TREND MICRO™

Trend Micro™ Threat Intelligence Manager 1

Administrator's Guide

Security Management

Document Part No. ZREM14780/110112

Release Date: June 2011

The user documentation of Trend Micro™ Threat Intelligence Manager is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the Online Help file and the online Knowledge Base at Trend Micro's Web site.

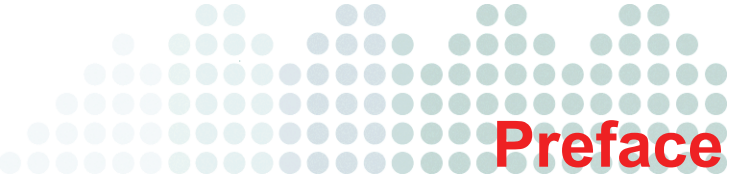
Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Chapter 3: Investigation

Chapter 4: Alerts and Reports



Preface

Welcome to the *Trend Micro™ Threat Intelligence Manager Administrator's Guide*. This guide contains information about product settings and service levels.

This preface discusses the following topics:

- *Trend Micro™ Threat Intelligence Manager Documentation*
- *Audience*
- *Document Conventions*
- *Terminology*

Trend Micro™ Threat Intelligence Manager Documentation

The Threat Intelligence Manager documentation includes the following:

TABLE 1-1. Threat Intelligence Manager Documentation

DOCUMENTATION	DESCRIPTION
Trend Micro™ Threat Intelligence Manager Administrator's Guide	A PDF document that discusses getting started information and helps you plan for deployment and configure all product settings.
Online Help	Helps you configure all features through the user interface. You can access the Online Help by opening the Web console and then clicking the informational Help icon.
Trend Micro™ Threat Intelligence Manager Installation and Deployment Guide	A PDF document that discusses requirements and procedures for installing Trend Micro Threat Intelligence Manager, planning for deployment and configuring product settings.
Readme File	Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history. The readme is available at: http://www.trendmicro.com/download
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

Audience

This document is intended to be used by new users of Threat Intelligence Manager, including system administrators, operators, sensitive content contributors, information security staff, executives, and other users with other specific roles.

The audience should have a thorough understanding of the Threat Intelligence Manager system, including general operations and critical concepts.

Document Conventions

To help you locate and interpret information easily, the Threat Intelligence Manager documentation uses the following conventions.

TABLE 1-2. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Tools > Client Tools	A “bread crumb” found at the start of procedures that helps users navigate to the relevant Web console screen. Multiple bread crumbs means that there are several ways to get to the same screen.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, `C:\Program Files\<file_name>` can be `C:\Program Files\sample.jpg`.
Note: text	Provides configuration notes or recommendations

TABLE 1-2. Document Conventions (Continued)

CONVENTION	DESCRIPTION
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! *text*	Provides warnings about activities that may harm computers on your network

Terminology

The following table provides the official terminology used throughout the Threat Intelligence Manager documentation:

TABLE 1-3. Threat Intelligence Manager Terminology

TERMINOLOGY	DESCRIPTION
Administrator	The person managing the Threat Intelligence Manager server.
Alert	Item of interest generated from a qualifying event or group of events.
Client	The Threat Intelligence Manager client program.
Client computer or endpoint	The computer where the Threat Intelligence Manager client is installed.
Client installation folder	The folder on the computer that contains the Threat Intelligence Manager client files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: `C:\Program Files\Trend Micro\Threat Intelligence Manager Client`

TABLE 1-3. Threat Intelligence Manager Terminology (Continued)

TERMINOLOGY	DESCRIPTION
Client user (or user)	The person managing the Threat Intelligence Manager client on the client computer.
Components	Responsible for collecting, managing, displaying, and investigating event that occur between Trend Micro and third-party products.
Console	The user interface for configuring and managing the Threat Intelligence Manager server and client settings. The console for the Threat Intelligence Manager server program is called the “Web console,” while the console for the client program is called the “client console.”
Dashboard	UI screen in which Widgets are displayed.
Generated Report	Displays the results of a TMQL query in a given visualization, e.g. pie chart, table, line graph, and so on, in the form of a widget displayed on the Console UI or printable form.
Hibernate	Open source facility that provides relational database table to object mapping. It is the tool used by report management system to interact with the report database.
Investigation Baskets	Collection of report baskets that are available to the user from the Console UI.
Notification	The item sent out to inform a registered user that an event has occurred.
POJO	Acronym for Plain Old Java Objects which is one form of database interface provided by Hibernate.
RBAC	Role-based access control
Report Basket	Collection of reports maintained in the Investigation Baskets UI object.

TABLE 1-3. Threat Intelligence Manager Terminology (Continued)

TERMINOLOGY	DESCRIPTION
Report Template	Object that contains the TMQL query and visualization information necessary to generate a report.
Scheduled Report	Generated report that is run at regular time intervals.
Security risk	The collective term for virus/malware, spyware/grayware, and Web threats
Server	The Threat Intelligence Manager server program
Server computer	The computer
Server installation folder	The folder on the computer that contains the Threat Intelligence Manager server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: `C:\Program Files\Trend Micro\Threat Intelligence Manager`
Threat Intelligence Manager service	Threat Intelligence Manager is a collection of Windows services that provide the ability to analyze security events generated by other security products.
TIM	Threat Intelligence Manager
TMQL	Trend Micro Query Language. Provides a unified query interface to Threat Intelligence Manager SOLR and DB data stores.
VP	Visibility Platform
Widget	Visual renderings of the report templates. Widgets are contained in the Dashboard.
Workbench	UI screens in which Threat Intelligence Manager logs and event data are queried and analyzed.

Chapter 1

Introduction

This chapter introduces the Trend Micro™ Threat Intelligence Manager.

The topic includes the following:

Overview

The Trend Micro™ Threat Intelligence Manager is designed to be the next generation in Trend Micro's security visibility and central management products. The mission of the first Threat Intelligence Manager is to:

- collect, aggregate, manage, and analyze Trend Micro product event logs into a centralized storage space on a server
- provide advanced visualization and investigation tools that can enable you to monitor, explore, and diagnose security events within your own environment

Threat Intelligence Manager provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. The flexibility of the Threat Intelligence Manager server enables third-party applications, as well as future Trend Micro products, to seamlessly and easily integrate into Threat Intelligence Manager.

The Threat Intelligence Manager documentation is written for IT administrators and security analysts. The documentation assumes that the readers have an in-depth knowledge of Trend Micro security products from where the security events are generated. The document does not assume the reader has any knowledge of threat intelligence with event correlation.

