        - IPv4 address
        - Domain
        - URL

    > **Note**
    >
    > Only supported by SMS 5.0 or higher.

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

8. Select the frequency at which object information should be distributed.

9. Click **Save**.

    The following tag categories are displayed in the TippingPoint SMS Reputation Database.

Tag Category	Value
Trend Micro Source	The host name of Deep Discovery Director (Internal Network Analytics Version)
Trend Micro Severity	Possible values: • High • Medium • Low
Trend Micro Publisher	The product name of Deep Discovery Director (Internal Network Analytics Version)
Trend Micro Detection Category	The detection type of the threat.
Reputation Entries TTL	The time to live (TTL) as a timestamp in YYYY-MM-DD hh:mm:ss TZ format. **Note** Only supported by SMS 5.1 or higher.

10. (Optional) To view distributed C&C callback addresses and suspicious objects in TippingPoint SMS, do the following:

    a. Verify that the following tag categories exist in the **Tag Categories** list of the TippingPoint SMS Client.

       • Trend Micro Severity

       • Trend Micro Source

       • Trend Micro Publisher

       • Trend Micro Detection Category

    b. On the **Profile** tab, go to **Reputation Database** > **Search**.
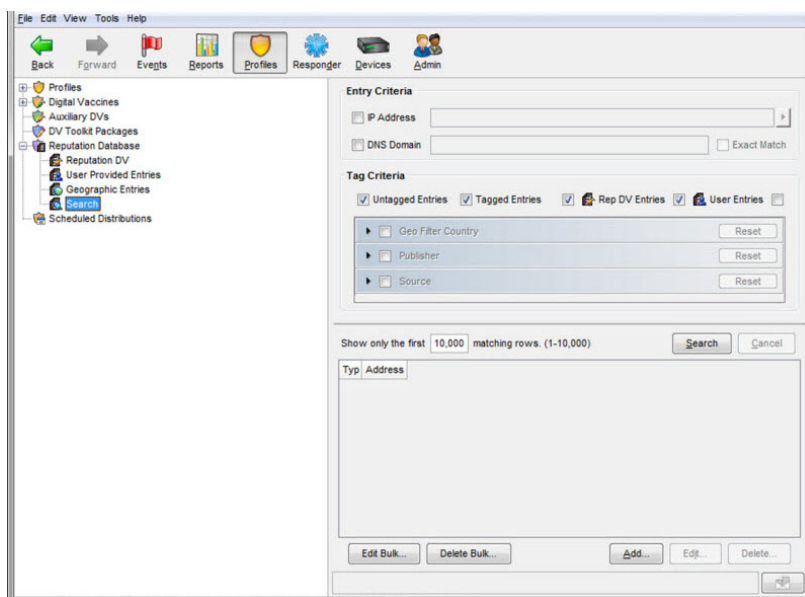
c. On the **Entry Criteria** screen, type search parameters and then click **Search**.

Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Internal Network Analytics Version) are displayed.

Check Point Open Platform for Security (OPSEC)

Check Point Open Platform for Security (OPSEC) manages network security through an open, extensible management framework.

Deep Discovery Director (Internal Network Analytics Version) integrates with Check Point OPSEC via the Suspicious Activities Monitoring (SAM) API.

The SAM API implements communications between the SAM client (Deep Discovery Director (Internal Network Analytics Version)) and the Check Point firewall, which acts as a SAM Server. Deep Discovery Director (Internal Network Analytics Version) uses the SAM API to request that the Check Point firewall take specified actions for certain connections.

For example, Deep Discovery Director (Internal Network Analytics Version) may ask Check Point OPSEC to block a connection with a client that is attempting to issue illegal commands or repeatedly failing to log on.

Configuring Check Point Open Platform for Security (OPSEC)

Procedure

1. On the Deep Discovery Director (Internal Network Analytics Version) management console, go to **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

   The **Auxiliary Products/Services** screen appears.

2. Select **Distribute objects to auxiliary products/services**.

3. Select **Check Point Open Platform for Security (OPSEC)**.

4. Click **Legal Statement**.

   The **Legal Statement** dialog appears.

5. Read and accept the **Legal Statement**.

   > **Important**
   >
   > To enable integration with this auxiliary product/service, you must accept the **Legal Statement**.

6. Select a connection type.

> **Note**
>
> Ensure that your network configuration allows Deep Discovery Director (Internal Network Analytics Version) to connect to the Check Point appliance.
>
> Deep Discovery Director (Internal Network Analytics Version) may connect to the Check Point appliance through the secured connection port or clear connection port that is configured on the Check Point appliance. Deep Discovery Director (Internal Network Analytics Version) also pulls the certificate from the Check Point appliance through port 18210.

7. Type the server address.

> **Note**
>
> The server address must be the IPv4 address or resolvable host name of the auxiliary product/service.

8. Type the port.

> **Note**
>
> This port must be the same port that is configured on the security gateway. For details, see *Preconfiguring a security gateway on page 5-50*.

9. If you selected **Secured connection**, type the **OPSEC application name** and **SIC one-time password**.

   For more details, see *Configuring a secured connection on page 5-52*.

> **Note**
>
> If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

10. (Optional) Click **Test Connection**.

11. On your Check Point firewall appliance, preconfigure a security gateway. For details see *Preconfiguring a security gateway on page 5-50*.

12. On the Check Point SmartConsole, do the following to configure your Check Point appliance for deploying suspicious objects and C&C callback addresses from Deep Discovery Director (Internal Network Analytics Version):

   a. On the left pane, click **Security Policies**.

   b. On the **Standard** tab, under **Access Control**, click **Policy**.

   c. To add a rule, click the **Add rule above**

   ![Add rule above icon]

   icon.

   d. Right-click the source and select **Add new items…**.
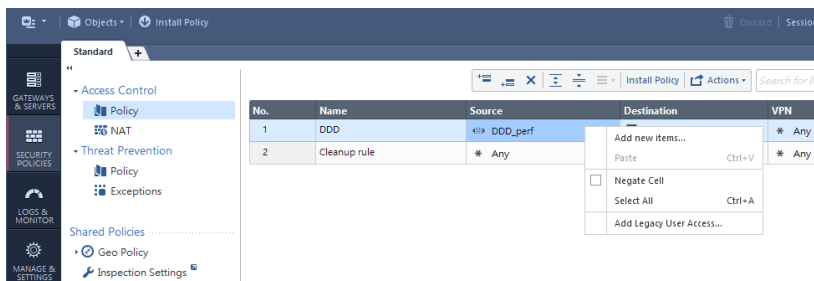
   e. Click the **New**

   ![New icon]

   icon, and select **Address Ranges** > **Address Range…**.

The **New Address Range** window appears.

f. Type DDD as name.

g. In **First IP address**, type the Deep Discovery Director (Internal Network Analytics Version) IP address.

h. In **Last IP address**, type the Deep Discovery Director (Internal Network Analytics Version) IP address.

i. Click **OK**.

An item named **DDD** should be created and automatically selected as the source.

    j. Right-click the destination and select your CheckPoint appliance.

    k. Right-click the action and select **Accept**.

    l. Click **Install Policy**.

       The Check Point SmartConsole will prompt you to publish your changes before installing the policy.

    m. Click **Publish & Install**.

       The **Install Policy** dialog appears.

    n. Click **Install**.

       The Check Point appliance is enabled to receive suspicious objects and C&C callback addresses from Deep Discovery Director (Internal Network Analytics Version).

13. On the Deep Discovery Director (Internal Network Analytics Version) management console, configure the following criteria to send suspicious object and C&C callback address information from Deep Discovery Director (Internal Network Analytics Version) to this inline product/service:

    - Object type:

        - C&C Callback Address

            - IPv4 address

        - Suspicious Object

            - IPv4 address

    - Risk level:

        - High only

        - High and medium

        - High, medium, and low

14. Under **Advanced Settings**, click one of the following actions:

    - **Reject**: Packets will be rejected and a notification sent to the communicating peer that the packet has been rejected.

- **Drop**: Packets will be dropped without sending the communicating peer a notification.

- **Notify**: A notification about the defined activity will be sent but the activity will not be blocked.

15. Select the frequency at which object information should be distributed.

16. Click **Save**.

    The **Distribute Now** option appears.

17. (Optional) Click **Distribute Now** to distribute suspicious objects and C&C callback addresses to Check Point immediately.

18. To view suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Internal Network Analytics Version) on the Check Point SmartConsole, do the following:

    a. On the left pane, click **Logs & Monitor**.

    b. Create a new tab by clicking the

    icon.

    c. On the new tab, click **Tunnel & User Monitoring**.

       The **SmartView Monitor** screen appears.

    d. On the **SmartView Monitor** screen, click **Launch Menu** icon, and then select **Tools** > **Suspicious Activity Rules...**.

       The **Enforced Suspicious Activity Rules** dialog appears.

    e. At **Show On**, select your Check Point appliance.

    f. Click **Refresh**.

    Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Internal Network Analytics Version) are displayed.

Preconfiguring a security gateway

Procedure

1. Log on to your Check Point appliance.

2. (Optional) Set a password for expert mode.

3. Type the password to enter expert mode.

4. Use the vi editor to open `/var/opt/CPsuite-R80/fw1/conf/fwopsec.conf`.

> **Note**
>
> The image of the default configuration is for reference only. The actual file contents may vary.

5. In `fwopsec.conf`, configure the SAM communication mode ports using one of the following options:

- Secured connection (default port)

    - No changes in `fwopsec.conf` are necessary. The default port 18183 is used for the **sam_server auth_port** setting.

        > **Note**
        >
        > On Deep Discovery Director (Internal Network Analytics Version), verify that the **Check Point Open Platform for Security (OPSEC) Port** setting at **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services** is also 18183.

- Secured connection (user-defined port)

    - In `fwopsec.conf`, remove the comment sign (#) from `sam_server auth_port: 18183` and then change the port number.

        > **Note**
        >
        > Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Director (Internal Network Analytics Version) at **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

- Clear connection (user-defined port)

    - In `fwopsec.conf`, remove the comment sign (#) from `sam_server port: 0` and then change the port number.

> **Note**
>
> Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Director (Internal Network Analytics Version) at **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

6. If changes were made to the `fwopsec.conf` file, save the `fwopsec.conf` file and restart your Check Point appliance.

Configuring a secured connection

Procedure

1. Open the Check Point SmartConsole and click the main menu icon ( ).

2. Go to **New object** > **More object types** > **Server** > **OPSEC Application** > **New Application…**.

The **OPSEC Application Properties** window appears.

3. Type a **Name**.
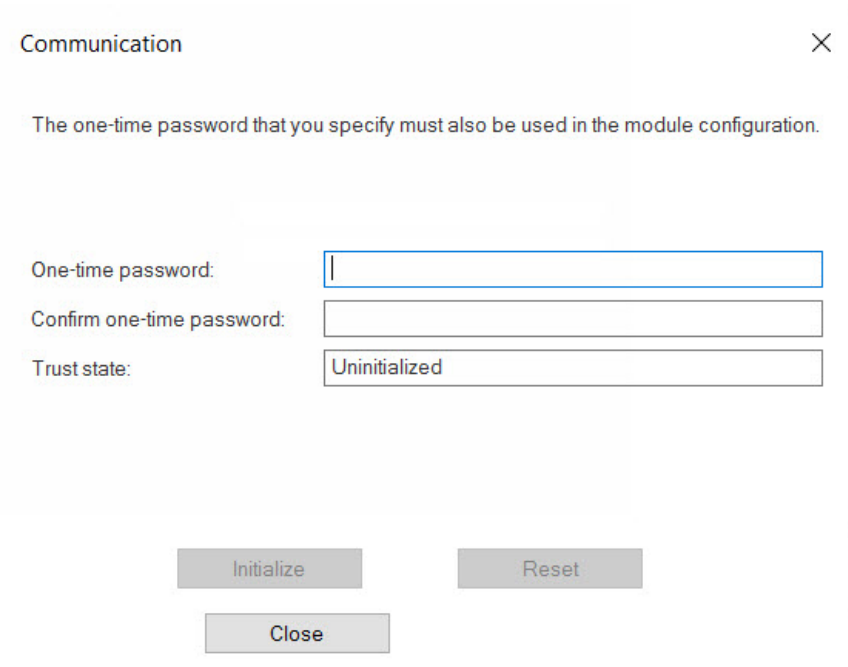
> 📝 **Note**
>
> - Use this name as the **OPSEC application name** in Deep Discovery Director (Internal Network Analytics Version).
>
> - The application name must be less than 101 characters, start with an English alphabetical letter, and contain only English alphabetical letters, periods, underscores, or dashes.

---

4. Select a **Host**.

5. Under **Client Entities**, select **SAM**.

6. Click **Communication…**.

The **Communication** window appears.

7. Type a password in **One-time password** and type the same password in **Confirm one-time password**.

> **Note**
>
> Use this password as the **SIC one-time password** in Deep Discovery Director (Internal Network Analytics Version).

> **Note**
>
> If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

8. Click **Initialize**.

The **Trust state** becomes **Initialized but trust not established**.

9. Install the user definition.

a. In the **Check Point SmartConsole** main window, click and select **Install database…**.

The **Install database** window appears.

b. Choose the installation components and then click **OK**.

The user definition starts installing.

IBM Security Network Protection (XGS)

IBM Security Network Protection (XGS) provides a web services API that enables third-party applications such as Deep Discovery Director (Internal Network Analytics Version) to directly submit suspicious objects. IBM XGS can perform the following functions:

- Quarantine hosts infected with malware
- Block communication to C&C servers
- Block access to URLs found to be distributing malware

To integrate Deep Discovery Director (Internal Network Analytics Version) with IBM XGS, configure a generic agent to do the following:

- Accept alerts that adhere to a specific schema
- Create quarantine rules based on a generic ATP translation policy

The ATP translation policy allows several categories of messages to take different actions on IBM XGS, including blocking and alerting.

Configuring IBM Security Network Protection (XGS)

Procedure

1. On the IBM XGS console, do the following to configure the generic agent:

    a. Go to **Manage System Settings** > **Network Settings** > **Advanced Threat Protection Agents**.
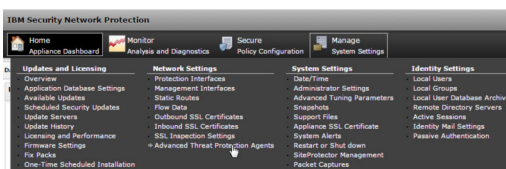
    The **Advanced Threat Protection Agents** window opens.

    b. Click **New**.

    c. Provide the following information:

    - Name: Type a name

    - Agent Type: Select **Generic**

    - Address: Deep Discovery Director (Internal Network Analytics Version) management port IP address in IPv4 or IPv6 format

    - User name: Existing authentication credential

    - Password: Existing authentication credential

    TABLE 5-7. Valid Character Sets

	USER NAME	**PASSWORD**
Minimum length	1 character	1 character
Maximum length	15 characters	15 characters
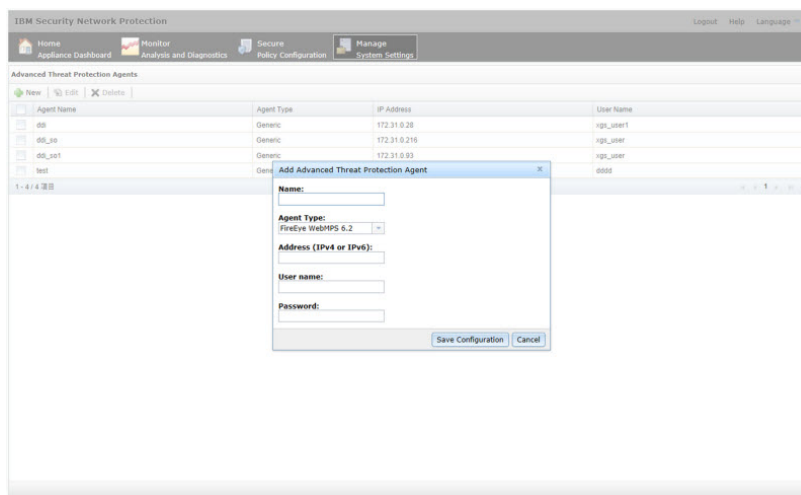
2. Click **Save Confirmation**.

   The **Deploy Pending Changes** window opens.

3. To apply changes to IBM XGS, click **Deploy**.
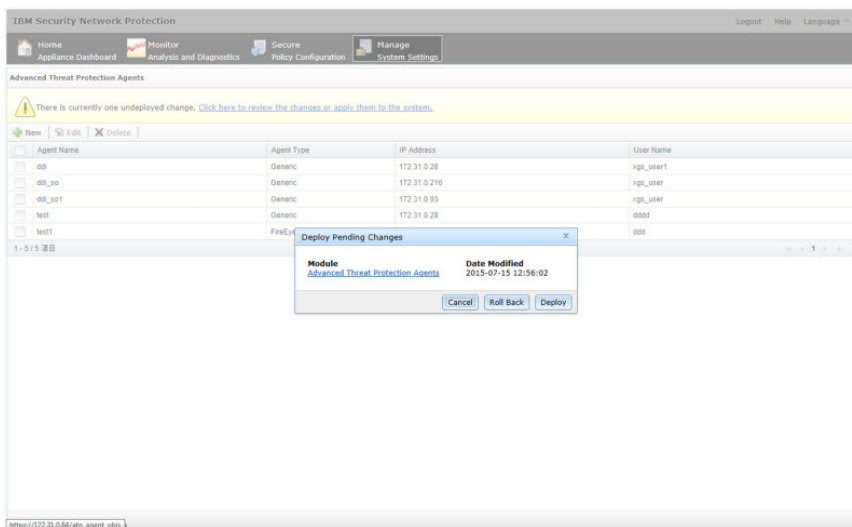
The new agent appears in the **Advanced Threat Protection Agents** list.

4. On the Deep Discovery Director (Internal Network Analytics Version) management console, go to **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

    The **Auxiliary Products/Services** screen appears.

5. Select **Distribute objects to auxiliary products/services**.

6. Select **IBM Security Network Protection (XGS)**.

7. Click **Legal Statement**.

    The **Legal Statement** dialog appears.

8. Read and accept the **Legal Statement**.

> **Important**
>
> To enable integration with this auxiliary product/service, you must accept the **Legal Statement**.

---

9. Type the server address.

> **Note**
>
> The server address must be the IPv4 address or FQDN of the auxiliary product/service.

---

10. Type the user name and password used for authentication.

11. (Optional) Click **Test Connection**.

12. To send object information from Deep Discovery Director (Internal Network Analytics Version) to this auxiliary product/service, configure the following criteria:

    - Object type:

        - C&C Callback Address

            - IPv4 address

- URL
    - Suspicious Object
        - IPv4 address
        - URL
- Risk level:
    - High only
    - High and medium
    - High, medium, and low

13. Select the frequency at which object information should be distributed.

14. Click **Save**.

15. (Optional) On the IBM XGS console, go to **Secure Policy Configuration** > **Security Policies** > **Active Quarantine Rules** to view suspicious objects and C&C callback addresses sent by Deep Discovery Director (Internal Network Analytics Version) to IBM XGS.
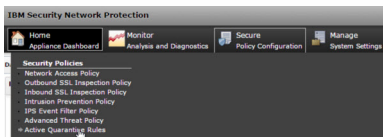
> **Note**
>
> Suspicious objects with a low risk level do not appear in the IBM XGS **Active Quarantine Rules**. To view all suspicious objects sent by Deep Discovery Director (Internal Network Analytics Version), go to **Security Policy Configuration** > **Advanced Threat Policy** and specify the following settings:
>
> - **Agent Type**: **Generic**
>
> - **Alert Type**: **Reputation**
>
> - **Alert Severity**: **Low**

Suspicious objects and C&C callback addresses distributed by Deep Discovery Director (Internal Network Analytics Version) are displayed.

Palo Alto Panorama or Firewalls

Palo Alto Networks® firewalls identify and control applications, regardless of port, protocol, encryption (SSL or SSH) or evasive characteristics.

Deep Discovery Director (Internal Network Analytics Version) generates IPv4, domain, and URL suspicious objects that can be downloaded to the URL category of Palo Alto Firewall or Palo Alto Panorama™ as match criteria to allow for exception-based behavior.

Use URL categories in policies as follows:

- Identify and allow exceptions to general security policies for users who belong to multiple groups within Active Directory

  Example: Deny access to malware and hacking sites for all users, while allowing access to users that belong to the security group.

- Allow access to streaming media category, but apply quality of service policies to control bandwidth consumption

- Prevent file download and upload for URL categories that represent higher risks

Example: Allow access to unknown sites, but prevent upload and download of executable files from unknown sites to limit malware propagation.

- Apply SSL decryption policies that allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.