Service Ports

List of open service ports for external access that are configurable during installation:

- Management Console Port (HTTPS) – TCP Port 443
- Web Services Port (HTTP) - TCP Port 8080
- Log Receiver – Plaintext Listening Port - TCP Port 7173
- Log Receiver – SSL Listening Port – TCP Port 7174
- Syslog Receiver (TCP/UDP) – Port 8514

Manually Configurable (By Support Only)

- Trend Micro Threat Intelligence Manager agent communication port – TCP Port 5118, 5120
- Trend Micro Web Service to Deep Security Manager or Intrusion Detection Firewall – TCP Port 4119
- Microsoft SQL Express – TCP Port 1433

System Requirements

The installation of Threat Intelligence Manager must be supported by a 64-bit Windows Server 2008 R2 or later (Standard, Enterprise, Datacenter or Web editions). The number of products and events per second requiring support from Threat Intelligence Manager determine the hardware requirements.

Ensure the installation of Threat Intelligence Manager installer has been copied over to the host machine. You will need to access the binary code and download it locally or through a shared directory on the FTP host site.

The Threat Intelligence Manager server can be installed on computers running the platforms shown in the paragraphs that follow:

Hardware Requirements

- CPU: Core 2 Duo 2.66GHz CPU system or above
- Memory: Minimum 4GB of RAM (Recommended: 16GB or above)
- Hard Disk: At least 250GB of available disk space for storage
- Network Protocol: TCP/IP, UDP for heartbeat, HTTP, HTTPS, TCP over VPN, or TCP port 43 for WhoIs utility.
- Others: .NET Framework 3.5 SP1 or above
- Display: VGA (1280 x 1024/256 color) or higher

Operating System Requirements

Microsoft® Windows Server® 2008 R2 with Service Pack 1

- * Windows Server 2008 R2 with Service Pack 1 (Standard, Enterprise, Datacenter and Web Editions), 64-bit versions

---

Note: * Threat Intelligence Manager cannot be installed on a Windows Server 2008 Server Core environment.

Database Requirements

- Microsoft® SQL Server® 2008 R2 Express
- Microsoft® SQL Server® 2008 SP1
- Microsoft® SQL Server® 2008 R2 SP1

Web Console Requirements

- Mozilla® Firefox® 3.5, 3.6 and 4.0
- Adobe® Flash® version 10 or above
- Microsoft® Silverlight™ 4.0 or above
- Microsoft® Internet Explorer version 8 or above

Virtualization

Threat Intelligence Manager supports server installations on guest Windows 2008 R2 with Service Pack 1 operating systems hosted on the following virtualization applications:

- VMware® ESX /ESXi™ Server 4 or above (Server Edition)
- VMware Server 1.0.3 or above (Server Edition)
- VMware Workstation and Workstation ACE Edition 7.0

The server can also be installed on guest Windows 2000, 2003 (32-bit), 2008 (32-bit) operating systems hosted on:

- Microsoft Virtual Server 2005 R2 with Service Pack 1
- Windows Server 2008 (64-bit) with Hyper-V™
- Windows Server 2008 R2 (64-bit) with Hyper-V

Agent System Requirements

Prior to installation, the agent requires the following:

Supported Trend Micro products - Agent, installed on 32/64 bit Windows

- OfficeScan Client/Server Edition (OSCE) 10.0 SP1 Patch 3 and hot fix 2881.
- OSCE 10.5 and hot fix 1286.
- OSCE 10.5 patch 1 and hot fix 1848.2.

Supported Trend Micro Products - Agentless

- Threat Discovery Appliance (TDA) 2.5, 2.55, 2.6
- Deep Security Manager (DSM) 7.0
- Intrusion Defense Firewall (IDF) 1.2

Getting Started

After a successful installation and agent deployment, the Treat Intelligence Manger is ready for personalization. While getting started, you will need to step through the Getting Started Wizard to help set the required configurations.

The Getting Started Wizard will initiate automatically after you log in to Threat Intelligence Manger for the first time. After you have successfully configured your product, you can deactivate the wizard to prevent it from appearing every time you log in.

The Wizard directs you through four, required and important elements that enable the features of the Threat Intelligence Manager: Log Collection, GeoIP Tagging, Asset Tagging, and Deploying the Logs. You can configure each of the four elements in any order you desire, or complete them all in the order as listed.

To enable important features in Threat Intelligence Manager:

1. Open the Getting Started Wizard (if it does not automatically appear - click **Resources > Getting Started**.)

The Getting Started Wizard appears.

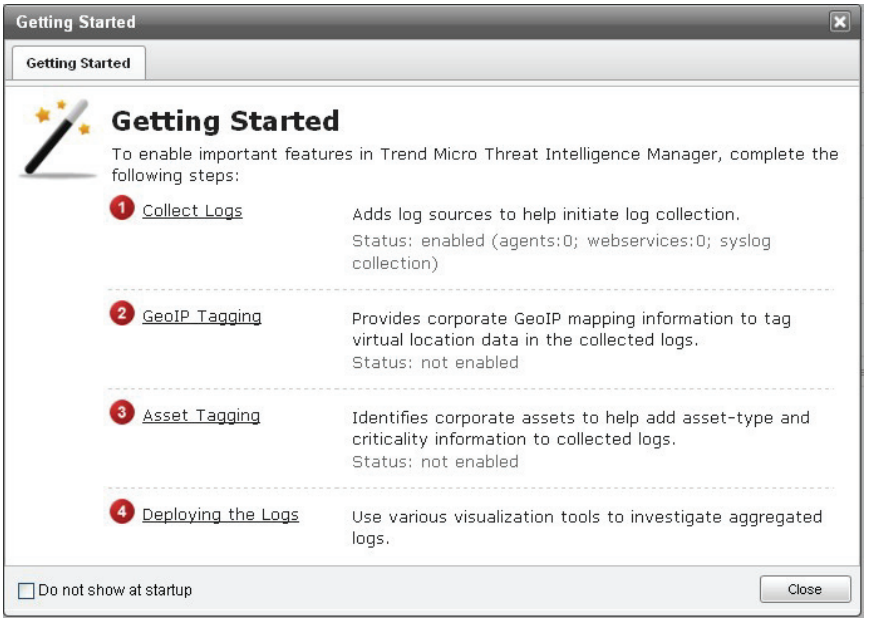


FIGURE 1-1 Getting Started Wizard

2. Click **Collect Logs** to help initiate log collection by adding log collection sources.

   The Wizard opens the Log Sources workbench located in **Administration > Log Sources**.
3. Add Agent-based, Syslog, and Webservice log sources as described in Log Sources on page 5-2.
4. After your Log Collection sources have been defined, you can define your tagging options. You need not define both, but you can configure your logs with Corporate Geo tagging or Asset tagging.
5. To define your logs with Corporate Geo Tagging information, click **GeoIP Tagging** in the wizard. The wizard opens the GeoIP Tagging page located in **Administration > Log Tagging > GeoIP Tagging**.
6. Define the GeoIP Tagging as described in GeoIP Tagging on page 5-19.

7. If you would like to define your logs with Asset tags while in the wizard, click **Asset Tagging**. The wizard opens the Asset Tagging page located in **Administration > Log Tagging > Asset Tagging**.
8. Define your asset tags as described in Asset Tagging on page 5-25.
9. Finally, complete the setup by deploying the logs you have configured. From the Getting Started Wizard, click **Deploying the Logs** to use the various visualization tools available (Charts, GeoMaps, LinkGraphs, and so on) to investigate your aggregated logs. You can learn more about deploying logs in Log View on page 3-15.