Configuring Palo Alto Panorama or Firewalls

Procedure

1. On the Deep Discovery Director (Internal Network Analytics Version) management console, go to **Threat Intelligence** > **Sharing Settings** > **Auxiliary Products/Services**.

    The **Auxiliary Products/Services** screen appears.

2. Select **Distribute objects to auxiliary products/services**.

3. Select **Palo Alto Panorama or Firewalls**.

4. Click **Legal Statement**.

    The **Legal Statement** dialog appears.

5. Read and accept the **Legal Statement**.

    > **Important**
    >
    > To enable integration with this auxiliary product/service, you must accept the **Legal Statement**.

6. (Optional) By default, Deep Discovery Director (Internal Network Analytics Version) shares threat intelligence data through HTTPS. You can also share using HTTP. Under Server Settings, select **Share information using HTTP** and specify the port number.

7. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.

8. Select the frequency at which object information should be distributed.

9. Click **Save**.

10. (Optional) Click **Generate Now**.

> **Note**
>
> After the file generation is successful, you can click the URL to download the threat intelligence data file to view the content.

---

11. Configure Palo Alto Firewall or Palo Alto Panorama™ to obtain threat intelligence data from Deep Discovery Director (Internal Network Analytics Version). For more information, see the documentation for the integrated product/service.

Chapter 6

Appliances

Learn how to manage appliances, perform plan related tasks, maintain the repository, manage file passwords, and configure network asset settings in the following topics.

Note

This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Directory

The Directory displays information about Deep Discovery appliances that are registered to Deep Discovery Director (Internal Network Analytics Version).

- Left pane: Appliance tree with groups (represented by folders) and appliances (identified by display names, initially identical to their host names)

> **Note**
>
> An exclamation mark icon attached to the appliance icon indicates that the connection with this appliance has been lost.

- Right pane: Information about plans, appliances, installed or hosted update files, etc.

On fresh installations, the Directory is empty and only displays the following default groups:

- **Managed**: Appliances placed in this group can receive plan information, updates, and Virtual Analyzer images from Deep Discovery Director. Appliances can also replicate their configuration to and from other compatible appliances.

- **Unmanaged**: Appliances placed in this group cannot receive plan information, updates, Virtual Analyzer images, or replicate their configuration.

Appliances can register to Deep Discovery Director (Internal Network Analytics Version) on their respective management consoles. Newly registered appliances first appear in the Unmanaged group but can be moved to the Managed group at any time.

Directory Tasks

You can use the Directory mainly to view information about groups and appliances, and plans that are associated with these objects. Selecting an object in the left pane displays information in the right pane.

The following table describes the object types and the available information for each object.

TABLE 6-1. Directory Object Types

OBJECT	DISPLAYED INFORMATION

Appliances	• **Plan**: Plans that were or will be deployed to the appliance
	
	• **Appliance**: Identifiers such as IP address, virtual IP address, host name and display name, threat intelligence sync times, file password sync time, and other information
	
	Note
	For Deep Discovery Analyzer clusters, Deep Discovery Director (Internal Network Analytics Version) also displays the following:
	  • **Active primary appliance**: Information on the active primary appliance (high availability cluster and load balancing cluster)
	  • **Passive primary appliance**: Information on the passive primary appliance (high availability cluster)
	  • **Secondary appliances**: Information on the secondary appliance (load balancing cluster)
	
	• **Updates**: Build number and installation time of all installed updates, and information about where and when the appliance's configuration settings were replicated from
	
	• **Virtual Analyzer**: Information about the Virtual Analyzer configuration of the appliance, such as type, internal Virtual Analyzer maximum images and instances, and deployed images and instances
	
	Note
	For Deep Discovery Analyzer active primary appliances, click on **All Nodes** to display the total number of instances in use for all nodes in the cluster.

Object	Displayed Information
Groups	Overview of appliances and plans associated with that group, including statuses and connection information.

Other Directory Tasks

You can also perform the following actions:

Table 6-2. Other Directory Tasks

Action	Description
Add groups	Add groups to better organize appliances, such as by location or business unit. To add a group: 1. Click the menu icon beside the group name and then select **Add**. 2. In the text box, type a name with a maximum of 256 characters.
Edit group or appliance names	To edit a group or appliance name: 1. Click the menu icon beside the group or appliance name and then select **Edit**. 2. In the text box, type a name with a maximum of 256 characters.
Sync Threat Intelligence	Tells the appliance to sync threat intelligence from Deep Discovery Director (Internal Network Analytics Version). To sync threat intelligence, click the menu icon beside the appliance name and then select **Sync Threat Intelligence**. **Note** Appliances automatically sync threat intelligence from Deep Discovery Director (Internal Network Analytics Version). Syncing threat intelligence requires some time to complete. Avoid using this action if possible.

Action	Description
Sync File Passwords	Tells the appliance to sync file passwords from Deep Discovery Director (Internal Network Analytics Version).
	To sync file passwords, click the menu icon beside the appliance name and then select **Sync File Passwords**.
	Note Registered appliances can be configured to automatically sync file passwords from Deep Discovery Director (Internal Network Analytics Version).
Sync Network Asset Settings	Tells the appliance to sync network asset settings from Deep Discovery Director (Internal Network Analytics Version).
	To sync network asset settings, click the menu icon beside the appliance name and then select **Sync Network Asset Settings**.
	Note Registered appliances can be configured to automatically sync network asset settings from Deep Discovery Director (Internal Network Analytics Version).
Move groups or appliances	To move a group or an appliance to a different group: 1. Click the menu icon beside the group or appliance name and then select **Move**. 2. In the window, select the new folder and then click **Move**. This function is disabled whenever: • Deployment of one or more associated plans is pending or in progress. • The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**.

Action	Description
Delete groups	Delete empty or unused groups to simplify the Directory.
	To delete a group, click the menu icon beside the group name and then select **Delete**.
	WARNING!
	Deleting a group cancels the plans associated with that group and moves appliances to the **Unmanaged** group. Only groups without unfinished plans can be deleted.
	This function is disabled whenever:
	• Deployment of one or more associated plans is pending or in progress.
	• The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**.

Action	Description
Delete appliances	To delete an appliance, click the menu icon beside the display name and then select **Delete**. This function is disabled whenever the appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**. --- **WARNING!** • Deleting an appliance unregisters it from Deep Discovery Director (Internal Network Analytics Version), stops all connections, and cancels all associated plans. • Deleting a Deep Discovery Inspector appliance causes that Deep Discovery Inspector appliance to automatically unregister from Deep Discovery Director - Network Analytics. Correlated events that were derived from data provided by that Deep Discovery Inspector appliance become unavailable. Re-registering that Deep Discovery Inspector appliance to Deep Discovery Director does not automatically re-register it to Deep Discovery Director - Network Analytics. To restore full functionality, go to the management console of the Deep Discovery Inspector appliance and re-register it to its originally registered Deep Discovery Director - Network Analytics server.
Switch views	To switch between custom views, click on the name beside **Views** and then select the view to switch to.

Action	Description
Customize columns	Customize columns and save new custom views to better organize all the information. To create a custom view: 1. Click on the name beside **Views** and then select **Customize columns**. 2. Type a unique custom view name. 3. Select any combination of columns to include in the custom view. 4. Click **Apply**. --- **Tip** The column order can be rearranged using drag-and-drop.
Edit custom views	To edit a custom view: 1. Click on the name beside **Views** and then select the **pencil** icon beside the view. 2. (Optional) Edit the custom view name. 3. Edit the combination of columns. 4. Click **Apply**.
Delete custom views	To delete a custom view, click on the name beside **Views** and then select the **trash can** icon beside the view.

Plans

Plans provide control over the scope and schedule of deployments to target appliances.

Each plan is created for a specific set of target appliances and is deployed based on either a on-time or recurring schedule. Plans must match the product and language of the target appliances.

When a plan is deployed, Deep Discovery Director (Internal Network Analytics Version) sends instructions to the target appliances on when to download required files, and when to execute the plan.

There are two kinds of plan schedules listed on separate tabs in the Plans screen:

Schedule	Description
One-time plans on page 6-9	Single-use plans which execute immediately or according to a future schedule There are three types of one-time plan deployments: • **Hotfix/ Critical patch/ Firmware** • **Virtual Analyzer images** • **Configuration replication**
Recurring plans on page 6-17	Plans which execute based on a recurring schedule Recurring plans only support the **Configuration replication** deployment.

One-time Plans

One-time plans are single run deployments which execute immediately or at a scheduled time.

The **One-time Plans** screen lists plans you have created and displays information such as plan type, status, and schedule.

Tip

The list view can be filtered by clicking the **Filters** button and using the drop-down lists and search box that appear.

You can perform the following tasks on the **One-time Plans** screen:

Table 6-3. One-time Plans

Task	Description
View plan details	Click a plan name to view details including appliance statuses For details, see *Plan Details on page 6-19*.

TASK	DESCRIPTION
Add plans	Add one of the following types of plans to Deep Discovery Director (Internal Network Analytics Version): • **Hotfix / Critical Patch / Firmware** For details, see *Adding a Hotfix / Critical Patch / Firmware Deployment Plan on page 6-10*. • **Virtual Analyzer images** For details, see *Adding a Virtual Analyzer Images Deployment Plan on page 6-12*. • **Configuration replication** For details, see *Adding a Configuration Replication Plan on page 6-15*. ⚠️ **Important** Deep Discovery Director (Internal Network Analytics Version) does not allow the creation of new plans when the license status is **Not Activated** or **Expired**. Existing plans will deploy and execute as usual.
Copy plans	Select a plan in the list and click **Copy**
Delete plans	Select a plan in the list with the status **Pending** and click **Delete**

Adding a Hotfix / Critical Patch / Firmware Deployment Plan

Use this type of plan to deploy product updates and upgrades to compatible appliances.

Procedure

1. Go to **Appliances** > **Plans** > **One-time Plans** and click **Add**.

   The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select **Hotfix / Critical patch / Firmware** as type.

4. (Optional) Type a description.

5. Select a hotfix, critical patch, or firmware file from the list.

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) displays the list of files that are available in the repository. Verify that the file matches the product and language of the target appliances.

6. Select target appliances. Deep Discovery Director (Internal Network Analytics Version) only displays compatible appliances.

> **Note**
>
> Installing updates automatically restarts the target appliances.

7. Specify the schedule.

   - **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.

     - **Deployment start**: Date at which this plan will be deployed.

       > **Note**
       >
       > Plans are always deployed at 12:00 am (00:00) of the selected date.

     - **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

> **Note**
>
> - If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
>
> - Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

- **Execution start**: Date and time at which this plan will be executed.

> **Tip**
>
> Select **By schedule** to prevent the plan from executing at an unexpected time.

- **Immediate**: Starts immediately after the plan is saved.

8. Click **Save**.

Adding a Virtual Analyzer Images Deployment Plan

Use this type of plan to deploy Virtual Analyzer images to compatible appliances.

The following table lists requirements that must be fulfilled by compatible appliances:

TABLE 6-4. Requirements for Compatible Appliances

REQUIREMENT	DESCRIPTION
License	- **Status**: Activated - **Type**: Full

Requirement	Description
Virtual Analyzer	• **Status**: Enabled **Note** Virtual Analyzer images can be deployed to Deep Discovery Inspector appliances whose Virtual Analyzer status is disabled. Deep Discovery Inspector automatically enables Virtual Analyzer after the images have been deployed. • **Type**: Internal
Deep Discovery Director (Internal Network Analytics Version)	• Integration with Deep Discovery Director (Internal Network Analytics Version) 5.2 or later • Must be registered to Deep Discovery Director (Internal Network Analytics Version) • Must be in a Managed group

Procedure

1. Go to **Appliances** > **Plans** > **One-time Plans** and click **Add**.

   The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select **Virtual Analyzer images** as type.

4. (Optional) Type a description.

5. Select a product from the list.

6. Select an OS type combination from the list.

7. Select a maximum images value from the list.

8. Select a maximum instances value from the list.

9. Click **Select**.

   The **Virtual Analyzer Images** dialog appears.

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) displays the list of Virtual Analyzer images that are available in the repository.

10. Select the final configuration of Virtual Analyzer images to deploy and click **Save**.

> **Important**
>
> - The selected configuration replaces any configuration currently deployed on target appliances.
>
> - To keep currently deployed images on target appliances, select them as part of the final configuration. The target appliances will automatically determine if the selected images are identical and need to be deployed.

11. (Optional) Modify the instances allocated to any image.

12. Select target appliances. Deep Discovery Director (Internal Network Analytics Version) only displays compatible appliances.

> **Note**
>
> Deep Discovery Analyzer secondary appliances are not displayed because Virtual Analyzer images and settings are automatically synced from the primary appliance. To deploy Virtual Analyzer images to Deep Discovery Analyzer secondary appliances, select the corresponding primary appliance.

13. Specify the schedule.

    - **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.

        - **Deployment start**: Date at which this plan will be deployed.

> **Note**
>
> Plans are always deployed at 12:00 am (00:00) of the selected date.

- **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

> **Note**
>
> - If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
>
> - Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

- **Execution start**: Date and time at which this plan will be executed.

> **Tip**
>
> Select **By schedule** to prevent the plan from executing at an unexpected time.

  - **Immediate**: Starts immediately after the plan is saved.

14. Click **Save**.

Adding a Configuration Replication Plan

Use this type of plan to replicate the configuration settings of one appliance to compatible appliances.

Each Deep Discovery product supports the replication of a different combination of configuration settings. For details, see *Settings Replicated by Deep Discovery Director on page B-1*.

Procedure

1. Go to **Appliances** > **Plans** > **One-time Plans** and click **Add**.

   The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select **Configuration replication** as type.

4. (Optional) Type a description.

5. Select the replication source from the list.

   > **Tip**
   >
   > Select a product from the **View** drop-down list to only display the selected product's appliances.

6. Select target appliances. Deep Discovery Director (Internal Network Analytics Version) only displays compatible appliances.

7. Specify the schedule.

   - **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.

     - **Deployment start**: Date at which this plan will be deployed.

       > **Note**
       >
       > Plans are always deployed at 12:00 am (00:00) of the selected date.

     - **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

> **Note**
>
> - If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
>
> - Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

- **Execution start**: Date and time at which this plan will be executed.

> **Tip**
>
> Select **By schedule** to prevent the plan from executing at an unexpected time.

  - **Immediate**: Starts immediately after the plan is saved.

8. Click **Save**.

Recurring Plans

Recurring plans are deployments which execute based on a scheduled frequency.

The **Recurring Plans** screen lists plans you have created and displays information such as plan type, schedule, and last deployment.

> **Tip**
>
> The list view can be filtered by clicking the **Filters** button and using the drop-down lists and search box that appear.

You can perform the following tasks on the **Recurring Plans** screen:

TABLE 6-5. Recurring Plans

TASK	DESCRIPTION
View plan details	Click a plan name to view details including appliance statuses
	For details, see *Plan Details on page 6-19*.
Add plans	Add a new recurring plan
	Recurring plans only support the **Configuration replication** type.
	For details, see *Adding a Recurring Plan on page 6-18*.
	Important
	Deep Discovery Director (Internal Network Analytics Version) does not allow the creation of new plans when the license status is **Not Activated** or **Expired**. Existing plans will deploy and execute as usual.
Delete plans	Select a plan in the list and click **Delete**

Adding a Recurring Plan

Recurring plans replicate the configuration settings of one appliance to compatible appliances.

Each Deep Discovery product supports the replication of a different combination of configuration settings. For details, see *Settings Replicated by Deep Discovery Director on page B-1*.

> **Note**
> Recurring plans only supports the **Configuration replication** type.

> **Important**
> Source appliances and target appliances cannot be the target of another configuration replication plan.

Procedure

1. Go to **Appliances** > **Plans** > **Recurring Plans** and click **Add**.

    The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. (Optional) Type a description.

4. Select the replication source from the list.

> 💡 **Tip**
>
> Select a product from the **View** drop-down list to only display the appliances with the selected product.

5. Select target appliances. Deep Discovery Director (Internal Network Analytics Version) only displays compatible appliances.

6. Specify the **Frequency** of the schedule.

7. Click **Save**.

Plan Details

Clicking a plan name opens the details screen for that specific plan.

The **Plan Details** screen allows you to view detailed information about the plan, source appliance, and target appliance status.

You can perform the following tasks from the **Plan Details** screen:

TABLE 6-6. Plan Tasks

TASK	DESCRIPTION
View plan information	View plan deployment status and schedule, file details, source appliance and other related information
View target appliance information	View details of target appliances including appliance status, deployment start and completion, and appliance path For details, see *Appliance Statuses on page 6-20*.

Task	Description
Edit plans	To change the settings of a plan, click **Edit** **Note** For one-time plans, only plans which have the **pending** status and which have not been deployed can be edited.
Cancel plans (One-time plans only)	To stop a plan from deploying, click **Cancel Plan** You can only cancel a plan if the status is one of the following: • **Pending** • **In progress** • **Suspended**
Create plans (One-time plans only)	To create a new plan based on a plan with an **Unsuccessful** status, click **Create Plan**.
Export history (Recurring plans only)	To download the deployment history, click **Export History** and specify a **Period** You can specify a custom date range by selecting "Custom period". Click **Export** to download the history.

Appliance Statuses

Deep Discovery Director (Internal Network Analytics Version) displays any of the following appliance statuses.

TABLE 6-7. Appliance Statuses

Status	Description
Pending	The appliance has not received the plan information from Deep Discovery Director (Internal Network Analytics Version).

Status	Description
In progress	Any of the following situations may apply. • The appliance has acknowledged receipt of the plan information and has started downloading files. • The appliance has acknowledged receipt of the plan information and has started executing the plan. • The appliance is downloading the files required to execute the plan. • The appliance has downloaded the files and is executing the plan.
Suspended	The appliance has temporarily stopped downloading files and will resume on the specified download period.
Completed	The appliance executed the plan successfully.
Unsuccessful	Any of the following situations may apply. • The appliance was unable to execute the plan. • The appliance is performing tasks that do not match the plan information.
Unreachable	Any of the following situations may apply. • The appliance has unregistered from Deep Discovery Director (Internal Network Analytics Version). • The appliance has been deleted from Deep Discovery Director (Internal Network Analytics Version).
Cancelled	Any of the following situations may apply: • The plan was manually cancelled before the appliance received the plan information from Deep Discovery Director (Internal Network Analytics Version). • The plan was manually cancelled while the appliance was downloading files or executing the plan. • The plan was manually cancelled while the appliance temporarily stopped downloading files.

Repository

The Repository screen displays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here.

Hotfixes / Critical Patches / Firmware

Use the **Hotfixes / Critical Patches / Firmware** screen, in **Appliances** > **Repository** > **Hotfixes / Critical Patches / Firmware**, to view already uploaded update files, delete unused update files, and upload new update files for deployment.

Use filters to search by update or upgrade type, product, language, and file name or version.

To delete a file, select the file from the list and then click **Delete**.

Uploading a Hotfix / Critical Patch / Firmware File

Deep Discovery Director (Internal Network Analytics Version) supports simultaneous uploading of up to five files through single-file upload sessions.

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

Procedure

1. Go to **Appliances** > **Repository** > **Hotfixes / Critical Patches / Firmware**.

2. Click **Upload**.

3. Click **Select** and then select a valid TAR file.

4. (Optional) Type or paste the 64-character SHA-256 hash value of the selected file for verification.

5. (Optional) Type a description.

6. Click **Upload**.

Virtual Analyzer Images

Use the **Virtual Analyzer Images** screen, in **Appliances** > **Repository** > **Virtual Analyzer Images**, to view already uploaded image files, delete unused image files, and upload new image files for deployment.

To delete a file, select the file from the list and then click **Delete**.

> **Important**
>
> Only Virtual Analyzer images compressed in TAR format by the **Virtual Analyzer Image Preparation Tool** can be uploaded to and deployed from Deep Discovery Director (Internal Network Analytics Version).
>
> For details, see https://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Uploading Virtual Analyzer Images

Deep Discovery Director (Internal Network Analytics Version) supports consecutive uploading of up to three Virtual Analyzer image files through SFTP or network folder. Deep Discovery Director (Internal Network Analytics Version) opens a connection to the SFTP or network server in the background for the upload session, allowing you to navigate away from the screen and perform other tasks while waiting for the upload to complete.

Procedure

1. Go to **Appliances** > **Repository** > **Virtual Analyzer Images**.

2. Click **Upload**.

3. Select a source from the list.

    - **SFTP**

    - **Network Folder**

4. Type the server details.

- **SFTP**: Type the IP address or FQDN of the server, the port number, the user name, and the password.

- **Network Folder**: Type the user name and password.

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) saves the server information and logon credentials automatically.