Resources/Status Bar

The status bar at the bottom of Threat Intelligence Manager allows you quick access to your pending alerts, available resources, and when a page's content exceeds the available screen space, you can use scroll up to view hidden information.

Status Bar

The following figure is a representation of the Status Bar.

FIGURE 1-2 Status Bar

Use your mouse to click any of the Status Bar buttons to access the associated features.

Alerts

The Status Bar button for Alerts (#) feature indicates how many alerts have occurred since your last visit. After clicking the **Alerts Status** button, you will jump to the **Alerts/Reports > Triggered Alerts** page where you can view additional details (including their severity) about the alerts that have been triggered, forward an alert to another party, mark the alert as resolved - if it's been investigated, and open the alert in the Workbench to continue with additional investigation.

Resources

The resources button will reveal quick access to external locations where you can research additional information about Threat Intelligence Manager, as shown in the following figure.

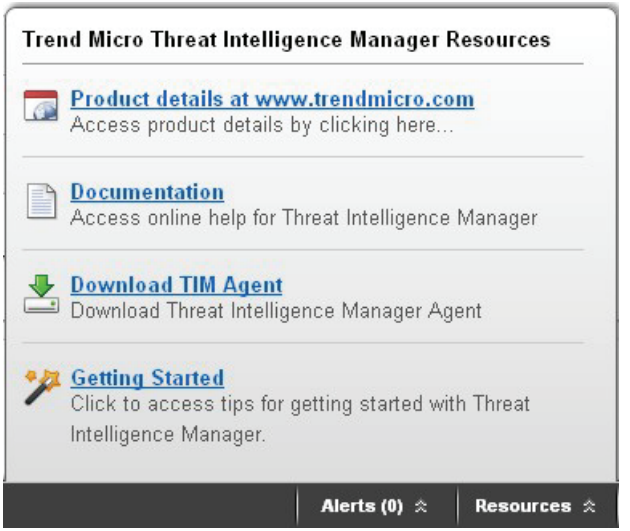


FIGURE 1-3 Additional Threat Intelligence Manager External Resources

Product Details at www.trendmicro.com - Clicking will send you to the Threat Intelligence Manager product page at `www.trendmicro.com`, where you can access additional product information.

Documentation - Clicking this option will open the Threat Intelligence Manager's Online Help. You can also access the Online Help on any page by clicking the blue Help icon (the question mark) in the top right corner of Threat Intelligence Manager.

Download Agent - Clicking this option will popup a dialog box where you can begin downloading the Threat Intelligence Manager agent as shown in the following figure. You can also download the agent from the login page without actually logging in.

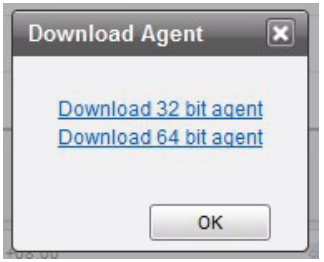


FIGURE 1-4 Downloading the Agent

Getting Started - The Getting Started Wizard initiates automatically when you first log in to Threat Intelligence Manger. You can deactivate this feature by clicking the box in the lower left corner of the Wizard. Click the Getting Started button in Resources to reinitiate the Getting Started feature.

Deactivating/Activating the Getting Started Wizard

To deactivate the Getting Started Wizard:

1. From the Getting Started Wizard window, check the box "**Do not show at startup**" in the lower left corner of the wizard.
2. Click **Close**.

To return to the wizard:

1. Click **Resources > Getting Started**. The Getting Started Wizard appears. Deselect the check box "**Do not show at startup**" in the lower left corner of the wizard to make the Wizard reappear each time you start up the Threat Intelligence Manger.

Chapter 2

Dashboard

The Trend Micro™ Threat Intelligence Manager Dashboard is discussed in this chapter. The Dashboard is the place where you can monitor the overall security posture of your company's assets. You can track threats through a series of widgets that contain visual charts and graphs. You will associate them with the logs accumulated from your agent servers. These can be tracked through the Threat Intelligence Manager's predefined widgets, a Threat Intelligence Map, the Smart Protection Network, or by creating a series of customized widgets to fit your particular needs.

The topics include the following:

Content Source of the Dashboard

The default widgets display:

- Detections
- Settings

General Features

Interaction with the "Investigation" page.

1. Click the graph points, chart, or table rows on the widgets and use them as keywords to initialize new searches in your investigation.
2. Smart Protection Network widgets do not contain links to help you reinvestigate.

Tab Settings

In addition to the default tabs, you can create other tabs to help you with tracking threats. A tab is a page on the dashboard that can hold up to 20 widgets. The Dashboard can host a maximum of 30 tabs. There is no limit to the number of tabs that a user can delete, but you cannot delete all tabs from the dashboard (one must remain).

There are several layout options from which you can select to display your widgets. You can access these options by selecting either the **New Tab** icon or the **Tab Settings** button on the page. The configuration of the New Tab and Tab Settings pop-up is very similar except that the New Tab option loads the default settings, and the Tab Settings option loads the current tab settings (such as the tab name and layout options defined when creating the tab).

To create a new tab:

1. Click the "+" to create a **New Tab** on the Dashboard.

The New Tab design template appears.

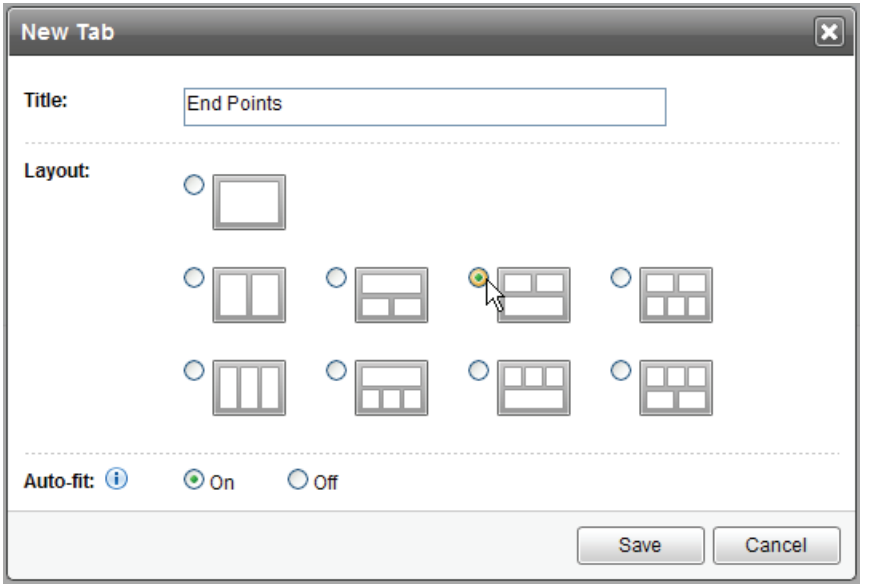


FIGURE 2-1 New Tab Design Template

2. Enter a title for the tab.
3. Select a layout design from the predesigned options that appear.
4. Click **Save** to create the new tab. The tab layout can be changed at any time. The next section details the steps for adding widgets to your new tab.