---

5. Type the details of at least one Virtual Analyzer image file.

    a. Type file paths.

    b. Type unique image names.

    c. (Optional) Type descriptions.

6. Click **Upload**.

Upload Center

Information about files that are uploading and that have been uploaded can be displayed using the Upload Center panel. Toggle the panel by clicking on the up-arrow-drawer icon in the top right corner of the screen. The panel is divided into the following two tabs:

- *Uploading Files on page 6-24*
- *Upload History on page 6-25*

Uploading Files

Information about files that are being uploaded to Deep Discovery Director (Internal Network Analytics Version) is displayed in this tab.

To cancel a file upload, click on the **x** beside the upload.

File uploads are done in the following stages:

TABLE 6-8. File Upload Stages

STAGE	DESCRIPTION
1: Calculating	The first parts of the file upload are being verified to ensure that the file upload is valid.
2: Uploading to the repository	The file is being uploaded to the repository. All SFTP server and network folder file uploads can be cancelled by any user.
3: Processing	The file upload to the repository has completed and integrity is being verified. File uploads cannot be cancelled in this stage.

File uploads display the following information:

TABLE 6-9. Information about File Uploads

INFORMATION	DESCRIPTION
File name	The file name.
(X KB / MB / GB)	The file size in KB / MB / GB.
Time left	The estimated time until the file upload is complete based on the file size and upload speed.
(X KB/s / MB/s / GB/s)	The upload speed in KB/s / MB/s / GB/s.

Upload History

Information about files that have been uploaded to Deep Discovery Director (Internal Network Analytics Version) is displayed in this tab.

To clear the upload history, click **Clear All**.

Uploaded files display the following information:

TABLE 6-10. Information about Uploaded Files

INFORMATION	DESCRIPTION
Status	One of the following statuses: • **Successful**: The file upload was successful. • **Unsuccessful**: The file upload was unsuccessful. • **Cancelled**: The file upload was cancelled.
File name	The file name.

File Passwords

Always handle suspicious files with caution. Trend Micro recommends adding such files to a password-protected archive file or password-protecting document files from being opened before transporting the files across the network.

Click the **Sync to Registered Appliances** toggle to enable or disable syncing of the **File Passwords** settings to all registered Deep Discovery Analyzer appliances.

Note

- Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.

- The **User-Defined Passwords** list is only synced to registered Deep Discovery Analyzer appliances.

- The **Heuristically Discovered Passwords** settings are not synced to Deep Discovery Email Inspector appliances.

User-Defined Passwords

The **User-Defined Passwords** screen displays a list of user-defined passwords that **Virtual Analyzer** on registered Deep Discovery Analyzer appliances uses to extract files or open password-protected documents. For better performance, list commonly used passwords first.

> **Note**
>
> File passwords are stored as unencrypted text.

Adding Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **User-Defined Passwords**.

2. Click **Add**.

   The **Add Password** dialog appears.

3. Type a password with only ASCII characters.

   > **Note**
   >
   > Passwords are case-sensitive and must not contain spaces.

4. (Optional) Repeat steps 2 to 3 to add more passwords.

   > **Note**
   >
   > A maximum of 100 passwords can be added to the **User-Defined Passwords** list.

5. (Optional) Drag and drop the password to move it up or down the list.

6. (Optional) Delete a password by clicking the cross (X) button on the right side of the row.

7. Click **Save**.

Editing Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **User-Defined Passwords**.

2. Click the password you want to edit.

The password changes into a text box.

3. Edit the password.

4. (Optional) Repeat steps 2 to 3 to edit more passwords.

5. (Optional) Drag and drop the password to move it up or down the list.

6. (Optional) Delete a password by clicking the cross (X) button on the right side of the row.

7. Click **Save**.

Importing Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **User-Defined Passwords**.

2. Click **Import**.

The **Import Passwords** dialog appears.

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

> **Note**
>
> If you are importing a TXT file for the first time, click **Download sample file** and save the file. Populate the TXT file with properly formatted items, save the file, and then click **Select** to locate the TXT file.

4. Click **Next**.

Deep Discovery Director (Internal Network Analytics Version) checks the entries in the file to identify any invalid or duplicate passwords.

5. Click **Import**.

The passwords are added to the **User-Defined Passwords** list.

6. Click **Save**.

Exporting Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **User-Defined Passwords**.

2. Click **Export**.

The file download begins.

Deleting Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **User-Defined Passwords**.

2. Click the cross (X) button on the right side of a row.

> **Note**
>
> Repeat this step to delete additional passwords.

3. Click **Save**.

Heuristically Discovered Passwords

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen is not available in Deep Discovery Director (Internal Network Analytics Version).

Syncing Heuristically Discovered Passwords

Procedure

1. Go to **Appliances** > **File Passwords** > **Heuristically Discovered Passwords**.

2. Select **Sync heuristically discovered passwords**.

3. Modify the number of minutes before Password Analyzer and heuristically discovered passwords time out.

4. Click **Save**.

Network Assets

Network asset configuration defines and establishes the profile of the network that Deep Discovery Inspector products monitor for the Network Content Correlation Engine, and helps you make the most of Deep Discovery Director - Network Analytics.

Click the **Sync to Registered Products** toggle to enable or disable syncing of the **Network Assets** settings to all supported, registered Deep Discovery Inspector and Deep Discovery Director - Network Analytics products.

> **Note**
>
> • The **Domain Exceptions**, **Priority Watch List**, **Network Groups**, and **Registered Services** lists are synced to Deep Discovery Director - Network Analytics products.
>
> • The **Registered Domains**, **Network Groups**, and **Registered Services** lists are synced to Deep Discovery Inspector products.
>
> • Syncing overwrites products' existing settings.

Domain Exceptions

Add domains that you consider safe to the **Domain Exceptions** list. Listed domains and any interactions with them will not be included in the

Correlated Events screen. You can later remove a domain from the list to include it and related interactions in past and future events.

The following table outlines the actions available for the **Domain Exceptions** screen.

> 📝 **Note**
>
> This feature or screen is read-only when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Action	Description
Add	Add an item to the list. For more information, see *Adding a Domain Exception on page 6-31*.
Import	Import and overwrite the existing list. For more information, see *Importing a Domain Exceptions List on page 6-32*.
Export All	Export the current list.
Delete	Delete one or more selected items.

Adding a Domain Exception

Procedure

1. Go to **Appliances** > **Network Assets** > **Domain Exceptions**.

    The **Domain Exceptions** screen appears.

2. Click **Add**.

    The **Add Domain Exception** dialog appears.

3. Type the **Domain** name.

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

4. Click **Add**.

   The item appears in the **Domain Exceptions** list.

Importing a Domain Exceptions List

Importing a list overwrites the existing list. Trend Micro recommends exporting the existing list first before proceeding.

Procedure

1. Go to **Appliances** > **Network Assets** > **Domain Exceptions**.

   The **Domain Exceptions** screen appears.

2. Click **Import**.

   The **Import Domain Exceptions From CSV** dialog appears.

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

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

4. Click **Import**.

   The items appear in the **Domain Exceptions** list.

Priority Watch List

Add servers from your environment that you consider high-priority for event tracking and incident reporting.

The following table outlines the actions available for the **Priority Watch List** screen.

> **Note**
>
> This feature or screen is read-only when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Action	Description
Add	Add an item to the list.
	For more information, see *Adding a Priority Watch List Item on page 6-33*.
Import	Import and overwrite the existing list.
	For more information, see *Importing a Priority Watch List on page 6-34*.
Export All	Export the current list.
Delete	Delete one or more selected items.

Adding a Priority Watch List Item

Procedure

1. Go to **Appliances** > **Network Assets** > **Priority Watch List**.

   The **Priority Watch List** screen appears.

2. Click **Add**.

   The **Add Priority Watch List Item** dialog appears.

3. Type the **IP address**.

> **Note**
>
> Single IPv4 and IPv6 addresses and address ranges supported, subnet mask optional.

4. Click **Add**.

   The item appears in the **Priority Watch List** list.

Importing a Priority Watch List

Importing a list overwrites the existing list. Trend Micro recommends exporting the existing list first before proceeding.

Procedure

1. Go to **Appliances** > **Network Assets** > **Priority Watch List**.

   The **Priority Watch List** screen appears.

2. Click **Import**.

   The **Import Priority Watch List From CSV** dialog appears.

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

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

4. Click **Import**.

   The items appear in the **Priority Watch List**.

Registered Domains

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

The following table outlines the actions available for the **Registered Domains** screen.

Action	Description
Add	Add one or more items to the list.
	For more information, see *Adding Registered Domains on page 6-35*.
Import	Import and overwrite the existing list.
	For more information, see *Importing a Registered Domains List on page 6-36*.
Export All	Export the current list.
Delete	Delete one or more selected items.

Adding Registered Domains

Procedure

1. Go to **Appliances** > **Network Assets** > **Registered Domains**.

   The **Registered Domains** screen appears.

2. Click **Add**.

   The **Add Registered Domains** dialog appears.

3. Type the **Domain** name.

   Note

   Add multiple domains by pressing ENTER after typing a domain, no wildcard support.

4. (Optional) Type a description.

5. Click **Add**.

The items appear in the **Registered Domains** list.

Importing a Registered Domains List

Importing a list overwrites the existing list. Trend Micro recommends exporting the existing list first before proceeding.

Procedure

1. Go to **Appliances** > **Network Assets** > **Registered Domains**.

The **Registered Domains** screen appears.

2. Click **Import**.

The **Import Registered Domains From CSV, XML** dialog appears.

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

> **Tip**
>
> - If you are importing a CSV for the first time, click **Download sample CSV** and save the file. Populate the CSV file with properly formatted items (see the instructions in the CSV file), save the file, and then click **Select** to locate the CSV file.
>
> - You can import items from an XML file exported from Deep Discovery Inspector 5.5 and later.

4. Select a delimiter to use.

5. Click **Import**.

The items appear in the **Registered Domains** list.

Registered Services

Add dedicated servers for specific services that your organization uses internally or considers trustworthy. Identifying trusted services in the network helps ensure detection of unauthorized applications and services.

The following table outlines the actions available for the **Registered Services** screen.

> **Note**
>
> This feature or screen is read-only when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

ACTION	DESCRIPTION
Add	Add an item to the list. For more information, see *Adding Registered Services on page 6-37*.
Import	Import and overwrite the existing list. For more information, see *Importing a Registered Services List on page 6-38*.
Export All	Export the current list.
Delete	Delete one or more selected items.

Adding Registered Services

Procedure

1. Go to **Appliances** > **Network Assets** > **Registered Services**.

   The **Registered Services** screen appears.

2. Click **Add**.

   The **Add Registered Services** dialog appears.

3. Select one or more items from **Type**.

4. Type the **IP address**.

> **Note**
>
> - Single IPv4 and IPv6 addresses and address ranges supported, subnet mask optional.
>
> - The IP address or address range cannot belong to Class D or Class E.
>
> - The IP address or address range cannot be a loopback address.
>
> - Add multiple IP addresses or address ranges by pressing ENTER after typing an IP addresses or address ranges, no wildcard support.

5. (Optional) Type a description.

6. Click **Add**.

   The item appears in the **Registered Service** list.

Importing a Registered Services List

Importing a list overwrites the existing list. Trend Micro recommends exporting the existing list first before proceeding.

Procedure

1. Go to **Appliances** > **Network Assets** > **Registered Service**.

   The **Registered Service** screen appears.

2. Click **Import**.

   The **Import Registered Services List From CSV, XML** dialog appears.

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

> **Tip**
>
> - If you are importing a CSV for the first time, click **Download sample CSV** and save the file. Populate the CSV file with properly formatted items (see the instructions in the CSV file), save the file, and then click **Select** to locate the CSV file.
>
> - You can import items from an XML file exported from Deep Discovery Inspector 5.5 and later.

> **Note**
>
> Descriptions that have more than 256 characters will be truncated.

4. Select a delimiter to use.

5. Click **Import**.

   The items appear in the **Registered Services** list.

Network Groups

Add IP addresses or ranges to establish groups of monitored networks to allow Deep Discovery products to determine whether attacks originate from within or outside the network.

The following table outlines the actions available for the **Network Groups** screen.

Action	Description
Add	Add one or more items to the list.
	For more information, see *Adding a Network Group on page 6-40*.

Action	Description
Add sub-group	To add a sub-group to an existing group, click the menu icon beside a group name and then select **Add sub-group**. For more information, see *Adding a Sub-Group on page 6-41*. --- **Note** You can add up to three layers of sub-groups.
Import	Import and overwrite the existing list. For more information, see *Importing a Network Groups List on page 6-43*.
Export All	Export the current list.
Delete	To delete a group, click the menu icon beside a group name and then select **Delete**.

Adding a Network Group

Procedure

1. Go to **Appliances** > **Network Assets** > **Network Groups**.

   The **Network Groups** screen appears.

2. Click **Add**.

   The **Add New Group** dialog appears.

3. Type a group name.

   Note

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

   ---

4. Type an IP address or range.

> **Note**
>
> - You can add up to 1,000 IP addresses or address ranges per group.
>
> - The IP address or range cannot belong to Class D or Class E.
>
> - The IP address or range cannot be a loopback address.

   a. Use a dash to specify an IP address range.

      The **Network Groups** window supports IPv4 and IPv6:

- IPv4 example: `192.168.1.0-192.168.1.255`

- IPv6 example: `2620:1005::123-2620:1005::460`

   b. Use a slash to specify the subnet mask/prefix for IP addresses.

- IPv4 subnet mask example: `192.168.1.0/24`

- IPv6 subnet prefix example: `fd00:1:1111:200::1000/116`

5. Select whether to mark the IP address or address range as **Trusted** or **Untrusted**.

6. Click **Add** located next to the **Monitored IP addresses** field.

The IP address or address range is added to the table below.

7. (Optional) Repeat steps 4 to 6 to add additional IP addresses or address ranges to this group.

8. Click **Add**.

The item appears in the **Network Groups** list.

Adding a Sub-Group

You can add up to three layers of sub-groups.

Procedure

1. Go to **Appliances** > **Network Assets** > **Network Groups**.

   The **Network Groups** screen appears.

2. Click the menu icon beside a group name and then select **Add sub-group**.

   The **Add New Sub-Group** dialog appears and displays the parent group's IP address ranges.

3. Type a group name.

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

4. Type an IP address or range.

> **Note**
>
> - Added IP addresses must be inside the parent group's IP address ranges.
>
> - You can add up to 1,000 IP addresses or address ranges per group.
>
> - The IP address or range cannot belong to Class D or Class E.
>
> - The IP address or range cannot be a loopback address.

   a. Use a dash to specify an IP address range.

      The **Network Groups** window supports IPv4 and IPv6:

      - IPv4 example: `192.168.1.0-192.168.1.255`

      - IPv6 example: `2620:1005::123-2620:1005::460`

   b. Use a slash to specify the subnet mask/prefix for IP addresses.

- IPv4 subnet mask example: `192.168.1.0/24`

- IPv6 subnet prefix example: `fd00:1:1111:200::1000/116`

5. Select whether to mark the IP address or address range as **Trusted** or **Untrusted**.

6. Click **Add** located next to the **Monitored IP addresses** field.

   The IP address or address range is added to the table below.

7. (Optional) Repeat steps 4 to 6 to add additional IP addresses or address ranges to this group.

8. Click **Add**.

   The item appears in the **Network Groups** list.

Importing a Network Groups List

Importing a list overwrites the existing list. Trend Micro recommends exporting the existing list first before proceeding.

Procedure

1. Go to **Appliances** > **Network Assets** > **Network Groups**.

   The **Network Groups** screen appears.

2. Click **Import**.

   The **Import Network Groups From JSON, XML** dialog appears.

3. Click **Select** to locate a JSON or XML file to import.

> **Tip**
>
> - If you are importing a JSON for the first time, click **Download sample JSON** and save the file. Populate the JSON file with properly formatted items (see the instructions in the JSON file), save the file, and then click **Select** to locate the JSON file.
>
> - You can import items from an XML file exported from Deep Discovery Inspector 5.5 and later.

4. Click **Import**.

   The items appear in the **Network Groups** list.

Analyze

Analyze detections and select from detected domains and services to add to the **Registered Domains** and **Registered Services** lists.

Add Registered Domains and Services From Detections

Procedure

1. Go to **Appliances** > **Network Assets** > **Analyze**.

   The **Analyze** screen appears.

2. Click **Analyze Detections**.

   The **Add Registered Domains and Services From Detections** dialog appears.

3. Review your network configuration and select the domains and services to add to the **Registered Domains** and **Registered Services** lists.

4. (Optional) Type descriptions for the selected domains and services.

5. Click **Add**.

The items are added to the **Registered Domains** and **Registered Services** lists.

Logs

> **Note**
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Email Message Tracking

> **Note**
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

MTA

> **Note**
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Message Queue

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances.
>
> This feature or screen will not contain any actual data or only display **No data to display.**

Chapter 7

Alerts

Learn about alert notifications and how to configure them in the following topics.

About Alerts

Deep Discovery Director (Internal Network Analytics Version) monitors a variety of events and can be configured to generate alerts to inform users of those events.

Token Variables

The following table describes the token variables that can be used to customize the subject line of alert notifications.

> **Note**
>
> Not all tokens are available for all alerts.

TABLE 7-1. Subject Line Tokens

TOKEN	DESCRIPTION
%AlertLevel%	The level of the alert notification.
%AlertName%	The name of the alert notification.
%AlertType%	The type of the alert notification.
%HostName%	The Deep Discovery Director (Internal Network Analytics Version) host name.
%ProductShortName%	The Deep Discovery Director (Internal Network Analytics Version) short name.

The following table describes the token variables used in the message body of alert notifications.

> **Note**
>
> The message body of alert notifications cannot be modified.

TABLE 7-2. Message Body Tokens

Token	Description
%LoopStart% %LoopEnd%	Any text between these two tokens is repeated until all system errors have been listed.
%IssueDescription%	The description of the system error.
%Recommendation%	The recommendation on how to resolve the system error.
%DateTime%	The date and time the alert was triggered.
%ConsoleURL%	The Deep Discovery Director (Internal Network Analytics Version) management console URL.
%DataBaseUsage%	The total database partition usage.
%FreeDataBaseSpace%	The free database partition space.
%YaraRulesPage%	The URL to the YARA Rules screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%STIXPage%	The URL to the STIX screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%LicenseLoopStart% %LicenseLoopEnd%	Any text between these two tokens is repeated until all license items have been listed.
%LicenseDescription%	The description of the license.
%LicenseType%	The license type.
%LicenseStatus%	The license status.
%ExpirationDate%	The license expiration date.
%DaysBeforeExpiration%	The number of days before the license expires.

Token	Description
%LicensePageURL%	The URL to the License screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%ServiceLoopStart% %ServiceLoopEnd%	Any text between these two tokens is repeated until all stopped services have been listed.
%ServiceID%	The ID of the stopped service.
%TriggerTime%	The date and time the service stopped.
%HighRiskLevelDetections%	The number of correlated events that have been found.
%AlertConsole%	The URL to the rule page on the Deep Discovery Director (Internal Network Analytics Version) management console.
%LastDetectedTime%	The date and time of the last detection.
%CorrelatedEventsPage%	The URL to the Correlated Events screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%AttachmentHint%	A hint about the attached file.
%TotalDetections%	The total number of detections.
%HighRiskLevelDetections%	The number of email messages that were assigned a high risk level.
%MediumRiskLevelDetections%	The number of email messages that were assigned a medium risk level.
%LowRiskLevelDetections%	The number of email messages that were assigned a low risk level.
%UnavailableRiskLevelDetections%	The number of email messages that were assigned an unavailable risk level.
%EmailMessagePage%	The URL to the Email Messages screen on the Deep Discovery Director (Internal Network Analytics Version) management console.

Token	Description
%HighSeverityDetections%	The number of network detections that were assigned a high severity level.
%MediumSeverityDetections%	The number of network detections that were assigned a medium severity level.
%LowSeverityDetections%	The number of network detections that were assigned a low severity level.
%InformationalSeverityDetections%	The number of network detections that were assigned an informational severity level.
%NetworkDetectionPage%	The URL to the Network Detections screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%SuccessLoopStart% %SuccessLoopEnd%	Any text between these two tokens is repeated until all completed plans have been listed.
%CompletedPlanName%	The name of the completed plan.
%Detail_page_URL%	The URL to the Details screen of the plan on the Deep Discovery Director (Internal Network Analytics Version) management console.
%CompletedPlanType%	The type of the completed plan.
%CompletedDateTime%	The date and time the plan was completed.
%FailedLoopStart% FailedLoopEnd	Any text between these two tokens is repeated until all unsuccessful plans have been listed.
%UnsuccessfulPlanName%	The name of the unsuccessful plan.
%UnsuccessfulPlanType%	The type of the unsuccessful plan.

Token	Description
%ApplianceUnsucc essfulNumber%	The number of appliances that unsuccessfully executed the plan.
%ApplianceUnreac hableNumber%	The number of appliances that were unreachable.
%ApplianceCancel edNumber%	The number of appliances where the plan was canceled.
%LogPartitionUsa ge%	The total log partition usage.
%FreeLogPartitio nSpace%	The free log partition space.
%LogPartitionSpa ceThreshold%	The low free disk space threshold value.
%StoragePage%	The URL to the Storage screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%RepositoryUsage %	The total repository usage.
%FreeRepositoryS pace%	The free repository space.
%PageURL%	The URL to the Repository screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%FileUploadLoopS tart% %FileUploadLoopE nd%	Any text between these two tokens is repeated until all file upload results have been listed.
%FileName%	The name of the uploaded file.
%FileType%	The type of the uploaded file.
%UploadResult%	The result of the upload.
%UploadDateTime%	The date and time the file was uploaded.

Token	Description
%RepositoryURL%	The URL to the Repository screen on the Deep Discovery Director (Internal Network Analytics Version) management console.
%PlanPageURL%	The URL to the Plans screen on the Deep Discovery Director (Internal Network Analytics Version) management console.

Triggered Alerts

The **Triggered Alerts** screen displays the following information:

TABLE 7-3. Triggered Alerts Columns

Column	Information
Triggered	The date and time when the alert was triggered.
Alert Level	An alert can be classified as any of the following levels. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **Informational**: The event requires limited observation
Type	The type of rule that can trigger an alert can be any of the following: • **System**: A built-in, system related rule. • **Email Security**: An email security related rule. • **Network Security**: A network security related rule. • **Custom**: A user-specified custom rule. • **Network Analytics**: A network analytics related rule.
Rule	The rule that triggered the alert.
Criteria	The summarized criteria of the rule. For custom rules, displays the advanced search filter.

COLUMN	INFORMATION

Events	The triggered alert occurrences. Click the number to drill down to the **Network Detections** or **Email Messages** screen.
	
	Note
	The number of records displayed on the **Network Detections** or **Email Messages** screen may differ from the number of events displayed on the **Triggered Alerts** screen because the related detection logs have been purged, or because appliances with related detections have been:
	
	    • Moved to the **Unmanaged** group
	
	    • Deleted from Deep Discovery Director (Internal Network Analytics Version)
	
	    • Unregistered from Deep Discovery Director (Internal Network Analytics Version)

Details	Click the icon to view the full alert details, including the list of recipients, subject, and message of the alert. **Note** For recurring plans, if you click the link in the email to open the Plan Results alert details, the screen displays information for the latest execution only.

Tip

The list view can be filtered by clicking the **Filters** button and using the drop-down lists and search box that appear.

Built-in Rules

The **Built-in Rules** screen displays the following information:

TABLE 7-4. Built-in Rules Columns

Column	Information
Alert Level	An alert can be classified as any of the following levels. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **Informational**: The event requires limited observation
Type	The type of rule that can trigger an alert can be any of the following: • **System**: A built-in, system related rule. • **Email Security**: An email security related rule. • **Network Security**: A network security related rule. • **Network Analytics**: A network analytics related rule.
Rule	The rule that triggers the alert. To edit a rule, click on any link in the **Rule** column.
Criteria	The summarized criteria of the rule.
Alert Frequency	The frequency at which the alert is generated when the rule criteria are met or exceeded.
Last Triggered	The date and time when the alert was last triggered.
Status	Click the toggle to enable or disable the rule.

Editing a Built-in Rule

Edit rules to modify the frequency at which alerts are generated, the criteria, and the alert recipients.

Note

• By default, built-in rules are enabled and configured to send alerts to all contacts with valid email addresses.

• Only the criteria of **Email Security** rules can be modified.

Procedure

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

   The **Built-in Rules** screen appears.

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

   The **Edit Rule** screen appears.

3. Toggle the status of this rule.

4. Configure how often alerts are generated:

   - **Check frequency**: Select the frequency at which the rule criteria are checked

   - **Alert frequency**: Select the frequency at which the alert is generated when the rule criteria are met or exceeded

   ---

   ![Note icon] **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 and custom rules are configured to immediately generate alerts if rule criteria are met or exceeded. Only the **Check frequency** can be modified.

   ---

5. For **Email Security** alerts, configure the following:

   - **Recipient watchlist**: Type an email address and press ENTER to add the specified email address to the recipient watchlist.

   - **Threshold**: Specify the detection threshold.

   - **Risk level**: Select the risk level and then click **Apply**.

6. (Optional) Select or disable **Send to all accounts**.

> **Note**
>
> This setting can be used in combination with the additional recipients field.

7. (Optional) Select a contact, type to search, or type an email address and press ENTER.

   The contact or account is added to the recipients.

8. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

   For more information, see *Token Variables on page 7-2*.

9. Click **Save**.

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

Custom Rules

The **Custom Rules** screen displays the following information:

TABLE 7-5. Custom Rules Columns

COLUMN	INFORMATION
Alert Level	An alert can be classified as any of the following levels. **Critical**: The event requires immediate attention **Important**: The event requires observation **Informational**: The event requires limited observation
Type	The type of rule that can trigger an alert can be any of the following: **Email Security**: An email security related rule. **Network Security**: A network security related rule.

COLUMN	INFORMATION
Rule	The rule that triggers the alert. To edit a rule, click on any link in the **Rule** column.
Criteria	The advanced search filter used as criteria for this rule.
Check Frequency	The frequency at which the rule criteria are checked.
Last Triggered	The date and time when the alert was last triggered.
Status	Click the toggle to enable or disable the rule.

Note

This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Adding a Custom Rule

Add custom rules based on saved search filters to be alerted of specific threats.

Note

A maximum of 500 custom rules can be added.

Procedure

1. Go to **Alerts** > **Custom Rules**, and then click **Add Rule**.

    The **Add Rule** screen appears.

2. Toggle the status of this rule.

3. Type a name for this rule.

4. Select the alert level to assign to this rule.

5. Click **Select Filter**, select a **Network Detections** or **Email Messages** saved search to use as criteria for this rule, and then click **Apply**.

> ⓘ **Important**
>
> Subsequent changes made to the selected filter will not be applied after the rule is created.

6. Do one of the following:

   - For **Network Detections** saved searches, select the appliances to include as data source of this rule.

   - For **Email Messages** saved searches, select domains from which email messages should be included in this rule.

7. Select the frequency at which the rule criteria are checked.

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

8. Specify the threshold.

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

10. (Optional) Select or disable **Send to all accounts**.

    > 📝 **Note**
    >
    > This setting can be used in combination with the additional recipients field.

11. (Optional) Select a contact, type to search, or type an email address and press ENTER.

    The contact or account is added to the recipients.

12. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

For more information, see *Token Variables on page 7-2*.

13. Click **Save**.

Other Custom Rules Tasks

You can also perform the following tasks:

TABLE 7-6. Other Tasks

TASK	DESCRIPTION
Edit a rule	Click on a rule name to open the **Edit Rule** screen and edit the rule. **Note** The advanced search filter used as criteria cannot be modified.
Delete rules	Select one or more rules to delete and then click **Delete**.
Toggle rule status	Click on the toggle in the **Status** column to enable or disable the rule.

Chapter 8

Reports

Learn how to generate and access Deep Discovery Director (Internal Network Analytics Version) scheduled and on-demand reports in the following topics.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

About Reports

Deep Discovery Director (Internal Network Analytics Version) provides reports to help you better understand complex threat scenarios, prioritize responses, and plan containment and mitigation.

All reports generated by are based on an operational report template.

Generate reports on demand or set a daily, weekly, or monthly schedule.

Generated Reports

The **Generated Reports** screen displays the following information:

TABLE 8-1. Generated Reports Columns

COLUMN	INFORMATION
Name	The name of the report.
Type	The type of the report can be any of the following: • **Email Security** **Note** Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances. This feature or screen will not contain any actual data or only display **No data to display.** • **Network Security**: A report generated from Deep Discovery Inspector appliance data.

Column	Information
Frequency	The frequency at which the report is generated can be any of the following: • **Daily** • **Weekly** • **Monthly** • **On demand**
Generated	The time the report was generated.
Download	Click the icon to download the report.

Viewing Generated Reports

Procedure

1. Go to **Reports** > **Generated Reports**.

2. Select a report type.

3. Select a frequency.

4. Select a time period.

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

6. (Optional) Click on the column titles to sort the list.

7. Click on the icon in the **Download** column to download and save the report in PDF format.

Deleting Generated Reports

Procedure

1. Go to **Reports** > **Generated Reports**.

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

Schedules

The **Schedules** screen displays the following information:

TABLE 8-2. Schedules Columns

	INFORMATION
Name	The name of the report.
Type	The type of the report can be any of the following: • **Email Security** > 📝 **Note** > Deep Discovery Director (Internal Network Analytics Version) does not support Deep Discovery Email Inspector appliances. > > This feature or screen will not contain any actual data or only display **No data to display.** • **Network Security**: A report generated from Deep Discovery Inspector appliance data.
Frequency	The frequency at which the report is generated can be any of the following: • **Daily** • **Weekly** • **Monthly**
Description	The description of the report.
Last Updated	The time the report schedule was last updated.
Last Generated	The time the report was last generated.

Viewing Schedules

Procedure

1. Go to **Reports** > **Schedules**.

2. Click the **Filter** button.

   Filter drop-down lists and a search box appear.

3. Select a report type.

4. Select a frequency.

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

6. (Optional) Click on the column titles to sort the list.

Adding a Schedule

Procedure

1. Go to **Reports** > **Schedules**.

2. Click **Add Schedule**.

   The **Add Schedule** screen appears.

3. Select the report type.

4. Type a name for this report.

5. Do one of the following:

   - For **Network Security** reports, select the appliances to include as data source.

   - For **Email Security** reports, select the domains from which email messages should be included.

6. (Optional) Type a description for this report.

7. (Optional) Type notes that will be displayed on the cover of this report.

8. Select the frequency at which this report is generated:

   - **Daily**: Select or type the time this report is generated at.

   - **Weekly**: Select the weekday and the time this report is generated at.

   - **Monthly**: Do one of the following:

     - Select **Full month report, generate on the first day of a month at**, and then select or type the time this report is generated at. The reporting period is the previous full month (day 1 to day 31).

     - Select **30-day report, start month on day**, and then select the day and the time this report is generated at. The reporting period is the last 30 days from the specified day (for example, from day 15 to day 15).

       > **Note**
       >
       > The report will start on the last day of the current month if the specified day (29, 30, or 31) does not exist.

9. Select the report content:

   - For **Network Security** reports:

     a. Select the hosts to include in this report:

        - To include all hosts, select **All monitored hosts**.

        - To only include certain hosts, select **Filtered hosts**, click **Select Filter**, select a **Affected Hosts** saved search to use as criteria, and then click **Apply**.

     b. Select the number of top hosts to include in this report.

   - For **Email Security** reports:

     a. Select whether to include detailed information in this report.

b. Select whether to include only inbound or outbound messages, or to include both inbound and outbound messages in this report.

10. (Optional) Select or disable **Send to all accounts**.

> ✎ **Note**
>
> This setting can be used in combination with the additional recipients field.

11. (Optional) Select an account, type to search, or type an email address and press ENTER.

   The account or email address is added to the recipients.

12. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

13. Click **Save**.

Editing a Schedule

Procedure

1. Go to **Reports** > **Schedules**.

2. Click the name of the report you want to edit.

   The **Edit Schedule** screen appears.

3. Modify the settings.

4. Click **Save**.

Deleting Schedules

Procedure

1. Go to **Reports** > **Schedules**.

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

On demand

Generate one-time reports anytime you need them. On-demand report are generated as soon as possible and are available for viewing immediately after they are generated.

Generating On-demand Reports

Procedure

1. Go to **Reports** > **On demand**.

2. Select the report type.

3. Type a name for this report.

4. Do one of the following:

   - For **Network Security** reports, select the appliances to include as data source.

   - For **Email Security** reports, select the domains from which email messages should be included.

5. (Optional) Type notes that will be displayed on the cover of this report.

6. Select the reporting period.

7. Select the report content:

   - For **Network Security** reports:

     a. Select the hosts to include in this report:

- To include all hosts, select **All monitored hosts**.

- To only include certain hosts, select **Filtered hosts**, click **Select Filter**, select a **Affected Hosts** saved search to use as criteria, and then click **Apply**.

b. Select the number of top hosts to include in this report.

- For **Email Security** reports:

a. Select whether to include detailed information in this report.

b. Select whether to include only inbound or outbound messages, or to include both inbound and outbound messages in this report.

8. (Optional) Select or disable **Send to all accounts**.

> **Note**
>
> This setting can be used in combination with the additional recipients field.

---

9. (Optional) Select an account, type to search, or type an email address and press ENTER.

   The account or email address is added to the recipients.

10. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

11. Click **Generate**.

   The new on-demand report appears in the **Generated Reports** screen.

Customization

Use the **Customization** screen to configure report cover options.

Customizing Reports

Procedure

1. Go to **Reports** > **Customization**.

2. Type a company name.

3. To display a company logo, select **Display company logo**, click **Select File** to locate an image file.

   > **Note**
   >
   > The image file must be in JPEG or PNG format and the file size cannot exceed 200 KB.

4. (Optional) Clear the **Display Trend Micro logo** check box if you do not want to display the Trend Micro logo on the report's cover page.

5. Click **Save**.

Chapter 9

Administration

Learn how to administer Deep Discovery Director (Internal Network Analytics Version) in the following topics.

Updates

Use the **Updates** screen, in **Administration** > **Updates**, to update components and install hotfixes, patches, and firmware upgrades to Deep Discovery Director (Internal Network Analytics Version).

Components

Deep Discovery Director (Internal Network Analytics Version) uses components to display related information about detections. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest threats.

Deep Discovery Director (Internal Network Analytics Version) automatically checks the availability of new components upon opening the **Components** screen.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Updating Components

Manually update components at any time.

Procedure

1. Go to **Administration** > **Updates** > **Components**.

    The **Component** screen appears.

2. Click **Update All**.

Configuring Component Update Settings

Configure Deep Discovery Director (Internal Network Analytics Version) to automatically update components

Procedure

1. Go to **Administration** > **Updates** > **Components**.

    The **Components** screen appears.

2. Click **Settings**.

    The **Component Update Settings** screen appears.

3. Select a source to download updates from:

    - **Trend Micro ActiveUpdate server**: The Trend Micro ActiveUpdate server is the default source for the latest components.

    - **Other update source**: Select this option to specify a different update source. The update source URL must begin with "http://" or "https://".

4. Select **Automatically check for updates**.

5. Select whether to update every few hours or daily at a specific time.

    > **Tip**
    > Trend Micro recommends setting the update frequency to every two hours.

6. Click **Save**.

Hotfixes / Patches

Use the **Hotfixes / Patches** screen, in **Administration** > **Updates** > **Hotfixes / Patches**, to install Deep Discovery Director (Internal Network Analytics Version) hotfixes and patches. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

TABLE 9-1. Hotfixes / Patches

SYSTEM UPDATE	DESCRIPTION
Hotfix	A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.
	Note
	A new hotfix may include previous hotfixes until Trend Micro releases a patch.
Patch	A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Non-Windows patches commonly include a setup script.

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

https://downloadcenter.trendmicro.com/

Installing a Hotfix / Patch

Procedure

1. Obtain the product update file from Trend Micro.

    - If the file is an official patch, download it from the download center.

        http://downloadcenter.trendmicro.com/

    - If the file is a hotfix, send a request to Trend Micro support.

2. Go to **Administration** > **Updates** > **Hotfixes / Patches**.

    The **Hotfixes / Patches** screen appears.

3. Click **Select** and select the product update file.

4. Click **Upload**.

5. Click **Install**.

> ⚠ **Important**
>
> - Some updates cannot be rolled back once installed.
>
> - Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.

Deep Discovery Director (Internal Network Analytics Version) installs the update and will automatically restart if it is required to complete the update.

6. Log on to the management console.

7. Go back to the **Administration** > **Updates** screen.

8. Verify that the hotfix / patch displays in the **History** section as the latest update.

Rolling Back a Hotfix / Patch

Deep Discovery Director (Internal Network Analytics Version) has a rollback function to undo an update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular hotfix or patch is applied.

> 📝 **Note**
>
> Rolling back a hotfix or patch will automatically restart Deep Discovery Director (Internal Network Analytics Version) if it is required to complete the rollback. Verify that all tasks on the management console have been completed before rollback.

Procedure

1. Go to **Administration** > **Updates** > **Hotfixes / Patches**.

2. In the **History** section, click **Roll Back**.

   Deep Discovery Director (Internal Network Analytics Version) will automatically restart if it is required to complete the rollback.

3. Log on to the management console.

4. Go back to the **Administration** > **Updates** > **Hotfixes / Patches** screen.

5. Verify that the hotfix or patch rollback is displayed as the most recent entry in the **History** section.

Firmware

Use the **Firmware** screen, in **Administration** > **Updates** > **Firmware**, to install a Deep Discovery Director (Internal Network Analytics Version) upgrade. Trend Micro prepares a readme file for each upgrade. Read the accompanying readme file before installing an upgrade for feature information and for special installation instructions.

Installing a Firmware Upgrade

Procedure

1. Go to **Administration** > **Updates** > **Firmware**.

   The **Firmware** screen appears.

2. Click **Select** and select the firmware upgrade file.

3. Click **Upload**.

4. Click **Install**.

> **Important**
>
> • Deep Discovery Director (Internal Network Analytics Version) does not allow the installation of firmware upgrades when the license status is **Not Activated** or **Expired**.
>
> • Firmware upgrades cannot be rolled back once installed.
>
> • Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the server until upgrading is complete.

Deep Discovery Director (Internal Network Analytics Version) will automatically restart after the upgrade is complete.

5. Log on to the management console.

6. Go back to the **Administration** > **Updates** > **Firmware** screen.

7. Verify that the firmware version is correct.

Integrated Products/Services

Deep Discovery Director (Internal Network Analytics Version) integrates with other products and services.

Deep Discovery Director

The **Deep Discovery Director** screen, under **Administration** > **Integrated Products/Services**, is only available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Deep Discovery Director (Internal Network Analytics Version) cannot function by itself when operating in **Standalone Network Analytics mode** and must register to another Deep Discovery Director (Internal Network Analytics Version) or **Deep Discovery Director (Consolidated Mode)** server.

For details, see *Operation Mode on page 9-47*.

The **Deep Discovery Director** screen displays the following information:

FIELD	INFORMATION
Status	Displays either **Registered	Connected**, **Registered	Not connected**, or **Registered	Untrusted fingerprint**.
Last connected	Displays the date and time Deep Discovery Director (Internal Network Analytics Version) last connected to the specified **Deep Discovery Director** server.
Host name	Displays the host name of the specified **Deep Discovery Director** server.
Server address	The **Deep Discovery Director** server address.
Port	The **Deep Discovery Director** server port.
API key	The **API key** obtained from the **Deep Discovery Director** server management console.
Fingerprint (SHA-256)	The **Deep Discovery Director** server fingerprint. **Note** If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the **Deep Discovery Director** server fingerprint is valid and then click **Trust**.

Registering to Deep Discovery Director

The following procedure is for registering to Deep Discovery Director. If you have already registered and want to change the connection settings, you must first unregister.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.

2. Type the **Server Address**.

3. Type the **Port** number.

4. Type the **API key**.

> ✎ **Note**
>
> You can find this information on the **Help** screen on the management console of Deep Discovery Director.

5. Click **Register**.

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

> ✎ **Note**
>
> If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust**.
>
> After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.

Unregistering from Deep Discovery Director

Follow this procedure to unregister from Deep Discovery Director or before registering to another Deep Discovery Director.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.

2. Click **Unregister**.

Deep Discovery Director (Internal Network Analytics Version) unregisters from **Deep Discovery Director**.

Apex Central

Trend Micro Apex Central is a software management solution that gives you the ability to control antivirus and content security programs from a central location, regardless of the program's physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

Important

- Deep Discovery Director (Internal Network Analytics Version) integrates with Trend Micro Apex Central for the express purpose of retrieving endpoint analysis reports to provide Deep Discovery Director - Network Analytics with even more data for more thorough advanced threat analysis.

- The management of Deep Discovery appliances and the sharing of threat intelligence will continue to be handled by Deep Discovery Director (Internal Network Analytics Version).

The **Apex Central** screen displays the following information.