Adding New Widgets

Widgets can be added or removed from the dashboard tabs. Each widget includes a description of its purpose. There are two categories of widgets from which you can choose to add into the dashboard. These widget categories are described in detail throughout the sections that follow.

- Predefined widgets
- Widgets generated in the process of saving report templates on the Investigation page

You can also change the configuration of the widget. Widget configuration includes the widget name, annotation, chart type (table, pie, bar, and line), as well as the chart configuration.

To add a predefined widget:

1. Click **Add Widgets** in the upper right corner of the Dashboard.

   The "Add Widgets" selection page appears.

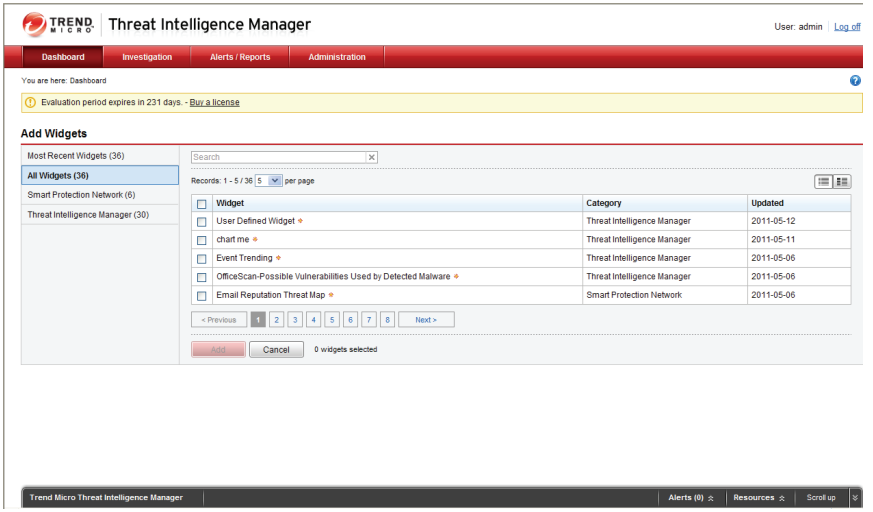


FIGURE 2-2 Adding Predefined Widgets

2. Select from the list of predefined widget designs that appear. You can select multiple widgets at one time.
3. Click **Add**.

The widgets you selected will appear on the New Tab you created. The widgets you added can be deleted or drag-and-dropped to various locations within the widget container, and their configuration can still be modified.

Predefined Widgets

There are two predefined widgets that you can use to get started, the "Event Trending Widget" and the "OfficeScan-Possible Vulnerabilities Used by Detected Malware widget," The Event Trending Widget can display the event trending numbers in a Line Chart for users to monitor.

The OfficeScan-Possible Vulnerabilities Used by Detected Malware widget displays the number of Common Vulnerabilities and Exposures (CVE), Malware, Detections, and Host Detections.

Threat Intelligence Manager includes five default Dashboard tabs that include:

- Event Trending Widget
- OfficeScan Widgets
- Threat Discovery Appliance Widgets
- Deep Security Manager Widgets
- Threat Intelligence Map Widget

In addition to the predefined widgets, you can also add Custom widgets that can be generated from the Report Template. See Customized Widgets on page 2-16.

Note: Threat Intelligence Manager uses Widget Framework 2.0.

Operations on the Widget

Provides an entry where you can enter an Investigation from the widget. For predefined widgets, refer to the descriptions that follow.

Event Trending Widget

This is a representation of the Event Trending widget.

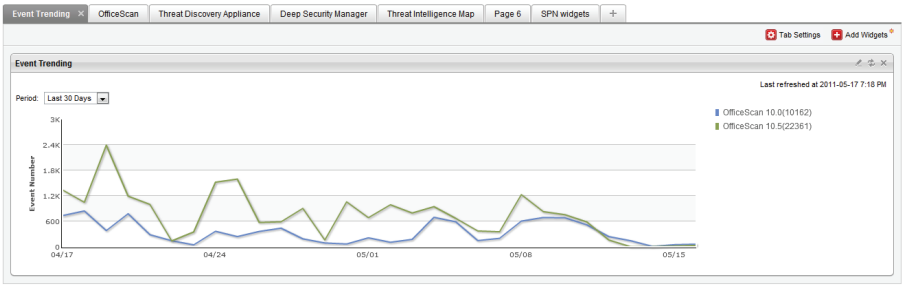


FIGURE 2-3 Display of the Predefined Event Trending Widget

The predefined widget for Event Trending can be displayed for the last 4 hours, every 24 hours, every 7 days, every 30 days, every 90 days. You can edit the widget settings by clicking the pencil icon in the widget title bar. The Event Trending widget settings page appears as shown in the following figure.

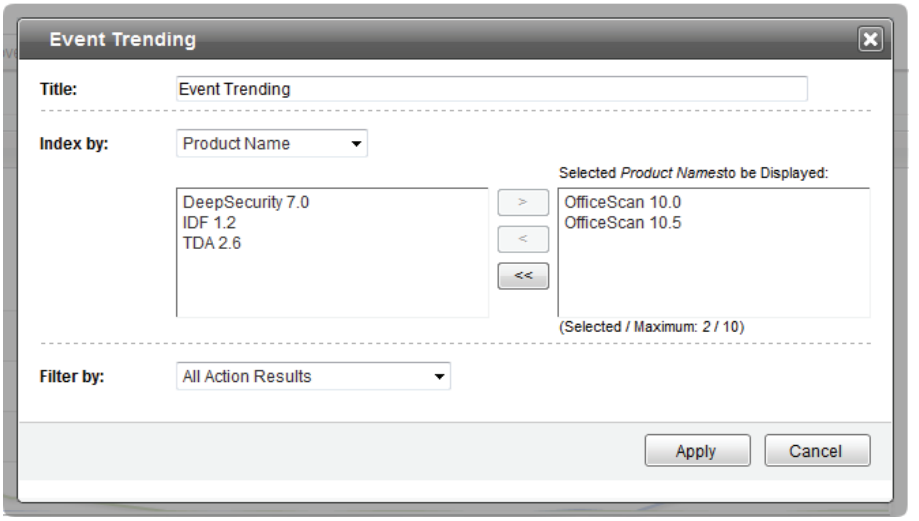


FIGURE 2-4 Event Trending Widget Settings

Index by:

The Event Trending widget settings page can be configured to be indexed by Product Name, Entity, Asset Tags, or Geographic Location. Use the drop-down list to select the indexing method to suit your requirements.