Note

This feature or screen is read-only when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

FIELD	INFORMATION
Server type	Deep Discovery Director (Internal Network Analytics Version) can integrate with the on-premises version or the software as a service version of Trend Micro Apex Central. **Note** If proxy settings are enabled, Deep Discovery Director (Internal Network Analytics Version) connects to **Apex Central as a Service** using the proxy server.
Status	Displays either **Connected to Apex Central**, **Not connected to Apex Central**, or **N/A**.
Last connected	Displays the date and time Deep Discovery Director (Internal Network Analytics Version) last connected to Trend Micro Apex Central.
Endpoint Sensor license	Displays either **Activated** or **Not activated**.
Apex Central server address	The Trend Micro Apex Central server address.
Port	The Trend Micro Apex Central port.
Application ID	The **Application ID** generated on the Trend Micro Apex Central console for Deep Discovery Director (Internal Network Analytics Version).
API key	The **API key** generated on the Trend Micro Apex Central console for Deep Discovery Director (Internal Network Analytics Version).

Configuring Apex Central Settings

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Apex Central**.

    The **Apex Central** screen appears.

2. Select **Retrieve endpoint analysis reports from Apex Central**.

> **Important**
>
> - On the Trend Micro Apex Central console, go to **Administration** > **Settings** > **Automation API Access Settings** to add Deep Discovery Director (Internal Network Analytics Version) as application.
>
> - Endpoint Sensor must be configured in Trend Micro Apex Central to enable this feature.

3. Select the **Server type**.

4. Type the IP address or FQDN of the Trend Micro Apex Central server.

5. Type the port of the Trend Micro Apex Central server.

6. Type the **Application ID** generated on the Trend Micro Apex Central console for Deep Discovery Director (Internal Network Analytics Version).

7. Type the **API key** generated on the Trend Micro Apex Central console for Deep Discovery Director (Internal Network Analytics Version).

8. (Optional) Click **Test Connection**.

9. Click **Save**.

LDAP

Deep Discovery Director (Internal Network Analytics Version) integrates with LDAP servers for user-group definition and administrator privileges.

Deep Discovery Director (Internal Network Analytics Version) supports the following types of directory servers:

- Microsoft Active Directory on Windows Server 2016 and 2019

- Microsoft AD Global Catalog on Windows Server 2016 and 2019

- OpenLDAP

The following table describes the tasks that you can perform on the **LDAP** screen.

Task	Description
Add an LDAP server	Click **Add** to add a new directory server.
	Deep Discovery Director (Internal Network Analytics Version) supports up to ten directory servers.
	For more information, see *Configuring an LDAP Server on page 9-13*.
Edit an LDAP server	Click a server name to edit the settings.
	For more information, see *Configuring an LDAP Server on page 9-13*.
Enable or disable an LDAP server	Toggle the button in the **Status** column to:
	• Enable the LDAP server that you selected to enable on the configuration screen
	• Disable both primary and secondary LDAP servers
Synchronize directory information	Click **Sync All** to synchronize directory information with all the LDAP servers.
Delete a directory server	Click **Delete** to remove one or more selected entries.

Configuring an LDAP Server

Procedure

1. Obtain the information required to configure LDAP integration from the server administrator.

2. Go to **Administration** > **Integrated Products/Services** > **LDAP**.

3. Do one of the following:

    • Click **Add** to add a new entry.

    • Click a name to change the server settings.

4. Select to enable or disable the server.

5. Select a server type.

6. Specify the name of the server.

7. Configure the server settings (server address, access protocol, and port number).

Note

Trend Micro recommends using the following default ports:

- For Microsoft Active Directory, or OpenLDAP:

  - **SSL**: 636

  - **STARTTLS**: 389

- For Microsoft AD Global Catalog:

  - **SSL**: 3269

  - **STARTTLS**: 3268

---

8. Configure administrative settings for the LDAP server.

   The following table provides the configuration recommendations for each supported LDAP server type.

LDAP Server Type	User Name (example)	Base Distinguished Name (example)
Active Directory	user1@domain.com (UPN)	dc=domain, dc=com
Active Directory Global Catalog	user1@domain.com (UPN)	dc=domain, dc=com dc=domain1,dc=com (if multiple unique domains exist)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com

   a. Type the base distinguished name.

   b. Select an email address attribute option to apply policy settings based on the address information.

c. Type the user name.

d. Type the password.

e. (Optional) If your organization uses a CA certificate, select **Use CA certificate** and click **Select** to locate the CA certificate file.

9. If the LDAP server uses filter settings other than the default, specify the **User filter** and **Group filter**.

10. (Optional) Click **Test Connection** to verify that a connection to the LDAP server can be established using the specified information.

11. Click **Save**.

SAML Authentication

Security Assertion Markup Language (SAML) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports single sign-on (SSO), a technology that allows for a single user login to work across multiple applications and services. When you configure SAML settings in Deep Discovery Director (Internal Network Analytics Version), users signing in to your organization's portal can seamlessly sign in to Deep Discovery Director (Internal Network Analytics Version) without an existing Deep Discovery Director (Internal Network Analytics Version) account.

In SAML single sign-on, a trust relationship is established between the identity provider (IdP) and the service provider (SP) by using SAML metadata files. The identity provider contains the user identity information stored on a directory server. The service provider (which in this case is Deep Discovery Director (Internal Network Analytics Version)) uses the user identity information from the identity provider for user authentication and authorization.

Deep Discovery Director (Internal Network Analytics Version) supports the following identity providers for single sign-on:

- Microsoft Active Directory Federation Services (AD FS) 4.0 or 5.0

- Okta

To connect Deep Discovery Director (Internal Network Analytics Version) to your organization environment for single-sign-on, complete the following:

1. Access the Deep Discovery Director (Internal Network Analytics Version) management console to obtain the service provider metadata file.

   You can also update the certificate in Deep Discovery Director (Internal Network Analytics Version).

2. In your identity provider:

   a. Configure the required settings for single sign-on.

   b. Obtain the metadata file.

   For more information, see the documentation that comes with your identity provider.

3. In Deep Discovery Director (Internal Network Analytics Version):

   a. Import the metadata file for your identity provider.

   b. Create SAML user groups.

Service Provider Metadata and Certificate

Obtain the service provider metadata from Deep Discovery Director (Internal Network Analytics Version) to provide to your identity provider.

On the **SAML Authentication** screen, the Service Provider section displays the following service provider information:

- **Entity ID**: Identifies the service provider application

- **Single Sign On URL:** The endpoint URL responsible for receiving and parsing a SAML assertion (also referred to as "Assertion Consumer Service")

- **Single Sign Off URL:** The endpoint URL responsible for initiating the SAML logout process

- **Certificate:** The encryption certificate (verification certificate) in X.509 format

You can click the following in the Service Provide section:

- **Download Metadata**: Downloads the Deep Discovery Director (Internal Network Analytics Version) metadata file. You can import the metadata file on an Active Directory Federal Services (ADFS).

> **Note**
>
> If you change the Deep Discovery Director (Internal Network Analytics Version) FQDN after importing the metadata file on your identity provider, you will need to download the metadata file again and reimport the file on your identity provider.

- **Download Certificate**: Downloads the Deep Discovery Director (Internal Network Analytics Version) certificate file.

- **Update**: Uploads a new certificate on Deep Discovery Director (Internal Network Analytics Version). The certificate must meet the following specifications:

    - The certificate must be in X.509 PEM format.

    - The certificate must not be protected by a password or pass phrase.

    - Certificates from a private CA or a CA chain must include **Authority Information Access** and **CRL Distribution Points**.

Configuring Identity Provider Settings

> **Note**
>
> - Before you add an identity provider, obtain the metadata file from your identity provider.
>
> - You can add up to two identity providers in Deep Discovery Director (Internal Network Analytics Version), one each for AD FS and Okta.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **SAML Authentication**.

2. In the Identity Provider section, do one of the following:

    • In the drop-down box above the table, select **Custom Identity Provider** to add or view your Identity Providers, or select **Internal Identity Provider** to view to view the internal Identity Provider used for Vision One.

    > **Note**
    >
    > The drop-down box only appears when Deep Discovery Director (Internal Network Analytics Version) is integrated with Vision One.

    • Click **Add** to add a new entry.

    • Click an identity provider service name to change the settings.

3. Select a status option to enable or disable the identity provider settings.

4. Type a descriptive name for the identity provider.

    > **Note**
    >
    > Deep Discovery Director (Internal Network Analytics Version) displays the service name in the drop-down list on the Log On screen.

5. Type a description.

6. Click **Select** and choose the metadata file obtained from your identity provider.

    After importing the metadata file, the system displays the identity provider information.

7. Click **Save**.

Configuring Okta

Okta is a standards-compliant OAuth 2.0 authorization server that provides cloud identity solutions for your organization. Okta is a single sign-on provider that allows you to manage user access to Deep Discovery Director (Internal Network Analytics Version).

This section describes how to configure Okta as a SAML (2.0) identity provider for Deep Discovery Director (Internal Network Analytics Version) to use.

Before you begin configuring Okta, make sure that:

- You have a valid subscription with Okta that handles the sign-in process and that eventually provides the authentication credentials to the Deep Discovery Director (Internal Network Analytics Version) management console.

- You are logged on to the management console as a Deep Discovery Director (Internal Network Analytics Version) administrator.

Procedure

1. Log in to your Okta organization as a user with administrative privileges.

2. Click **Admin** in the upper right, and then navigate to **Applications** > **Applications**.

3. Click **Add Application**, and then click **Create New App**.

   The **Create a New Application Integration** screen appears.

4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.

5. On the **General Settings** screen, type a name for Deep Discovery Director (Internal Network Analytics Version) in **App name**, for example, "Deep Discovery Director (Internal Network Analytics Version)", and click **Next**.

6. On the **Configure SAML** screen, specify the following:

a. Type the **Single sign on URL** for Deep Discovery Director (Internal Network Analytics Version).

> **Note**
>
> To obtain the Deep Discovery Director (Internal Network Analytics Version) single sign on URL, go to **Administration** > **Integrated Products/Services** > **SAML Integration** in the Deep Discovery Director (Internal Network Analytics Version) management console, and copy the **Single Sign On URL** in the **Service Provider** section.

b. Select **Use this for Recipient URL and Destination URL**.

c. Specify the Audience URI in **Audience URI (SP Entity ID)** based on your serving site:

d. Type `EmailAddress` in **Name ID format**.

e. In the **Group Attribute Statements (Optional)** section, specify the following:

- **Name**: `DDD_GROUP`
- **Name format**: `Unspecified`
- **Filter**: Select **Matches regex** and type `^(.*)$`

f. Click **Next**.

7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, select **This is an internal app that we have created**, and then click **Finish**.

The **Sign On** tab of your newly created Deep Discovery Director (Internal Network Analytics Version) application appears.

8. Click **Identity Provider Metadata** to download the metadata file from Okta.

> **Note**
>
> Import this metadata file to Deep Discovery Director (Internal Network Analytics Version).

9. Assign the application to groups and add people to groups.

   a. Select **Directory** > **Groups**.

   b. Click the groups that you want to assign the application to, and then click **Manage Apps**.

      The **Assign Applications** screen appears.

   c. Locate Deep Discovery Director (Internal Network Analytics Version) you added and click **Assign**.

   d. Click **Manage People**.

      The **Add People to Groups** screen appears.

   e. Locate the user you want to allow access to Deep Discovery Director (Internal Network Analytics Version) and add the user to the Deep Discovery Director (Internal Network Analytics Version) group.

   f. Confirm that the application is assigned to the user and group.

      After assigning an application to a group, the system automatically assigns the application to all users in the group.

   g. Repeat the above steps to assign the application to more groups as necessary.

   You are now ready to configure Okta for single sign-on and create the required SAML groups in the Deep Discovery Director (Internal Network Analytics Version) management console.

Configuring Active Directory Federation Services

This section describes how to configure a federation server using Active Directory Federation Services (AD FS) to work with Deep Discovery Director (Internal Network Analytics Version).

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) supports connecting to the federation server using AD FS 4.0 and 5.0.

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

Before you begin configuring AD FS, make sure that:

- You have a Windows Server installed with AD FS 4.0 or AD FS 5.0 to serve as a federation server.

- You are logged on to the management console as a Deep Discovery Director (Internal Network Analytics Version) administrator.

- You have obtained the metadata file from Deep Discovery Director (Internal Network Analytics Version).

- You have enabled Windows Integrated Authentication on the federation server.

  For details, see *Enabling Windows Integrated Authentication on AD FS on page 9-25*.

- You have configured web browser settings on each endpoint to trust Deep Discovery Director (Internal Network Analytics Version) and the federation server.

  For details, see *Configuring Endpoints for Single Sign-on through AD FS on page 9-27*.

Procedure

1. Go to **Start** > **All Programs** > **Administrative Tools** to open the AD FS management console.

2. Click **AD FS** in the left navigation, and under the **Action** area on the right, click **Add Relying Party Trust…**.

3. Complete settings on each tab of the **Add Relying Party Trust Wizard** screen.

    a. On the **Welcome** tab, select **Claims aware** and click **Start**.

    b. On the **Select Data Source** tab, select **Import data about the relying party from a file**, click **Browse** to select the metadata file you obtain from Deep Discovery Director (Internal Network Analytics Version); then, click **Next**.

    c. On the **Specify Display Name** tab, specify a display name for Deep Discovery Director (Internal Network Analytics Version), for example, "Deep Discovery Director (Internal Network Analytics Version)", and click **Next**.

    d. On the **Choose Access Control Policy** tab, select **Permit everyone** and click **Next**.

    e. On the **Ready to Add Trust** tab, click **Next**.

    f. On the **Finish** tab, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** and click **Close**.

        The **Edit Claim Rules** screen appears.

4. On the **Issuance Transform Rules** tab, click **Add Rule…**.

5. Complete the settings on each tab of the **Add Transform Claim Rule Wizard** screen.

    a. On the **Choose Rule Type** tab, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list, and click **Next**.

    b. On the **Configure Claim Rule** tab, specify a claim rule name in the **Claim rule name** text box, and select **Active Directory** from the **Attribute store** drop-down list.

    c. Select the **User-Principal-Name** LDAP attribute and specify **Name ID** as the outgoing claim type for the attribute.

    d. Click **OK**.

6. Click **Add Rule…**.

The **Add Transform Claim Rule Wizard** screen appears.

7. Complete the settings on each tab of the **Add Transform Claim Rule Wizard** screen.

   a. On the **Choose Rule Type** tab, select **Send Group Membership as a Claim** from the **Claim rule template** drop-down list, and click **Next**.

      The **Configure Claim Rule** tab appears.

   b. For **Claim rule name**, type the name of the AD group.

   c. For **User's group**, click **Browse** and then select the AD group.

   d. For **Outgoing claim type**, type `DDD_GROUP`.

   e. For **Outgoing claim value**, type the name of the AD group.

   f. Click **Apply** and then click **OK**.

8. Collect the single sign-on URL and export the Identity Provider metadata for AD FS.

   a. On the AD FS management console, go to **AD FS** > **Service** > **Endpoints**.

   b. In the right pane, under **Endpoints** > **Metadata**, in the **Federation Metadata** row, copy the URL path.

   c. Add the host name of the AD FS computer to the URL path that you copied.

      For example, `https://hostname/FederationMetadata/2007-06/FederationMetadata.xml`

   d. To retrieve the Identity Provider metadata, use a web browser to navigate to the complete URL that you obtained in the previous step.

   e. Save the Identity Provider metadata file as an XML file.

Enabling Windows Integrated Authentication on AD FS

Windows Integrated Authentication (WIA) allows users to single sign-on
to Deep Discovery Director (Internal Network Analytics Version) using the
domain credentials they used to sign on to an endpoint.

Procedure

1. Log on to a Windows Server installed with AD FS 4.0 or AD FS 5.0.

2. Go to **Start** > **All Programs** > **Administrative Tools** to open the AD FS
   management console.

3. Select **AD FS** > **Service** > **Authentication Methods** in the left
   navigation, and under the **Actions** area on the right, click **Edit Primary
   Authentication Methods...**.

4. On the **Primary** tab, under **Intranet**, ensure that **Windows
   Authentication** is enabled.

5. Click **OK**.

6. Log on to your **Domain Controller**.

7. Go to **Start** > **All Programs** > **Administration Tools** > **Group Policy
   Management**.

8. Select **User Configuration** > **Policies** > **Administrative Templates** >
   Windows Components > **Internet Explorer** > **Internet Control Panel**
   > **Security Page**.

9. Double-click **Site to Zone Assignment List** to configure the settings.

10. Select **Enabled**.

11. Under **Options**, click **Show**.

12. Add the Deep Discovery Director (Internal Network Analytics Version) management console URL as **Value name** with a **Value** of `1`.

13. Click **OK.**

    The Deep Discovery Director (Internal Network Analytics Version) management console URL is added to the **Intranet zone**.

14. Select **User Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page** > **Intranet Zone**.

15. Double-click **Logon options** to configure the settings.

16. Select **Enabled**.

17. Under **Options**, click **Automatic logon with current username and password**.

18. Click **OK**.

    This enables web browsers to automatically log on to the Deep Discovery Director (Internal Network Analytics Version) management console with their current user name and password.

19. Deploy the updated group policy to your endpoints.

    > **Note**
    >
    > If group policy deployment is blocked by the Windows Firewall, add an inbound rule to allow the deployment, and execute `gpudate /force` in an administrator command prompt on your endpoints to force endpoints to accept the new firewall policy.

    Users who signed on to their endpoint using their domain credentials should now be able to single-sign on to Deep Discovery Director (Internal Network Analytics Version).

Configuring Endpoints for Single Sign-on through AD FS

Before endpoints can access Deep Discovery Director (Internal Network Analytics Version) using single sign-on through Active Directory Federation Services (AD FS), configure the web browser settings on each endpoint to trust both Deep Discovery Director (Internal Network Analytics Version) and the federation server.

You can configure the web browser settings on endpoints manually or through group policies.

The following provides the procedure for endpoints running Windows 10. Steps may vary depending on the Windows version.

Procedure

1. On an endpoint, open the **Control Panel** from the Start menu.

2. Click **Network and Internet** > **Internet Options**.

   The Internet Properties screen appears.

3. Click the **Security** tab.

4. Select **Local intranet** and click **Sites**.

5. Click **Advanced**.

6. In the **Add this website to the zone** field, type FQDN or IP address of the account federation server and click **Add**.

7. Repeat Step 6 to add the FQDN or IP address of Deep Discovery Director (Internal Network Analytics Version) to the Websites list.

8. Click **Close**.

9. Click **OK**.

10. Click **OK**.

Syslog

Use the **Syslog** screen to configure Deep Discovery Director (Internal Network Analytics Version) to send suspicious objects lists and Deep Discovery appliance logs to up to three syslog servers.

Note

This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Adding a Syslog Server Profile

Procedure

1. Go to **Adminstration** > **Integrated Products/Services** > **Syslog**, and then click **Add**.

    The **Add Syslog Server Profile** dialog appears.

2. Select the status of this server profile.

3. Type a unique profile name for the syslog server.

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

5. (Optional) Modify the port number.

    Note

    Trend Micro recommends using the following default syslog ports:

    - **SSL/TLS**: 6514
    - **TCP**: 601
    - **UDP**: 514

    ---

6. Select the protocol to be used when transporting log content to the syslog server.

7. Select the scope of the data to send to the syslog server.

8. Click **Save**.

Other Syslog Tasks

You can also perform the following tasks:

Task	Description
Edit a syslog server profile	Click on a server profile name to open the **Edit Syslog Server Profile** dialog and do the following: • Toggle the status • Modify the profile name • Modify the server address • Modify the port number • Change the protocol **Note** Modifying the server address or changing the protocol resends all suspicious objects lists.
Delete syslog server profiles	Select one or more syslog server profiles to delete and then click **Delete**. **Note** Queued detection and appliance logs will be discarded and not sent to deleted syslog servers.
Toggle syslog server profile status	Click on the toggle in the **Status** column to enable or disable the syslog server profile. **Note** Disabling a server profile causes queued detection and appliance logs to be discarded.

Network Analytics

Deep Discovery Director (Internal Network Analytics Version) provides advanced threat analysis for data correlations made between detections selected in the management console and other related events as they occur over time.

Deep Discovery Director (Internal Network Analytics Version) integrates with Deep Discovery Inspector to provide advanced protection against cyber threats and attacks that could threaten your network.

Use the **Network Analytics** screen, in **Administration** > **Network Analytics**, to view the status of Deep Discovery Director (Internal Network Analytics Version) and configure data sources.

To configure additional settings that will help you make the most of Deep Discovery Director (Internal Network Analytics Version), go to **Appliances** > **Network Assets**.

For more information, see *Network Assets on page 6-30*.