- **Product Name** - Choose from the available product names (up to 10) and use the arrow buttons to move selected product(s) to the appropriate column.
- **Entity** - Depending on the scanning products your system supports, the selected entities are associated with the IP addresses or host names in your network that have logs available for indexing. Keep all the entities in the right column, or filter out unnecessary IPs by moving them from the right column to the left.
- **Asset Tagging** - Select up to 10 assets that have been tagged with Asset Tagging, and move required assets to the right column for indexing purposes.
- **Geographic Location** - Filter up to 10 events through geographic location by selecting either the country or the city filter, then adding the affected location(s) to the right column for indexing.

Filter:

- **All Action Results** -
- **Both First and Final Actions Failed** -
- **Detected Bots** -

OfficeScan Widgets

Note: If your Threat Intelligence Manager server does not manage an OfficeScan server (or you have not yet added an OfficeScan server in the Log Sources settings), no data will be displayed on these widgets.

The predefined OfficeScan Widgets include:

- OfficeScan-Possible Vulnerabilities Used by Detected Malware

  The predefined widget for Possible Vulnerabilities Used by Detected Malware can be displayed for the last 4 hours, every 24 hours, every 7 days, every 30 days, every 90 days. You can edit the widget configuration by clicking the pencil icon in the

widget title bar. The OfficeScan-Possible Vulnerabilities Used by Detected Malware Widget settings page appears as shown in the following figure.

Index by:

The OfficeScan-Possible Vulnerabilities Used by Detected Malware Widget settings page can be configured to be indexed by Product Name, Entity, Asset Tags, or Geographic Location. Use the drop-down list to select the indexing method to suit your requirements.

- **Product Name** - Choose from the available product names (up to 10) and use the arrow buttons to move selected products to the appropriate column.
- **Entity** - Depending on the scanning products your system supports, the selected entities are associated with the IP and host name addresses in your network that have logs available for indexing. Keep all the entities in the right column, or filter out unnecessary IPs by moving them from the right column to the left.
- **Asset Tagging** - Select up to 10 assets that have been tagged with Asset Tagging, and move required assets into the right column for indexing purposes.
- **Geographic Location** - Filter up to 10 events through geographic location by selecting either the country or the city filter, then adding the affected location(s) to the right column for indexing.

Default Widgets

- Possible Vulnerabilities used by Detected Malware
- OfficeScan-Top 10 Hosts of Detected Malware
- OfficeScan-Action Results on Detected Malware: Further Action Required
- OfficeScan-Action Results on Detected Malware: Viewing All
- OfficeScan-Top 10 Web Security Events

Additional Widgets

- OfficeScan-Action Results on Detected Malware: Cleaned
- OfficeScan-Top 5 Device Control Policy Violations
- OfficeScan-Top 10 Device Control Violations
- OfficeScan-Top 5 Behavior Monitoring Policy Violations
- OfficeScan-Top 10 Network Threatened Hosts
- OfficeScan-Top 5 Threatened Ports

Threat Discovery Appliance Widgets

Note: If your Threat Intelligence Manager server does not manage any Threat Discovery Appliance (TDA) servers (or you have not yet added a TDA server in the Log Sources settings), no data will be displayed on these widgets.

The predefined Threat Discovery Appliance Widgets include:

- TDA-Attempted Exploitation Event Trends
- TDA-Top 10 Host Exploitation Attempts
- TDA-Event Trending for Brute Force Logins
- TDA-Top 10 Attempted Logins by Brute Force Attacks
- TDA-Malware Detection Event Trending
- TDA-Top 10 Hosts with Malware Detected

Note: See TDA Rules in the Online Help for additional information regarding the rules of TDA.

Deep Security Manager Widgets

Note: If your Threat Intelligence Manager server does not manage any Deep Security Manager (DSM) servers (or you have not yet added a DSM server in the Log Sources settings), no data will be displayed on these widgets.

The predefined Deep Security Manager widgets include:

- DSM-Total Event Distribution
- DSM-DPI Rules with most Violations
- DSM-Detected DPI Rule Violations Trending
- DSM-Top 20 Destination Port Numbers for DPI
- DSM-Prevented DPI Rule Violation Trending
- DSM-Detected Firewall Policy Violation Event Trending
- DSM-Top 20 Firewall Rules with Policy Violations
- DSM-Prevented Firewall Policy Violation Events

Threat Intelligence Map Widget

The Threat Intelligence Map powered by Smart Protection Network widget represents the geographic distribution of the Smart Protection Network's (SPN) top 20 malware events that have occurred on the Threat Intelligence Manager server.

- **24 hours tab**: Local (in the Threat Intelligence Manager server) top 20 malware detections from the past 24 hours
- **7 days tab**: Local (in the Threat Intelligence Manager server) top 20 malware detections from the past 7 days

When you click the name of the detected malware, its distribution will be displayed on the map, line chart, and pie chart.

Malware distribution is displayed on a:

- **Map**: Represents the geographic distribution of malware detection
- **Line chart**: Represents the trending of the malware detection counts over a determined period of time
- **Pie chart**: Represents the malware distribution of each regional slice

- **Global SPN**: Select to filter the distribution data based on the global smart protection network
- **Local SPN**: Select to filter the distribution data based on the local smart protection network.

  Select both options to view ALL detected malware threats.

Note: Enable the "Trend Micro Smart Feedback" setting on your OfficeScan server if you would like to see results after selecting the "Local SPN Data" option.

Smart Protection Network Widgets

The Smart Protection Network (SPN) widgets displays a series of threat statistics through the use of six SPN widgets. They have to be added manually through the "Add Widgets" page as they are not displayed by default.

The predefined Smart Protection Network widgets include:

- Smart Protection Network Threat Statistics

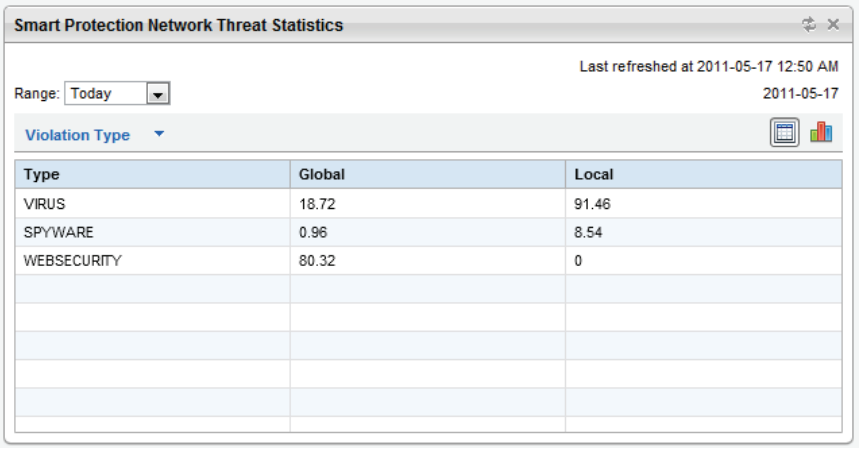


FIGURE 2-5 Smart Protection Network Threat Statistics page

Displays the number of threat detection events discovered globally and locally on the network. This widget displays its data by:

- Product Category
- Violation Type
- The data can be displayed with a Table or a Bar Chart as shown in the following figure.

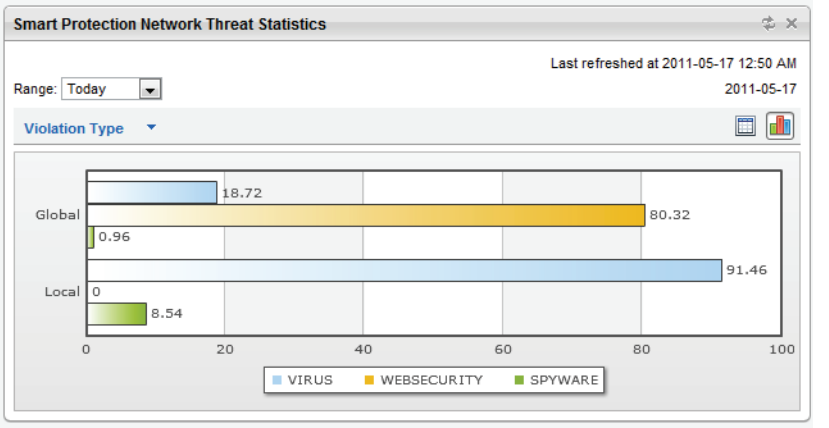
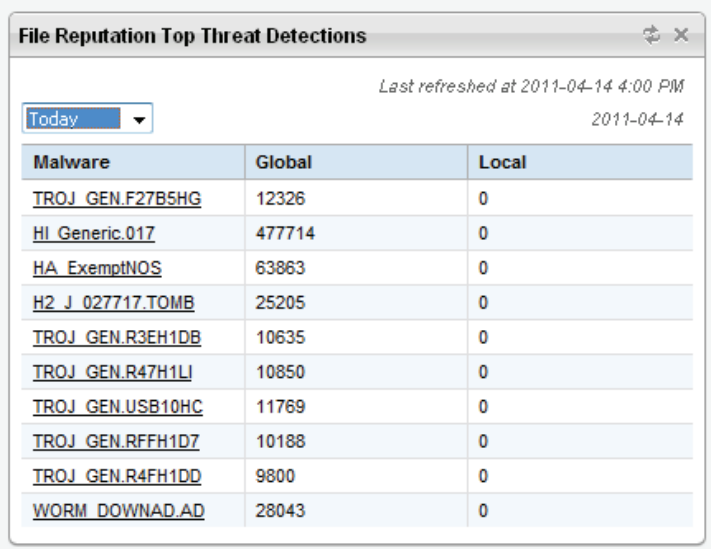


FIGURE 2-6 Smart Protection Network Threat Statistics Bar Chart

- File Reputation Top Threat Detections

- Displays the top 10 threat detections (Figure 2-7) made by File Reputation. The data represents a comparison between global and local threat detections.



File Reputation Top Threat Detections

Last refreshed at 2011-04-14 4:00 PM

Today

2011-04-14

Malware	Global	Local
TROJ_GEN.F27B5HG	12326	0
HI_Generic.017	477714	0
HA_ExemptNOS	63863	0
H2_J_027717.TOMB	25205	0
TROJ_GEN.R3EH1DB	10635	0
TROJ_GEN.R47H1LI	10850	0
TROJ_GEN.USB10HC	11769	0
TROJ_GEN.RFFH1D7	10188	0
TROJ_GEN.R4FH1DD	9800	0
WORM_DOWNAD.AD	28043	0

FIGURE 2-7 File Reputation Top 10 Detected Threats

- File Reputation Threat Map

- Displays the total number of security threats detected by File Reputation. The information is displayed on a world map (Figure 2-8) based on geographic locations of the threat events.

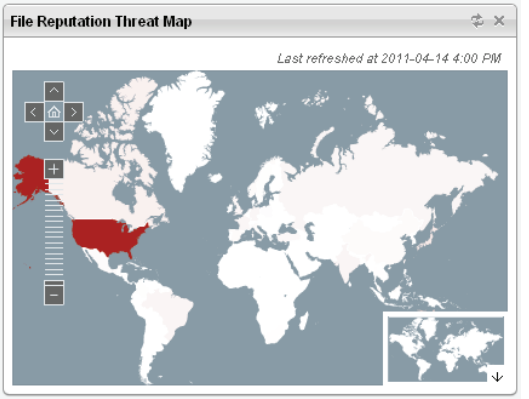


FIGURE 2-8 Mapped Security Threats Detected by File Reputation

- Email Reputation Threat Map
  - Displays the total number of spam events detected by Email Reputation. The information is displayed on a world map (Figure 2-9) based on geographic locations of the threat events.

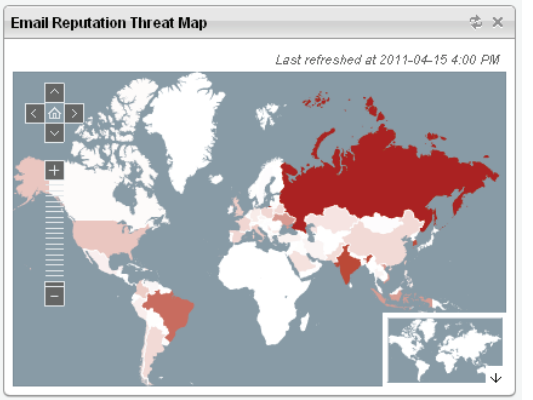


FIGURE 2-9 Mapped Security Threats Detected by Email Reputation

- Web Reputation Top Threatened Users
  - Displays the top number of users affected by malicious URLs detected by Web Reputation. The information is displayed on a world map (Figure 2-10) based on geographic locations of the threat events.

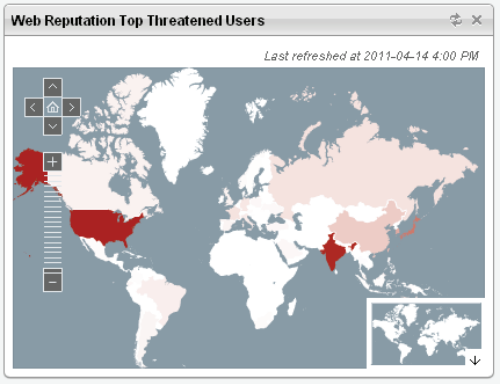


FIGURE 2-10 Threatened Users Detected by Web Reputation

- Web Reputation Top Threat Sources
  - Displays the total number of security threats detected by Web Reputation. The information is displayed on a world map (Figure 2-11) based on geographic locations of the threat events.