Server Information

Use the **Server Information** screen, in **Administration** > **Network Analytics** > **Server Information**, to view the status and basic information of all registered Deep Discovery Director - Network Analytics servers.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Data Sources

Use the **Data Sources** screen, in **Administration** > **Network Analytics** > **Data Sources**, to display and configure from which Deep Discovery Inspector appliances Deep Discovery Director (Internal Network Analytics Version) draws data for advanced threat analysis.

The **Data Sources** screen displays the following information:

TABLE 9-2. Data Sources Columns

COLUMN	INFORMATION
Display Name	The display name of the Deep Discovery Inspector appliance.
Host Name	The host name of the Deep Discovery Inspector appliance.
IP Address	The IP address of the Deep Discovery Inspector appliance.
Connected Network Analytics	The display name of the connected Deep Discovery Director - Network Analytics server.
Connection Status	The connection status of the Deep Discovery Director - Network Analytics server.
Version	The version of the Deep Discovery Inspector appliance.
Appliance Proxy Settings	Displays either **Enabled** or **Disabled**, depending on whether the Deep Discovery Inspector appliance's proxy settings are used.
Bandwidth	The bandwidth the Deep Discovery Inspector appliance consumes.
Last Synchronized	Date and time data was last synced from the Deep Discovery Inspector appliance.
Test Connection	Date and time the Deep Discovery Inspector appliance established connection to Deep Discovery Director - Network Analytics as a Service. Click **Test Connection** to have the Deep Discovery Inspector appliance try to connect to Deep Discovery Director - Network Analytics as a Service.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Configuring Data Sources

Procedure

1. Go to **Administration** > **Network Analytics** > **Data Sources**.

   The **Data Sources** screen appears.

2. Select one or more appliances and then click **Configure**.

3. Select one of the following.

   - **Individually**: Configure the settings of each Deep Discovery Inspector appliance individually.

   - **Collectively**: Configure the settings of all selected Deep Discovery Inspector appliances collectively.

   The **Configure Data Sources** dialog appears.

4. Configure the data sources.

   - **Individually**:

     a. Select the **Network Analytics** server to connect each Deep Discovery Inspector appliance to.

     b. Select whether to use each Deep Discovery Inspector appliance's proxy settings.

   - **Collectively**:

     a. Select whether to keep all current connections or specify a **Network Analytics** server to connect all Deep Discovery Inspector appliances to.

     b. Select whether to keep, enable or disable all Deep Discovery Inspector appliances' proxy settings.

5. Click **Save**.

   All settings are immediately applied to all appliances. You cannot perform additional configuration until the previous settings have been applied.

System Settings

The System Settings screen, in **Administration** > **System Settings**, includes the following.

Network

Use this screen to configure the host name or fully qualified domain name, IP address, and other network settings of the Deep Discovery Director (Internal Network Analytics Version) appliance.

Modify the IP address immediately after completing all deployment tasks.

> **Note**
> You can also use the preconfiguration console to modify the network settings.

> **Important**
>
> - Deep Discovery Director (Internal Network Analytics Version) uses the specified IP address to connect to the Internet. The IP address also determines the URL used to access the management console.
>
> - Changing the IP address causes the following:
>
>   - Registered Deep Discovery appliances must reregister using the updated IP address.
>
>   - Products and services using Deep Discovery Director (Internal Network Analytics Version) threat intelligence sharing URLs must be configured to use the updated URLs.
>
>   - Products and services that integrate with Deep Discovery must configure their settings to use the updated IP address.
>
>   - Products and services using web API to access Deep Discovery Director (Internal Network Analytics Version) must be configured to use the updated IP address.

Using Host Name as the Identity

Deep Discovery Director (Internal Network Analytics Version) supports using the host name instead of the IP address as the identity of the server.

When this feature is selected, appliances connect to Deep Discovery Director (Internal Network Analytics Version) using the host name to download files required to execute plans.

> **⚠ Important**
>
> - The host name must be resolvable within your network.
>
> - Changing the host name affects the following:
>
>   - Registered Deep Discovery appliances must reregister using the updated host name.
>
>   - Products and services using Deep Discovery Director (Internal Network Analytics Version) threat intelligence sharing URLs must be configured to use the updated URLs.
>
>   - Products and services that integrate with Deep Discovery must configure their settings to use the updated host name.
>
>   - Products and services using web API to access Deep Discovery Director (Internal Network Analytics Version) must be configured to use the updated host name.

Procedure

1. Select **Use host name instead of IP address as the identity of this server**.

2. Configure the IP address and other network settings.

3. Click **Save**.

Configuring Port Binding

Deep Discovery Director (Internal Network Analytics Version) supports the binding of services to a second network port.

When this feature is selected, Deep Discovery Director (Internal Network Analytics Version) directs all connections to the threat intelligence feeds, the license update server, and Active Update servers through eth1.

> **Note**
>
> This feature cannot be configured from the preconfiguration console.

Procedure

1. Select **eth0 (management) and eth1** to bind your services to.

   > **Important**
   >
   > This feature requires at least two network interface cards to be installed and configured. The feature will be hidden from the **Network** screen otherwise.

   A new **eth1** section to configure network settings for the second network port displays under the existing **eth0 (management)** section.

2. Configure the IP address and other network settings of the second network port.

3. Click **Save**.

Using IPv4 and IPv6 Dual Stack

Deep Discovery Director (Internal Network Analytics Version) supports IPv4 and IPv6 dual-stack configuration to function in network environments that communicate using the IPv6 protocol.

Procedure

1. Select **IPv4 and IPv6 (dual stack)** as **Type**.

   A new section to configure IPv6 settings displays between the existing IPv4 and DNS settings.

2. Configure the IPv6 settings.

3. Click **Save**.

Proxy

Deep Discovery Director (Internal Network Analytics Version) can be configured to use a proxy server to connect to the Internet. The proxy server will also be used to connect to the following features/services:

- **Apex Central as a Service**
- **Threat Connect**
- Threat intelligence feeds
- License update server
- Active Update servers

> **Note**
> When port binding is configured, only eth1 will use the proxy settings.

Procedure

1. Go to **Administration** > **System Settings** > **Proxy**.

   The **Proxy** screen appears.

2. Select **Use a proxy server to connect to the Internet**.

3. Type the IPv4 address or FQDN of the proxy server.

4. Type the port number. The default port number is **80**.

5. (Optional) If your proxy server requires authentication, select **Specify authentication credentials**, and then type the user name and password used for authentication.

6. (Optional) Click **Test Connection** to verify the connection to the proxy server.

7. Click **Save**.

SMTP

Use the **SMTP** screen, in **Administration** > **System Settings** > **SMTP**, to enable using a SMTP server to send alert notifications through email.

Procedure

1. Go to **Administration** > **System Settings** > **SMTP**.

    The **SMTP** screen appears.

2. Select **Use a SMTP server**.

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

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

5. (Optional) Modify the port number.

6. Type a sender email address.

7. (Optional) If the SMTP server requires authentication, select **SMTP server requires authentication**, and then type the user name and password used for authentication.

    > **WARNING!**
    > Verify that the user name and password are valid. Connections made using an incorrect user name and password may cause some SMTP servers to reject all network request originating from Deep Discovery Director (Internal Network Analytics Version).

8. (Optional) Verify that Deep Discovery Director (Internal Network Analytics Version) 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 (Internal Network Analytics Version) can communicate with the specified SMTP server, an email with the

predefined subject and message will be sent to the specified email addresses.

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

SNMP

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

Use the **Administration** > **System Settings** > **SNMP** screen to perform the following tasks:

- Configure Deep Discovery Director (Internal Network Analytics Version) to send trap messages.

  For details, see *Configuring Trap Messages on page 9-39*.

- Configure Deep Discovery Director (Internal Network Analytics Version) to listen for manager requests.

  For details, see *Configuring Manager Requests on page 9-41*.

Configuring Trap Messages

A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.

2. Under **Trap Messages**, select **Send SNMP trap messages**.

3. Specify the trap message settings.

Option	Description
Manager server address	Specify the manager server address.

SNMP version	Select the SNMP version:
	
	• SNMPv1/SNMPv2c
	
	• SNMPv3
	
	    If you use SNMPv3, configure the SNMP server as follows:
	
	      • Context Name: `""` (default context)
	
	      • Context Engine ID: `<Auto>`
	
	      • (Optional) Authentication protocol: `HMAC-SHA`
	
	      • (Optional) Privacy protocol: `CBC-AES-128`

Community name	Specify a community name.
Security model	**Note** This field is only available for SNMPv3. Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	**Note** This field is only available for SNMPv3. Specify the user name.
Password	**Note** This field is only available for SNMPv3. Specify the password.

OPTION	DESCRIPTION
Privacy passphrase	**Note** This field is only available for SNMPv3. Specify the privacy passphrase.

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

   Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request Deep Discovery Director (Internal Network Analytics Version) system information.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.

2. Under **Manager Requests**, select **Listen for requests from SNMP managers**.

3. Specify the manager request settings.

OPTION	DESCRIPTION
Device location	Specify the location of this appliance.
Administrator contact	Specify the administrator contact of this appliance.

OPTION	DESCRIPTION

SNMP version	Select the SNMP version:
	
	 • SNMPv1/SNMPv2c
	
	 • SNMPv3
	
	   If you use SNMPv3, configure the SNMP server as follows:
	
	     • Context Name: `""` (default context)
	
	     • Context Engine ID: `<Auto>`
	
	     • (Optional) Authentication protocol: `HMAC-SHA`
	
	     • (Optional) Privacy protocol: `CBC-AES-128`

Allowed community names	Specify a maximum of 5 community names.
Security model	**Note** This field is only available for SNMPv3. Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	**Note** This field is only available for SNMPv3. Specify the user name.
Password	**Note** This field is only available for SNMPv3. Specify the password.

Option	Description
Privacy passphrase	**Note** This field is only available for SNMPv3. Specify the privacy passphrase.
Trusted manager server addresses	Specify a maximum of 5 trusted manager server addresses.

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

Bandwidth

Use the **Bandwidth** screen, in **Administration** > **System Settings** > **Bandwidth**, to enable bandwidth usage throttling settings. Bandwidth usage throttling helps manage the impact downloading and uploading of files may have on your network and internet connection.

For details, see *Configuring Bandwidth Usage Throttling on page 9-43*.

Configuring Bandwidth Usage Throttling

Procedure

1. Go to **Administration** > **System Settings** > **Bandwidth**.

The **Bandwidth** screen appears.

2. Select **Enable bandwidth usage throttling**.

3. Type a speed limit value to limit the speed per connection for downloading files from Deep Discovery Director (Internal Network

Analytics Version) to the appliance. Each appliance establishes one connection.

4. Type a maximum value to limit the number of connections to.

5. Click **Save**.

Time

Configure date and time settings immediately after installation.

Procedure

1. Go to **Administration** > **System Settings** > **Time**.

   The **Time** screen appears.

2. Select one of the following methods and configure the applicable settings.

   - Select **Connect to an NTP server** and type the FQDN or IP address of the NTP server.

   - Select **Set manually** and configure the time.

3. Select the applicable time zone.

   > **Note**
   >
   > Daylight Saving Time (DST) is used when applicable.

4. Select the preferred date and time format.

5. Click **Save**.

Certificate

Digital certificates are electronic documents that are used to create secure connections between clients and servers or websites. A valid and trusted certificate ensures clients that they are connecting to a trusted server or website, and helps protect against man-in-the-middle attacks.

Certificates become trusted by going through a validation process of a Certificate Authority (CA). Certificate Authorities themselves are usually third-party companies that are trusted by both the client and server or website.

On first installation, Deep Discovery Director (Internal Network Analytics Version) creates a self-signed SSL certificate that will be used to securely communicate with other Deep Discovery appliances and Local Repository. In doing so, Deep Discovery Director (Internal Network Analytics Version) also acts as its own CA.

Users who wish to adopt their own organizations' CA can import a certificate signed by that CA to Deep Discovery Director (Internal Network Analytics Version).

> **Important**
>
> Accessing the management console of a Deep Discovery Director (Internal Network Analytics Version) server with an untrusted or expired certificate displays a security warning in the web browser.
>
> An untrusted or expired certificate does not affect the communication between Deep Discovery Director (Internal Network Analytics Version) servers and Deep Discovery appliances. Deep Discovery Director (Internal Network Analytics Version) servers with untrusted or expired certificates can still deploy plans to Deep Discovery appliances, and appliances can still download the files required to execute the plans from those servers.

Importing a Certificate

Deep Discovery Director (Internal Network Analytics Version) uses a certificate to create secure connections to clients. Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.

> **WARNING!**
>
> - Verify that your web browser accepts the new certificate before importing it. Importing a certificate that is not accepted by your web browser will leave you unable to access the management console.
>
> - Importing a certificate restarts the service. Existing connections to repositories and Deep Discovery appliances will be interrupted, and clients will have to trust the new fingerprint to restore the connection.

Procedure

1. Go to **Administration** > **System Settings** > **Certificate**.

    The **Certificate** screen appears.

2. Click **Import and Replace Certificate**, select the certificate, and then click **Open**.

    The certificate is imported immediately.

Generating a Certificate Signing Request

You can generate a certificate signing request (CSR) in Deep Discovery Director (Internal Network Analytics Version) to apply for a new certificate from a certificate authority (CA).

> **Note**
>
> Deep Discovery Director (Internal Network Analytics Version) supports certificates in X.509 PEM format.

Procedure

1. Go to **Administration** > **System Settings** > **Certificate**.

2. Click **Generate Certificate Signing Request**.

3. Configure the certificate signing request settings.

Field	Description
Common Name (CN)	Type the domain name or server host name.
Subject alternative names	Type one or more domain names to associate with the generated certificate.
Organization (O)	Type your company name.
Organizational Unit (OU)	Type the name of your department within your company.
Country (C)	Type the two-letter code for the country where your company is located.
State/Region (ST)	Type the state or region whee your company is located.
City/Locality (L)	Type the city where your company is located.
Email address	Type your email address.
Key type and size	Select the certificate key type and size.

4.   Click **Generate and Download**.

   After the certificate signing request is generated, the system automatically download the CSR file.

Session Timeout

Select the time period after which users are logged out due to inactivity. The default value is **15 minutes**.

Operation Mode

Deep Discovery Director (Internal Network Analytics Version) can be switched to operate in **Standalone Network Analytics mode** to dedicate all of the systems' resources to perform advanced threat analysis.

Deep Discovery Director (Internal Network Analytics Version) cannot function by itself when operating in **Standalone Network Analytics mode**

and must register to another Deep Discovery Director (Internal Network Analytics Version) or **Deep Discovery Director (Consolidated Mode)** server.

When operating in **Standalone Network Analytics mode**, features and management console items are limited to those that are required to perform basic server functionality and advanced threat analysis.

The following table outlines the availability of management console items in Deep Discovery Director (Internal Network Analytics Version) and when operating in **Standalone Network Analytics mode**.

Screen		Deep Discovery Director (Internal Network Analytics Version)	Deep Discovery Director - Standalone Network Analytics mode
Dashboard		Yes	No
Detections		Yes	No
Threat Intelligence > **Product Intelligence**		Yes	No
Threat Intelligence > **Custom Intelligence**	**YARA Rules**	Yes	No
	STIX	Yes	No
	User-Defined Suspicious Objects	Yes	
	Exceptions	Yes	
Threat Intelligence > **Feed Management**		Yes	No
Threat Intelligence > **Sharing Settings**		Yes	No
Appliances		Yes	No
Alerts	**Triggered Alerts**	Yes	
	Built-in Rules	Yes	
	Custom Rules	Yes	No

Screen		Deep Discovery Director (Internal Network Analytics Version)	Deep Discovery Director - Standalone Network Analytics mode
Reports		Yes	No
Administration > Updates	Components	Yes	No
	Hotfixes / Patches	Yes	
	Firmware	Yes	
Administration > Integrated Products/Services	Deep Discovery Director	No	Yes
	Apex Central	Yes	
	Microsoft Active Directory	Yes	
	SAML Authentication	Yes	
	Syslog	Yes	No
Administration > Network Analytics	Server Information	Yes	No
	Data Sources	Yes	No
	Domain Exceptions	Yes	
	Priority Watch List	Yes	
	Registered Service	Yes	
	Trusted Internal Network	Yes	
Administration > System Settings	Network	Yes	
	Proxy	Yes	
	SMTP	Yes	

SCREEN		DEEP DISCOVERY DIRECTOR (INTERNAL NETWORK ANALYTICS VERSION)	DEEP DISCOVERY DIRECTOR - STANDALONE NETWORK ANALYTICS MODE
	SNMP	Yes	
	Bandwidth	Yes	
	Time	Yes	
	Certificate	Yes	
	Session Timeout	Yes	
	Operation Mode	Yes	No
Administration > **Account Management**		Yes	
Administration > **System Logs**		Yes	
Administration > **System Maintenance**		Yes	
Administration > **License**		Yes	

Switching the Operation Mode

Important

- All registered appliances must be unregistered before this action can be performed.

- The current configuration settings and detection logs will be cleared. Trend Micro recommends backing up settings and logs. The backup can be used to restore a Deep Discovery Director (Internal Network Analytics Version) server to the point before the operation mode switch.

  For details, see *Troubleshooting on page 10-1*.

- Switching the operation mode is irreversible.

Procedure

1. Go to **Administration** > **System Settings** > **Operation Mode**.

2. Click **Switch Operation Mode**.

    Deep Discovery Director (Internal Network Analytics Version) verifies if all requirements are met before displaying the **Switch Operation Mode** dialog.

3. Select whether to back up data to an SFTP server.

    - **Do not back up any data**: The server switches the operation mode and restarts immediately without backing up any data.

    - **Back up data to SFTP server**: The server backs up data to the specified SFTP server before switching the operation mode and then restarts. If you select this option, perform the following additional steps.

        a. Select which items to back up.

            - **Back up configuration settings**

            - **Back up detection logs**

        b. Type the server address.

        c. Type the port number.

        d. Type the SFTP server folder path to back up the data to.

            > **Note**
            >
            > Ensure that the specified folder is empty.

        e. Type the user name and password used for authentication.

        f. (Optional) Click **Test Connection**.

4. Click **Switch Operation Mode**.

Deep Discovery Director (Internal Network Analytics Version) starts backing up data before switching the operation mode, or switches the operation mode immediately, and then restarts.

Account Management

Deep Discovery Director (Internal Network Analytics Version) uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks.

Each account is assigned a specific role. A role defines the level of access to the management console.

Accounts

Use the **Accounts** screen, in **Administration** > **Account Management** > **Accounts**, to create and manage user accounts. Users can use these accounts, instead of the default administrator account, to access the management console.

Deep Discovery Director (Internal Network Analytics Version) supports the creation of user accounts by using the following methods:

- *Adding a Local User Account on page 9-53*
- *Adding an LDAP User Account or Group on page 9-54*

  > **Note**
  >
  > This method is only available if LDAP server settings have been configured.
  >
  > For details, see *LDAP on page 9-12*.

- *Adding a SAML Group on page 9-56*

> **Note**
>
> This method is only available if SAML Authentication settings have been configured.
>
> For details, see *SAML Authentication on page 9-15*

Adding a Local User Account

Procedure

1. Go to **Administration** > **Account Management** > **Accounts**, and then click **Add**.

   The **Add Account** screen appears.

2. Toggle the **Status** of this account.

3. Select **Local user** as the **Type** of this account.

4. Type a valid user name.

5. Type a valid password.

6. Type the password again to confirm it.

   > **Tip**
   >
   > Click the **Show password** icon to unmask the password and skip this step.

7. (Optional) Type a valid email address that can be used to receive alerts sent by Deep Discovery Director (Internal Network Analytics Version).

8. Select a **Role** for this account. The role determines the level of access this account has.

   For details, see *Roles on page 9-60*.

9. Select **Allow this account system access via web API** to allow users to use this account's credentials and permission key to access the system using the web API.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

   a. Select the number of days before the permission key expires.

   b. Select **Allow this account to log on to the management console** to allow this account's credentials to log on to the management console. Disabling this option causes the account to only be able to access the system via web API.

10. (Optional) Type a description for this account.

11. Click **Save**.

    If **Allow this account system access via web API** is selected, a dialog with the permission key is displayed.

> **Note**
>
> This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.

Adding an LDAP User Account or Group

If your company uses LDAP servers, such as Microsoft Active Directory, to manage user accounts and groups, you can enable those user accounts and groups access to Deep Discovery Director (Internal Network Analytics Version).

> **Note**
>
> - LDAP server settings have to be configured before an LDAP user account or group can be added.
>
>   For details, see *LDAP on page 9-12*.
>
> - Deep Discovery Director (Internal Network Analytics Version) syncs LDAP user accounts and groups every 24 hours. User accounts or groups that are removed from the LDAP server will be removed from Deep Discovery Director (Internal Network Analytics Version) after syncing with the LDAP server.
>
> - If an LDAP user is a member of one or more groups, the user's level of access in Deep Discovery Director (Internal Network Analytics Version) is determined by the highest level of access granted to the user's Deep Discovery Director (Internal Network Analytics Version) account or any group the user is a member of.

Procedure

1. Go to **Administration** > **Account Management** > **Accounts**, and then click **Add**.

    The **Add Account** screen appears.

2. Toggle the **Status** of this account.

3. Select **LDAP user or group** as the **Type** for this account.

4. Type a user or group name and click **Search** to search the LDAP server for matching user accounts or groups.

    Matching user accounts and groups are displayed in the results table.

> **Note**
>
> User accounts are not displayed in the results table if:
>
> - The user account's User Principal Name (UPN) is not specified on the LDAP server
>
> - The user account is disabled on the LDAP server

5. Select the LDAP user account or group to add.

> **Note**
>
> The LDAP email address of the user account or group will be used on Deep Discovery Director (Internal Network Analytics Version).

6. Select a **Role** for this account. The role determines the level of access this account has.

   For details, see *Roles on page 9-60*.

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

8. Click **Save**.

Adding a SAML Group

Procedure

1. Go to **Administration** > **Account Management** > **Accounts**, and then click **Add**.

   The **Add Account** screen appears.

2. Toggle the **Status** of this account.

3. Select **SAML group** as the **Type** of this account.

4. Type the **Claim value**.

> **Note**
>
> The claim value is the outgoing claim value in ADFS Claim Issuance Policy Rules or the group name in Okta.

5. Select a **Role** for this account. The role determines the level of access this account has.

   For details, see *Roles on page 9-60*.

6. (Optional) Type a description for this account.

7. Click **Save**.

Other Accounts Tasks

You can also perform the following tasks:

TABLE 9-3. Other Tasks

TASK	DESCRIPTION
Edit account	Click on a user name to open the **Edit Account** screen and do the following: • Toggle the account status • Change the password • Change the email address • Change the role • Enable/Disable web API access **Note** This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**. • Modify the description **Note** • The passwords and email addresses of Microsoft Active Directory accounts cannot be changed from the management console. • Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically. • Users who are currently logged on to the management console and whose roles are changed will be logged off automatically.

Task	Description
Delete account	Select one or more user accounts to delete and then click **Delete**.
	Note • There must be at least one local user account using the built-in administrator role. • You cannot delete the logged-on account. • Users who are currently logged on to the management console will be logged off automatically.
View web API access status	For accounts that have web API access activated, click the **Generate New Permission Key** icon to generate a new permission key. **Note** This feature or screen is not available when Deep Discovery Director (Internal Network Analytics Version) is operating in **Standalone Network Analytics mode**.
View account lock status	Deep Discovery Director (Internal Network Analytics Version) includes a security feature that locks an account in case the user typed an incorrect password three times in a row. This feature cannot be disabled. Accounts locked this way, even administrator accounts, unlock automatically after ten minutes. **Note** Microsoft Active Directory accounts are never locked.

Task	Description
Toggle account status	Click on the toggle in the **Status** column to enable or disable the user account.
	Note
	• At least one local user account using the built-in administrator role must be enabled.
	• Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.

Roles

Use the **Roles** screen, in **Administration** > **Account Management** > **Roles**, to create and manage user roles. Assign each user a role that will restrict their activities to all but those necessary for the completion of their duties.

Deep Discovery Director (Internal Network Analytics Version) comes with a set of built-in user roles that you cannot delete:

Role	Description
Administrator	Built-in Administrator role with full access to all management console features
Investigator	Built-in Investigator role with read-only access to all management console features, but download access to investigation package and pcap data
Operator	Built-in Operator role with read-only access to all management console features

Deep Discovery Director (Internal Network Analytics Version) also supports custom user roles. Create new roles to limit access to the management console, and to restrict users from seeing and managing specific appliances.

Adding a Role

Procedure

1. Go to **Administration** > **Account Management** > **Roles**, and then click **Add**.

   The **Add Role** screen appears.

2. Type a role name.

3. Select a **Permission** for this role.

4. Select the appliances this role can see and manage.

5. Select the domains from which email message detections should be displayed.

   > **Note**
   >
   > To specify domains, you have to add them first. For details, see *Managing Domains on page 9-61*.

6. Select an account, or type to search and press ENTER, and then click **Add** to add the selected account to this role.

   > **Note**
   >
   > Added accounts will be removed from all other roles.

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

8. Click **Save**.

Managing Domains

In addition to finely controlling which appliances a role can see and manage, the integration with Deep Discovery Email Inspector calls for control over which email messages a role can see. To address this requirement, Deep Discovery Director (Internal Network Analytics Version) provides users with the control to separate email messages by using domains.

Procedure

1. Go to **Administration** > **Account Management** > **Roles**.

   The **Roles** screen appears.

2. Do one of the following:

   - Click **Add** to open the **Add Role** screen.

   - Click on a role name to open the **Edit Role** screen.

3. In the **Domain access** section, click on **Domain management**.

   The **Domain Management** dialog appears.

4. Type a domain in the left text box and click **Add** to add the domain to the list.

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

5. Select one or more domains from the list and click **Delete** to delete the selected domains.

6. (Optional) To search for a domain, type a keyword in the right search text box, and then press ENTER or click the magnifying glass icon.

7. Click **Close**.

Other Roles Tasks

You can also perform the following tasks:

TABLE 9-4. Other Tasks

Task	Description
Edit role	Click on a role name to open the **Edit Role** screen and do the following: • Modify the role name • Change the permission • Modify the appliances this role can see and manage • Add accounts to this role • Modify the description **Note** • You cannot modify the role name, permission, appliance access rights, and description of built-in roles. • Users who are currently logged on to the management console and whose appliance access rights are modified will be logged off automatically. • Users who are currently logged on to the management console and whose roles are changed will be logged off automatically.
Delete role	Select one or more user roles to delete and then click **Delete**. **Note** • You cannot delete built-in roles. • You cannot delete roles that are in use by at least one account.

System Logs

Use the **System Logs** screen, under **Administration** > **System Logs**, to view, query and export system logs.

Deep Discovery Director (Internal Network Analytics Version) maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.

Deep Discovery Director (Internal Network Analytics Version) stores system logs in the appliance hard drive.

Query system logs to gather information from the database. The queried system logs can be exported in CSV format for offline viewing.

For details, see *Querying System Logs on page 9-65*.

The following table lists all system-log-related information:

TABLE 9-5. System Log Information

COLUMN	DESCRIPTION
Logged	Event date and time
Event ID	Event identifier
	Each specific action has its own event ID. Examples:
	• 20001
	Description: User logged on
	• 20002
	Description: User logged off
Type	One of the following types displays:
	• Account Logon/Logoff
	• Apex Central Integration
	• External Web Service
	• Message Operation
	• System
	• Update

Column	Description
Level	One of the following levels displays: • `Informational` • `Warning` • `Error`
Result	One of the following results displays: • `Successful` • `Unsuccessful`
Source	Activity by source Information about the following sources may display: • user name Example: `johnadmin` • system Example: `SYSTEM`
IP Address	Event IP address
Description	Event details

Querying System Logs

The task of finding a specific system log entry can be difficult when there may be hundreds or thousands to go through. Use the filters and search box to lower the number of entries shown.

Procedure

1. Go to **Administration** > **System Logs**.

    The **System Logs** screen appears.

2. Click the **Filters** button.

    Filter drop-down lists and a search box appear.

3. Perform any of the following actions.

    - Select a log type.

    - Select a log level.

    - Select a log result.

    - Select a period or specify a custom period using the calendar and clock.

    - Type a event ID, source, or description keyword in the search box and press ENTER to only display system logs whose event ID, source, or description contain the keyword.

    The screen is updated immediately.

4. (Optional) Click **Export** to export the currently filtered system logs.

    The **Export** dialog displays.

5. Confirm the system log filters and select a delimiter to use.

6. Click **OK** to export and download the currently filtered system logs to a CSV file with the chosen delimiter.

> **Note**
>
> The exported system logs are ordered by **Log ID**, a consecutive number that coincides with the **Logged** date and time.

System Maintenance

The **System Maintenance** screen, in **Administration** > **System Maintenance**, includes the following tabs.

System Status

The **System Status** screen displays the utilization of key hardware components.

Storage

Use the **Storage** screen, in **Administration** > **System Maintenance** > **Storage**, to configure how long Deep Discovery Director (Internal Network Analytics Version) saves database entries, system logs, and detection logs, and to configure disk usage.

Under **Database Storage**, configure the following:

- **Delete database entries older than *X* days**: Type the number of days to save database entries. Entries older than the specified value are automatically deleted.

  > **Tip**
  >
  > A **database entry** in this context refers to a Deep Discovery Director (Internal Network Analytics Version) plan.

- **Delete system logs older than *X* days**: Type the number of days to save system logs. Logs older than the specified value are automatically deleted.

- **Delete detection logs older than *X* days**: Type the number of days to save detection logs. Logs older than the specified value are automatically deleted.

  > **Tip**
  >
  > - **Detection logs** in this context refers to Deep Discovery Inspector related detection details.

- **Delete generated reports older than *x* days**: Type the number of days to save generated reports. Reports older than the specified value are automatically deleted.

- **Delete Network Analytics data older than *x* days**: Type the number of days to save Network Analytics data. Data older than the specified value is automatically deleted.

> **Note**
>
> In addition to the settings above, Deep Discovery Director (Internal Network Analytics Version) automatically purges system logs until there is 200 MB free database disk space. This threshold cannot be modified.

The **Disk Usage** section displays information about the usage and total size of partitions. Any available space can be added to the any of the partitions. New disks can be added to further increase partition size.

> **Important**
>
> Disks only can be added to virtual appliances.

Configuring Disk Space

Add extra available disk space to Deep Discovery Director (Internal Network Analytics Version) partitions to increase the number of logs or repository files that can be stored.

Procedure

1. Go to **Administration** > **System Maintenance** > **Storage**, and click **Configure space**.

   The **Disk Space Configuration** dialog appears.

2. (Optional) To add more disks to Deep Discovery Director (Internal Network Analytics Version), do the following:

   a. Click **Add disks**.

      The disk selection dialog displays.

   b. Select at least one disk to add to the Deep Discovery Director (Internal Network Analytics Version) disk space configuration.

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

c. Click **Add**.

> **WARNING!**
>
> Disks cannot be removed after they are added.

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

3. To add available space to a partition, do one of the following:

- Select **Add all available space to this partition**
- Type values into the **Add** fields.

> **Note**
>
> - The **Available space** and **Total** values are automatically updated.
>
> - It is not required to distribute all available space among the partitions.

4. Click **Apply**.

Available space is added to the partitions as specified.

Back Up

Use the **Back Up** screen, in **Administration** > **System Maintenance** > **Back Up**, to export a backup file of most of the configuration settings and the database, and to configure automatic backups of those.

The following table shows the screens and elements with backed up configuration settings.

TABLE 9-6. Backed Up Configuration Settings

SCREEN		ELEMENT
Threat Intelligence > **Product Intelligence**	**Synchronized Suspicious Objects**	Objects
	C&C Callback Addresses	Objects
Threat Intelligence > **Custom Intelligence**	**YARA Rules**	YARA rules
	STIX	STIX
	User-Defined Suspicious Objects	Objects
	Exceptions	Objects
Threat Intelligence > **Feed Management**		All settings
Threat Intelligence > **Sharing Settings**	**TAXII 1.x**	All settings
	TAXII 2.0/2.1	All settings
	OpenDXL	All settings
	Web Service	All settings
	Auxiliary Products/Services	All settings
Appliances > **Directory**		Appliance tree with group structure
		Registered appliances and appliance details
Appliances > **Plans**		All plans
Alerts	**Triggered Alerts**	All triggered alert records
	Built-in Rules	All rule settings
	Custom Rules	All rule settings
Reports	**Schedules**	All schedules
	Customization	All settings

Screen		Element
Administration > **Integrated Products/Services**	**LDAP**	LDAP server settings
	Syslog	All syslog server profiles
Administration > **Network Analytics**	**Connected Sources**	All settings
Administration > **System Settings**	**Proxy**	Proxy settings
	Bandwidth	Bandwidth usage throttling settings
	Time	Time settings
	Certificate	Certificate
	Session Timeout	Session timeout value
Administration > **Account Management**	**Accounts**	All user accounts
	Roles	All roles
Administration > **System Logs**		All system logs
Administration > **System Maintenance**	**Storage**	Storage values
	Back Up	Automatic backup settings
Administration > **License**		Activation Codes
Help		API key

Exporting a Configuration Settings and Database Backup

Deep Discovery Director (Internal Network Analytics Version) can export a backup file of most configuration settings and the database. Use the backup file to restore Deep Discovery Director (Internal Network Analytics Version) to a previous point in time. Use the backup file on another server, when the active server is unresponsive and cannot be restored, to restore operation and minimize downtime.

Procedure

1. Go to **Administration** > **System Maintenance** > **Back Up**.

    The **Back Up** screen appears.

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

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

3. Download and save the backup file.

Configuring Automatic Backups

Deep Discovery Director (Internal Network Analytics Version) can be configured to create and upload automatic backups of its configuration settings and database to a SFTP server of your choice. Deep Discovery Director (Internal Network Analytics Version) creates up to five backup files, after which the oldest one is deleted in order to keep the number of backup files at five.

Procedure

1. Go to **Administration** > **System Maintenance** > **Back Up**.

    The **Back Up** screen appears.

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

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

4. Type the port number. The default port number is 22.

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

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

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

8. Click **Save**.

Restore

Use the **Restore** screen, in **Administration** > **System Maintenance** > **Restore**, to restore configuration settings and database from a backup file. If the active Deep Discovery Director (Internal Network Analytics Version) server is unresponsive or cannot be restored, a configuration settings and database backup can also be used on another server to restore operation and minimize downtime.

Restoring a Configuration Settings and Database Backup

A configuration settings and database backup can be used to restore Deep Discovery Director (Internal Network Analytics Version) to a previous point in time.

If the active Deep Discovery Director (Internal Network Analytics Version) is unresponsive or cannot be restored, a configuration settings and database backup can also be used on another server to restore operation and minimize downtime.

For details, see *Replacing the Active Server with Another Server on page 9-74*.

Procedure

1. Go to **Administration** > **System Maintenance** > **Restore**.

    The **Restore** screen appears.

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

3. Click **Upload**.

    The backup file is uploaded, and Deep Discovery Director (Internal Network Analytics Version) displays information about the backup file.

4. Click **Restore**.

    Deep Discovery Director (Internal Network Analytics Version) displays a confirmation message.

5. Click **OK**.

Deep Discovery Director (Internal Network Analytics Version) restores configuration settings and database from the backup file, and then restarts the server.

6. (Optional) Restore the repository by re-uploading all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

> **Important**
>
> Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.

7. (Optional) Configure the network addresses.

   The server is now ready to resume operation.

Replacing the Active Server with Another Server

If the Deep Discovery Director (Internal Network Analytics Version) server is unresponsive or cannot be restored, it can be replaced by another server.

Host machine hardware, host machine software, and Deep Discovery Director (Internal Network Analytics Version) version and build of the replacement server must be the same as the active server.

Procedure

1. Back up the configuration settings and database of the active server.

   a. On the management console of the active server, go to **Administration** > **System Maintenance** > **Back Up**.

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

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

    c. Download and save the backup file.

2. Install Deep Discovery Director (Internal Network Analytics Version) on the replacement server.

3. Configure temporary network addresses for the replacement server.

> **Important**
>
> Verify that the temporary network addresses are different from the network addresses of the active server to avoid IP addressing conflicts.

4. Log on to the management console of the replacement server.

5. Restore the configuration settings and database on the replacement server.

    a. On the management console of the replacement server, go to **Administration** > **System Maintenance** > **Restore**.

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

    c. Click **Upload**.

    The backup file is uploaded, and Deep Discovery Director (Internal Network Analytics Version) displays information about the backup file.

    d. Click **Restore**.

    Deep Discovery Director (Internal Network Analytics Version) displays a confirmation message.

    e. Click **OK**.

    Deep Discovery Director (Internal Network Analytics Version) restores configuration settings and database from the backup file, and then restarts the server.

6. Restore the repository by re-uploading all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

> **!** **Important**
>
> Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.

7. Power off the active server.

    a. On the management console of the active server, go to **Administration** > **System Maintenance** > **Power Off / Restart**.

    b. Click **Power Off**.

    The active server stops all services and gracefully shuts down.

    > **⚠** **WARNING!**
    >
    > The replacement server will be configured to use the network addresses of the active server. Leaving the active server powered on will cause IP addressing conflicts.

8. Configure the replacement server to use the network addresses of the active server.

    The replacement server is now ready to resume operation as the new active server.

Power Off / Restart

Use the **Power Off / Restart** screen, in **Administration** > **System Maintenance** > **Power Off / Restart**, to power off or restart the server.

- **Power Off**: All active tasks are stopped, and then the server gracefully shuts down.

- **Restart**: All active tasks are stopped, and then the server is restarted.

Integrated products may queue data while the server is unavailable.

License

The **License** screen includes the following information and options.

TABLE 9-7. License Details

FIELD	DETAILS
Status	Displays either **Activated**, **Not Activated**, or **Expired**. **Important** - Deep Discovery Director (Internal Network Analytics Version) does not allow the creation of new plans when the license status is **Not Activated** or **Expired**. Existing plans will deploy and execute as usual. - Deep Discovery Director (Internal Network Analytics Version) does not allow component updates or the installation of firmware upgrades when the license status is **Not Activated** or **Expired**. Click **View details** to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated on the screen, click **Refresh**. **Note** If proxy settings are enabled, Deep Discovery Director (Internal Network Analytics Version) connects to the license update server using the proxy server.
Type	**Full**: Provides access to all product features **Trial**: Provides access to all product features
Expiration date	View the expiration date of the license. Renew the license before it expires. Click **View renewal instructions** to view instructions from the Trend Micro website.

Field	Details
Activation Code	View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code. The **License** screen reappears displaying the updated expiration date.

Chapter 10

Troubleshooting

Learn about common troubleshooting options available in Deep Discovery Director (Internal Network Analytics Version).

Troubleshooting

To open the **Troubleshooting** screens, go to `https://<appliance IP address>/troubleshooting`.

Logs

Deep Discovery Director (Internal Network Analytics Version) generates and stores debug logs for various internal services. Export the debug logs for offline viewing and troubleshooting.

1. (Optional) Modify the levels at which the various services should generate debug logs in and click **Apply**.

2. Click **Export Debug Log Files** to display the **Export Debug Log Files** dialog.

3. Select the debug log files to export and then click **Export**.

   The system begins gathering the log files and creating an archive file for download.

(Optional) Click **Restore Defaults** to restore all settings to their default values.

Delete Crash Dumps

Deep Discovery Director (Internal Network Analytics Version) generates and stores dump files when processes crash.

Click **Delete** to manually delete process crash dump files to free up disk space.

Switch Mode Restore

The configuration settings and detection logs of Deep Discovery Director - Internal Network Analytics version can be restored to the point before the operation mode was switched to Standalone Network Analytics mode.

The configuration settings and detection logs of Deep Discovery Director - Internal Network Analytics version can be restored to the point before the operation mode was switched to Standalone Network Analytics mode.

(Optional) Click **Test Connection** to test the connection to the SFTP server.

Threat Intelligence

Modify threat intelligence sharing settings such as time before the integration process times out, the batch size for processing (Check Point only), and whether to remove query strings from URLs (Palo Alto only), and then click **Save**.

Bandwidth and Data Sources

View the **GUID** and **Bandwidth** of connected data sources.

Chapter 11

Technical support

Learn about the following topics:

Troubleshooting resources

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

Using the support portal

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

Procedure

1. Go to https://success.trendmicro.com.

2. Select from the available products or click the appropriate button to search for solutions.

3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Contact Support** and select the type of support needed.

   > **Tip**
   >
   > To submit a support case online, visit the following URL:
   >
   > https://success.trendmicro.com/en-US/contactus/

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

Threat encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated
	225 E. John Carpenter Freeway, Suite 1500
	Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900
	Toll-free: (888) 762-8736
Website	• https://www.trendmicro.com
	• https://success.trendmicro.com/en-US/contactus/

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html
- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding up the support call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information

- Computer brand, model, and any additional connected hardware or devices

- Amount of memory and free hard disk space

- Operating system and service pack version

- Version of the installed agent

- Serial number or Activation Code

- Detailed description of install environment

- Exact text of any error message received

Sending suspicious content to Trend Micro

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

Email Reputation Services

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

https://servicecentral.trendmicro.com/en-us/ers/

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

https://success.trendmicro.com/en-US/solution/KA-0001177

File Reputation Services

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

https://success.trendmicro.com/en-US/solution/KA-0002449

Record the case number for tracking purposes.