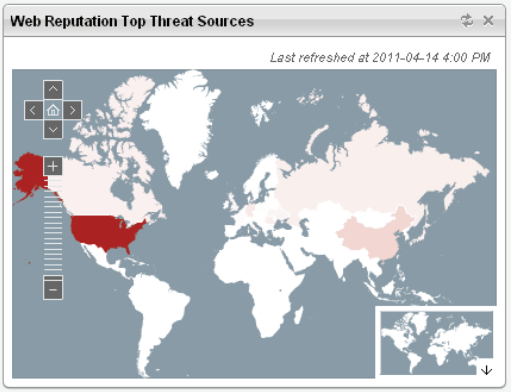


FIGURE 2-11 Top-Threatened Sources Detected by Web Reputation

Customized Widgets

The Threat Intelligence Managers allows you to create widgets based on search results from the Investigation page. On the Investigation page, when a search result is saved as a report template, a Customized Widget will also be generated. However, Customized Widgets cannot be generated by LinkGraph.

The following figure illustrates saving a Bar Chart from the investigated result to a report template. The queries and settings for that specific investigation will also be saved.

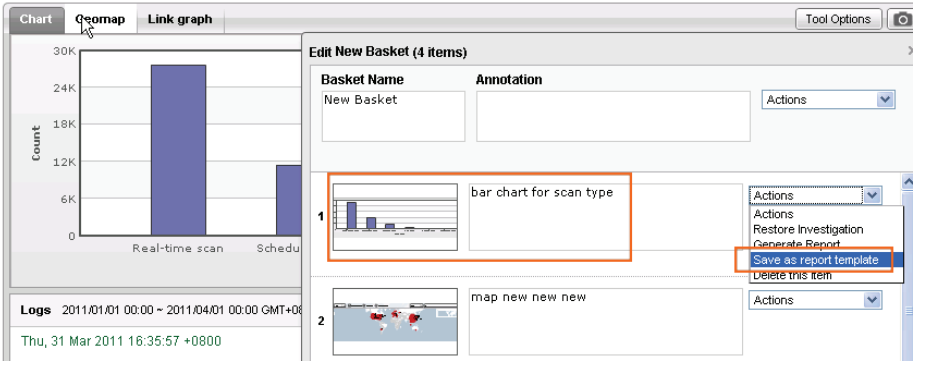


FIGURE 2-12 Saving a Customized Widget

Customized Widgets can be added to the Dashboard from the "Add Widgets" page as shown in the following figure.

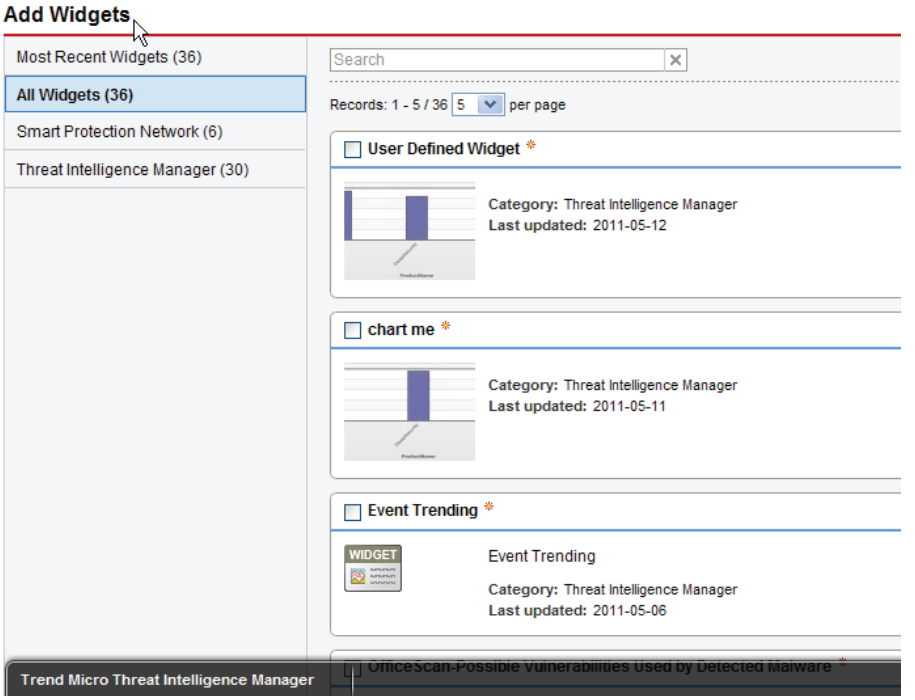


FIGURE 2-13 Adding a Customized Widget to the Dashboard

Chapter 3

Investigation

The features of the Trend Micro™ Threat Intelligence Manager Investigation tab are discussed in this chapter.

Topics include the following:

Using Investigation

The Investigation tab, as shown in the following figure, is a visualization-aided investigation flow that allows you to discover relevant information about particular incidents.

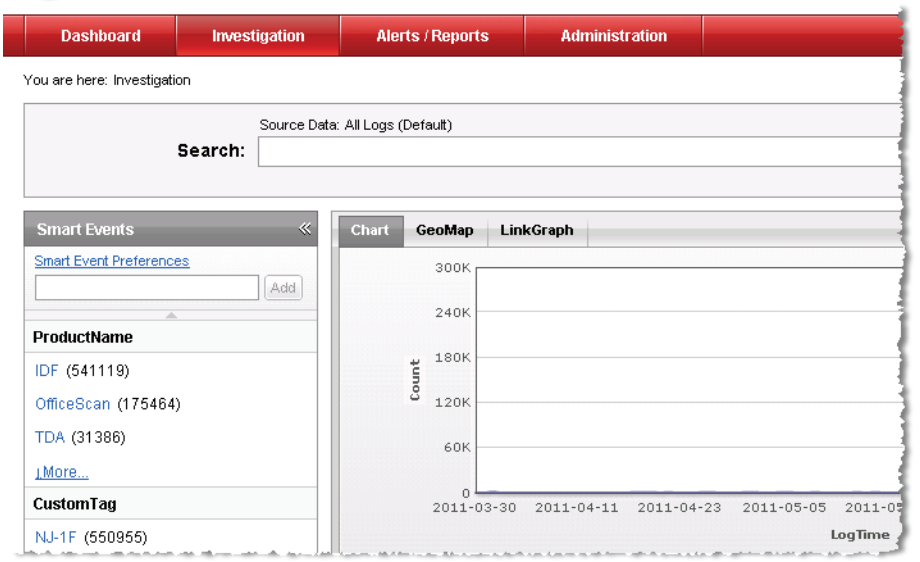


FIGURE 3-1 Investigation tab

Event logs (as seen in Figure 3-2) that are collected by the Threat Intelligence Manager platform through integrated products (see Agent System Requirements on page 1-4) are available for your investigative review.