Web Reputation Services

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

https://global.sitesafety.trendmicro.com/

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

Other resources

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

Download center

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

https://www.trendmicro.com/download/

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

Appendices

Appendices
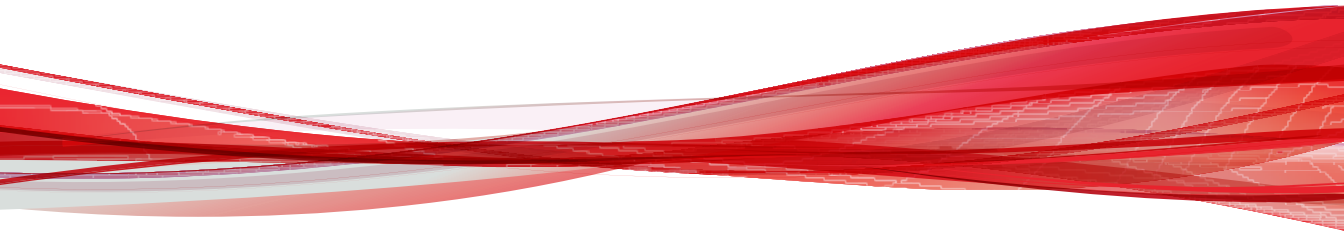
Appendix A

Service Addresses and Ports

This appendix discusses service addresses and ports used by Deep Discovery Director (Internal Network Analytics Version). Configure your proxy and firewall settings to allow Deep Discovery Director (Internal Network Analytics Version) to connect to the services to ensure optimal operation.

Service Addresses and Ports

Deep Discovery Director (Internal Network Analytics Version) accesses several Trend Micro services to obtain information about emerging threats and to manage your existing Trend Micro products. The following table describes each service and provides the required address and port information accessible to the product version in your region.

Note

All services connect using HTTPS with TLS 1.2 or above. If your environment has man-in-the-middle devices, verify that the devices support TLS 1.2 or above.

TABLE A-1. Service Addresses and Ports

SERVICE	DESCRIPTION	ADDRESS AND PORT	NOTES
ActiveUpdate Server	Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.	`ddd55-p.activeupdate.trendmicro.com/activeupdate:443`	Related to product version
Customer Licensing Portal	Manages your customer information, subscriptions, and product or service license.	`licenseupdate.trendmicro.com:443`	

SERVICE	DESCRIPTION	ADDRESS AND PORT	NOTES

Deep Discovery Director - Network Analytics as a Service	A hosted service that provides advanced threat analysis on historical network data based network detections, and other related events as they occur over time.	`api.nacloud.trendmicro.com:443`
		
		`api.eu.nacloud.trendmicro.com:443`
		
		`api.jp.nacloud.trendmicro.com:443`
		
		`api.sg.nacloud.trendmicro.com:443`
		
		`api.us.nacloud.trendmicro.com:443`
			Related to product region

Documentation Server	Hosts all Trend Micro product documentation. If Deep Discovery Director (Internal Network Analytics Version) is unable to connect to the server, a local copy of the product documentation will be displayed instead.	`docs.trendmicro.com:80`
		
		`docs.trendmicro.com:443`	

Email Encryption	Encrypts and decrypts email messages with registered domains using Identity-based Encryption (IBE) for secure private information delivery.	`root.ibe-ta.com:80`
		
		`public.ibe-ta.com:80`
		
		`ppconfig.ibe-ta.com:80`	

Proxy Connection Test	Deep Discovery Director (Internal Network Analytics Version) establishes a connection to this remote file to verify the validity of proxy settings.	`http://www.msftncsi.com/ncsi.txt`	

Service	Description	Address and Port	Notes
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.	`ddd55.threatconnect.tre ndmicro.com:443`	Related to product version

Trend Vision One	Extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With Trend Vision One, you can respond more effectively to threats, minimizing the severity and scope of a breach.	`*.xdr.trendmicro.com:44 3`
		
		`*.xdr.trendmicro.co.jp: 443`
			Related to product version and region

Ports Used by Deep Discovery Director (Internal Network Analytics Version)

The following section shows the ports that are used with Deep Discovery Director (Internal Network Analytics Version) and why they are used.

TABLE A-2. Ports used by Deep Discovery Director (Internal Network Analytics Version)

PORT	PROTOCOL	FUNCTION	PURPOSE
22	TCP	Listening and outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to: • Connect to the preconfiguration console • Download Virtual Analyzer images from an SFTP server • Back up configuration settings and data to an SFTP server
25	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to send alert notifications through SMTP.
53	TCP/UDP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port for DNS resolution.
80	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) connects to other computers and integrated Trend Micro products and hosted services through this port. In particular,Deep Discovery Director (Internal Network Analytics Version) uses this port to: • Connect to the Customer Licensing Portal • Connect to a proxy server
123	UDP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to connect to the NTP server to synchronize time.

Port	Protocol	Function	Purpose
139	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to download Virtual Analyzer images from a network folder.
161	UDP	Listening	Deep Discovery Director (Internal Network Analytics Version) uses this port for SNMP agent listening and protocol translation.
162	UDP	Listening and Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port: • For SNMP agent listening and protocol translation • To send SNMP trap notifications

Port	Protocol	Function	Purpose
443	TCP	Listening and outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to: • Access the management console with a computer through HTTPS • Listen to TAXII 1.x and 2.0/2.1 client requests • Listen to integrating product or service requests for threat intelligence data • Listen to auxiliary product or service requests for threat intelligence data • Communicate with auxiliary products or services for threat intelligence sharing • Communicate with Deep Discovery appliances • Communicate with Deep Discovery Director - Network Analytics as a Service • Communicate with the ActiveUpdate server • Communicate with Trend Micro Apex Central • Communicate with Trend Vision One
445	TCP/UDP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to download Virtual Analyzer images from a network folder.
601	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to send logs to a syslog server.

Port	Protocol	Function	Purpose
636	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to retrieve user information from LDAP servers.
4459	TCP	Listening	Deep Discovery Director (Internal Network Analytics Version) uses this port to access the End-User Quarantine console with a computer over HTTPS.
6514	TCP	Listening and Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to send logs to a syslog server over TCP with SSL encryption.
8080	TCP	Listening	Deep Discovery Director (Internal Network Analytics Version) uses this port to share threat intelligence with other products.
8883	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to distribute threat intelligence data to OpenDXL clients, services, and brokers.
18183	TCP	Outbound	Deep Discovery Director (Internal Network Analytics Version) uses this port to distribute threat intelligence data to Check Point Open Platform for Security.

Appendix B

Settings Replicated by Deep Discovery Director

This appendix lists the configuration settings replicated by Deep Discovery Director (Internal Network Analytics Version) for each Deep Discovery appliance and version.

Deep Discovery Analyzer 6.8 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

Table B-1. Deep Discovery Analyzer 6.8 Replicated Configuration Settings

Screen		Element
Dashboard		Widgets settings only
Virtual Analyzer	**Submissions**	Filter settings
	Suspicious Objects > **User-defined Suspicious Objects**	**User-defined Suspicious Objects**
	Exceptions	**Exceptions** list
Virtual Analyzer > **Sandbox Management**	**File Passwords**	Passwords list
	Submission Settings	File type filter settings
	Smart Feedback	**Smart Feedback** settings
	Sandbox for macOS	**Sandbox for macOS** setting
	YARA Rules	All YARA rules
Alerts / Reports > **Alerts**	**Rules**	All alert notification rule settings
Alerts / Reports > **Reports**	**Schedules**	All report schedules
	Customization	Report customization settings
Administration > **Updates** > **Component Update Settings**		Component update settings
Administration > **Integrated Products/Services**	**Smart Protection**	**Smart Protection** settings
	ICAP	ICAP settings
	Microsoft Active Directory	Microsoft Active Directory settings
	Log Settings	Log settings

SCREEN		ELEMENT
Administration > **System Settings**	**Network**	TLS setting
	Proxy	Proxy settings
	SMTP	SMTP settings
	Time	Time settings
	SNMP	SNMP settings
	Password Policy	Password policy setting
	Session Timeout	Session timeout values
Administration > **Accounts / Contacts**	**Accounts**	All user accounts
	Contacts	All contacts
Administration > **System Maintenance** > **Back Up**		Automatic backup settings

Deep Discovery Analyzer 6.9 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-2. Deep Discovery Analyzer 6.9 Replicated Configuration Settings

SCREEN		ELEMENT
Dashboard		Widgets settings only
Virtual Analyzer	**Submissions**	Filter settings
	Suspicious Objects > **User-defined Suspicious Objects**	**User-defined Suspicious Objects**
	Exceptions	**Exceptions** list
Virtual Analyzer > **Sandbox Management**	**File Passwords**	Passwords list
	Submission Settings	File type filter settings

Screen		Element
	Smart Feedback	**Smart Feedback** settings
	Sandbox for macOS	**Sandbox for macOS** setting
	YARA Rules	All YARA rules
Alerts / Reports > **Alerts**	**Rules**	All alert notification rule settings
Alerts / Reports > **Reports**	**Schedules**	All report schedules
	Customization	Report customization settings
Administration > **Updates** > **Component Update Settings**		Component update settings
Administration > **Integrated Products/Services**	**Smart Protection**	**Smart Protection** settings
	ICAP	ICAP settings
	Microsoft Active Directory	Microsoft Active Directory settings
	Log Settings	Log settings
Administration > **System Settings**	**Network**	TLS setting
	Proxy	Proxy settings
	SMTP	SMTP settings
	Time	Time settings
	SNMP	SNMP settings
	Password Policy	Password policy setting
	Session Timeout	Session timeout values
Administration > **Accounts / Contacts**	**Accounts**	All user accounts
	SAML	All SAML groups
	Contacts	All contacts
Administration > **System Maintenance** > **Back Up**		Automatic backup settings

Deep Discovery Analyzer 7.0 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-3. Deep Discovery Analyzer 7.0 Replicated Configuration Settings

SCREEN		ELEMENT
Dashboard		Widgets settings only
Virtual Analyzer	**Submissions**	Filter settings
	Suspicious Objects > **User-defined Suspicious Objects**	**User-defined Suspicious Objects**
	Exceptions	**Exceptions** list
Virtual Analyzer > **Sandbox Management**	**File Passwords**	Passwords list
	Submission Settings	File type filter settings
	Scan Settings	All settings
	Interactive Mode	All settings
	Smart Feedback	**Smart Feedback** settings
	Sandbox for macOS	**Sandbox for macOS** setting
	YARA Rules	All YARA rules
Alerts / Reports > **Alerts**	**Rules**	All alert notification rule settings
Alerts / Reports > **Reports**	**Schedules**	All report schedules
	Customization	Report customization settings
Administration > **Updates** > **Component Update Settings**		Component update settings
Administration > **Integrated Products/Services**	**Smart Protection**	**Smart Protection** settings
	ICAP	ICAP settings

Screen		Element
	Microsoft Active Directory	Microsoft Active Directory settings
	Log Settings	Log settings
Administration > **System Settings**	**Network**	TLS setting
	Proxy	Proxy settings
	SMTP	SMTP settings
	Time	Time settings
	SNMP	SNMP settings
	Password Policy	Password policy setting
	Session Timeout	Session timeout values
Administration > **Accounts / Contacts**	**Accounts**	All user accounts
	SAML	All SAML groups
	Contacts	All contacts
Administration > **System Maintenance** > **Back Up**		Automatic backup settings

Deep Discovery Inspector 5.6 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-4. Deep Discovery Inspector 5.6 Replicated Configuration Settings

Screen		Element
Detections	**Affected Hosts**	Only **Saved Searches**
	Affected Hosts - Host Details	
	All Detections	

Screen		Element
Reports	**Schedules**	All settings
	Customization	
Administration > **Updates** > **Component Updates**	**Scheduled**	All settings
	Source	All settings
Administration > **Notifications**	**Notification Settings** > **Threat Detections**	All settings
	Notification Settings > **High Risk Hosts Detections**	
	Notification Settings > **Suspicious Hosts Detections**	
	Notification Settings > **High Network Traffic**	
	Notification Settings > **Unanalyzed Sample Detections**	
	Notification Settings > **Virtual Analyzer Detections**	
	Notification Settings > **Deny List**	
	Notification Settings > **Retro Scan Detections**	
	Delivery Options > **Email Settings**	
Administration > **Monitoring / Scanning**	**Hosts / Ports**	All settings
	Threat Detections	
	Web Reputation	
	Application Filters	

Screen		Element
	Deny List / Allow List	
	Detection Rules	
	Exceptions	
	Packet Capture	
Administration > **Virtual Analyzer**	**Setup**	Only the internal Virtual Analyzer proxy settings and the sandbox for macOS setting.
	File Submissions	All settings
	Internal Virtual Analyzer > **Sandbox Management** > **Passwords**	
Administration > **Network Groups and Assets**	**Network Groups**	All settings
	Registered Domains	
	Registered Services	
Administration > **Integrated Products/Services**	**Threat Intelligence Sharing**	All settings
	Microsoft Active Directory	
	Syslog	
Administration > **System Settings**	**Network**	Only **Secure Protocol** setting
	Proxy	All settings
	SNMP	
	Time	
	Session Timeout	
Administration > **Accounts**		All settings

Screen	Element
Administration > **System Maintenance** > **Storage Maintenance**	Only **File Size Settings**

Deep Discovery Inspector 5.7 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-5. Deep Discovery Inspector 5.7 Replicated Configuration Settings

Screen		Element
Detections	**Affected Hosts**	Only **Saved Searches**
	Affected Hosts - Host Details	
	All Detections	
Reports	**Schedules**	All settings
	Customization	
Administration > **Updates** > **Component Updates**	**Scheduled**	All settings
	Source	All settings
Administration > **Notifications**	**Notification Settings** > **Threat Detections**	All settings
	Notification Settings > **High Risk Hosts Detections**	
	Notification Settings > **Suspicious Hosts Detections**	
	Notification Settings > **High Network Traffic**	
	Notification Settings > **Unanalyzed Sample Detections**	

Screen		Element
	Notification Settings > **Virtual Analyzer Detections**	
	Notification Settings > **Deny List**	
	Notification Settings > **Retro Scan Detections**	
	Delivery Options > **Email Settings**	
Administration > **Monitoring / Scanning**	**Hosts / Ports**	All settings
	Threat Detections	
	Web Reputation	
	Application Filters	
	Deny List / Allow List	
	Detection Rules	
	Detection Exceptions	
	Packet Capture	
Administration > **Virtual Analyzer**	**Setup**	Only the internal Virtual Analyzer proxy settings and the sandbox for macOS setting.
	File Submissions	All settings
	Internal Virtual Analyzer > **Sandbox Management** > **Passwords**	
Administration > **Network Groups and Assets**	**Network Groups**	All settings
	Registered Domains	
	Registered Services	

SCREEN		ELEMENT
Administration > **Integrated Products/Services**	**Threat Intelligence Sharing**	All settings
	Microsoft Active Directory	
	Syslog	
Administration > **System Settings**	**Network**	Only **Secure Protocol** setting
	Proxy	All settings
	SMTP	
	SNMP	
	Time	
	Session Timeout	
Administration > **Accounts**		All settings
Administration > **System Maintenance** > **Storage Maintenance**		Only **File Size Settings**

Deep Discovery Inspector 5.8 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-6. Deep Discovery Inspector 5.8 Replicated Configuration Settings

SCREEN		ELEMENT
Detections	**Affected Hosts**	Only **Saved Searches**
	Affected Hosts - Host Details	
	All Detections	
Reports	**Schedules**	All settings
	Customization	

SCREEN		ELEMENT
Administration > **Updates** > **Component Updates**	**Scheduled**	All settings
	Source	All settings
Administration > **Notifications**	**Notification Settings** > **Threat Detections**	All settings
	Notification Settings > **High Risk Hosts Detections**	
	Notification Settings > **Suspicious Hosts Detections**	
	Notification Settings > **High Network Traffic**	
	Notification Settings > **Unanalyzed Sample Detections**	
	Notification Settings > **Virtual Analyzer Detections**	
	Notification Settings > **Deny List**	
	Notification Settings > **Retro Scan Detections**	
	Delivery Options > **Email Settings**	
Administration > **Monitoring / Scanning**	**Hosts / Ports**	All settings
	Threat Detections	
	Web Reputation	
	Application Filters	
	Deny List / Allow List	
	Detection Rules	

Screen		Element
	Detection Exceptions	
	Packet Capture	
Administration > **Virtual Analyzer**	**Setup**	Only the internal Virtual Analyzer proxy settings and the sandbox for macOS setting.
	File Submissions	All settings
	Internal Virtual Analyzer > **Sandbox Management** > **Passwords**	
Administration > **Network Groups and Assets**	**Network Groups**	All settings
	Registered Domains	
	Registered Services	
Administration > **Integrated Products/Services**	**Threat Intelligence Sharing**	All settings
	Microsoft Active Directory	
	Syslog	
Administration > **System Settings**	**Network**	Only **Secure Protocol** setting
	Proxy	All settings
	SMTP	
	SNMP	
	Time	
	Session Timeout	
Administration > **Accounts**		All settings
Administration > **System Maintenance** > **Storage Maintenance**		Only **File Size Settings**

Deep Discovery Web Inspector 2.5 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-7. Deep Discovery Web Inspector 2.5 Replicated Configuration Settings

SCREEN		ELEMENT
Dashboard		All settings
Policy	**Policy**	All policy rules and policy global settings
	Decryption Rules	All HTTPS decryption rules (formerly known as HTTPS Inspection rules)
	Digital Certificates	All certificates in the trusted, untrusted, and invalid certificate stores and certificate exceptions
	HTTPS Tunnels	All domain tunnels
	Intelligent Decryption	All custom patterns and exceptions
Policy > **User Defined Settings**	**Network Objects**	All network objects
	Domain Objects	All domain objects
	Approved/Blocked Lists	Approved list and blocked list
	Notifications	All notification settings
Alerts / Reports	**Alerts** > **Rules**	All alert rules
	Reports > **Schedules**	All report schedules
Administration	**Component Updates** > **Schedules**	All schedule settings

Screen		Element
	System Settings > **X-Header Handling**	All settings
Administration > **Active Directory Services**	**Active Directory**	All settings
	Authentication Policy	All settings
	Global Authentication Settings	All settings **Note** The Kerberos keytable information is not backed up.

Deep Discovery Web Inspector 2.6 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-8. Deep Discovery Web Inspector 2.6 Replicated Configuration Settings

Screen		Element
Dashboard		All settings
Policy	**Policy**	All policy rules and policy global settings
	Decryption Rules	All HTTPS decryption rules (formerly known as HTTPS Inspection rules)
	Digital Certificates	All certificates in the trusted, untrusted, and invalid certificate stores and certificate exceptions
	HTTPS Tunnels	All domain tunnels

Screen		Element
	Intelligent Decryption	All custom patterns and exceptions
Policy > **User Defined Settings**	**Network Objects**	All network objects
	Domain Objects	All domain objects
	Approved/Blocked Lists	Approved list and blocked list
	Notifications	All notification settings
Alerts / Reports	**Alerts** > **Rules**	All alert rules
	Reports > **Schedules**	All report schedules
Administration	**Component Updates** > **Schedules**	All schedule settings
	System Settings > **X-Header Handling**	All settings
Administration > **Active Directory Services**	**Active Directory**	All settings
	Authentication Policy	All settings
	Global Authentication Settings	All settings **Note** The Kerberos keytable information is not backed up.

Deep Discovery Director (Standalone Network Analytics Mode) 5.2 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-9. Deep Discovery Director (Standalone Network Analytics Mode) 5.2 Replicated Configuration Settings

SCREEN		ELEMENT
Administration > **Integrated Products/Services** > **Microsoft Active Directory**		All settings
Administration > **System Settings**	**Proxy**	All settings
	SMTP	All settings
	SNMP	All settings
	Time	All settings except manually set date and time
	Session Timeout	All settings
Administration > **Account Management**		All settings

Deep Discovery Director (Standalone Network Analytics Mode) 5.3 Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

TABLE B-10. Deep Discovery Director (Standalone Network Analytics Mode) 5.3 Replicated Configuration Settings

SCREEN		ELEMENT
Administration > **Integrated Products/Services** > **Microsoft Active Directory**		All settings
Administration > **System Settings**	**Proxy**	All settings
	SMTP	All settings
	SNMP	All settings
	Time	All settings except manually set date and time

Screen		Element
	Session Timeout	All settings
Administration > **Account Management**		All settings

Index

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: APEM59981/250312