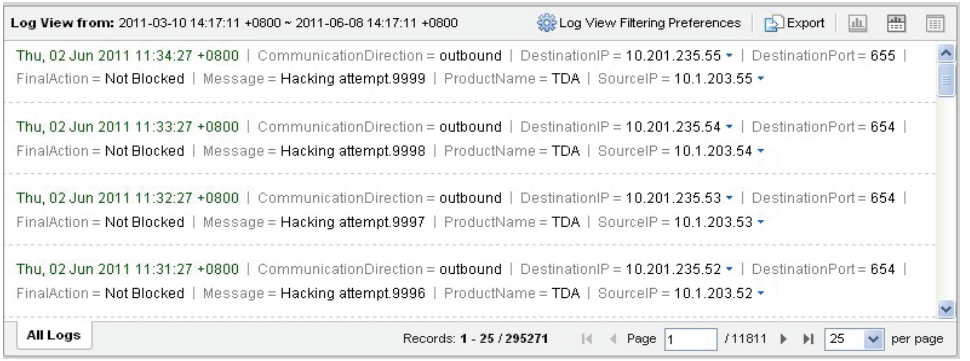


FIGURE 3-2 Event Logs Example

This review consists of:

- A search bar for inquiring on the scope of event logs for investigation.

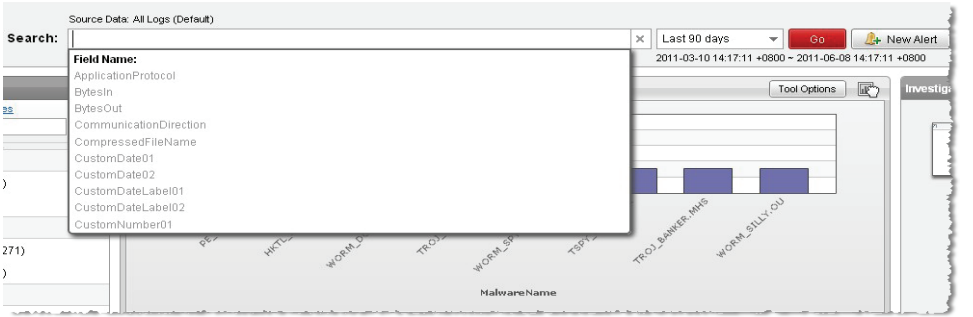


FIGURE 3-3 Search Bar Example

- Smart Events to categorize the queried event logs by showing the number of each category.

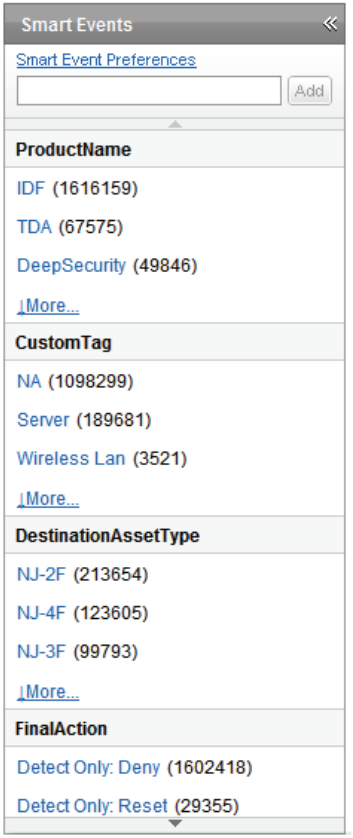


FIGURE 3-4 Smart Events Example

- Threat Intelligence Manager provides the following visualization tools:
  - The Charts tool is used to display logged events through table, bar, pie, and line charts.
  - GeoMap is a tool designed to display logged events that have been tagged using the Geo Information from a world map.

- LinkGraph is a tool designed to display the relationship of the source and destination IP addresses, as well as the destination port events.

- Event Logs that show the logs available to aid in your investigation.
- Investigation Basket(s) for saving investigation results from the report and then generating reports and report templates. See Investigation Baskets on page 3-27 for additional information.

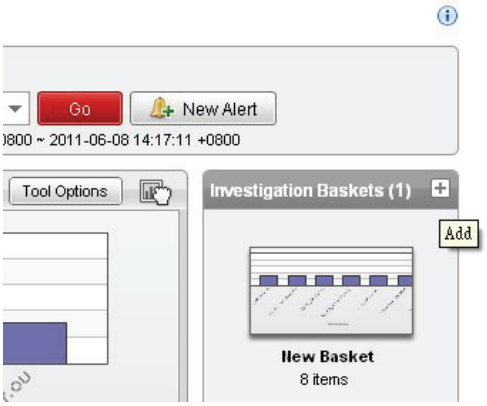


FIGURE 3-5 Investigation Baskets Example

- Utilities to provide extra information related to the keyword selected from the event log view or LinkGraph. See Context Menu on page 3-55 for additional information. You can also use this tool directly.

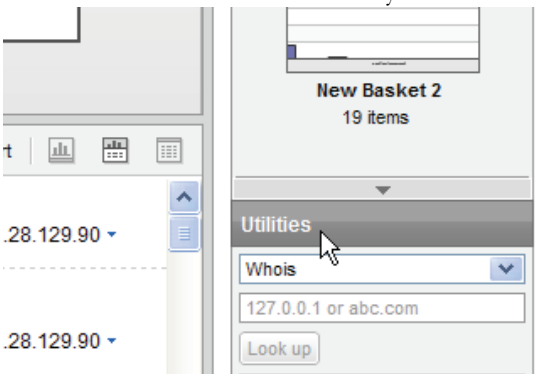


FIGURE 3-6 Event Log Utilities Example

Prerequisites

In order to effectively investigate the activity reported from your agents, you should have:

- added source logs to help initiate the log collection
- provided tagging data such as GeoIP or Asset tagging for your collected logs
- initiated log deployment

Search

Input query strings in the Search bar to help you decide your investigation event log scope. The Search bar consists of a search text field, bread crumb access, a time range drop-down list, the "Go" button, and the "New Alert" button.

FIGURE 3-7 Search Bar Detail

Source Data

Display a string above the search text field to explain the source of the current search query. The corresponding message is listed in the table that follows.

TABLE 3-1. Source Data

QUERY SOURCE	MESSAGE DISPLAYED
Widget on the Dashboard	Source Data: Widget: **Widget Name**
Report Template	Source Data: Report: **Report Template Name**
Report	Source Data: Report: **Report Name**
Alert	Source Data: Alert: **Alert Name**

TABLE 3-1. Source Data (Continued)

QUERY SOURCE	MESSAGE DISPLAYED
One Item in the Report Basket	Source Data: Report Cart: **(Basket Name: item number)**
Enter Investigation Directly	Source Data: **All Logs (Default)**

Search Bar

To utilize the Search feature, enter an input query string in the Search bar window. Input the query condition directly, or click the "Add as a keyword," "New Search," or "Free Form Search" options on the context menu from the Log View, GeoMap, or LinkGraph features.

Valid Search Input

To successfully enter valid Search content, follow the content guidelines defined in the following paragraphs.

Threat Intelligence Manager offers three different Search types. The first is the Free Form Search (such as OfficeScan or Quarantined). The second is the Name-Value Pair Search (such as `ProductName=OfficeScan` or `FinalAction=Quarantined`). The last is a Relational Expression Search (such as `SourceIP IS NULL`).

Tip: With the Free Form Investigation Search, your search can be expedited through partial matching. However, with the Name-Value Pair Search, the search requires an exact match. It is important you do **NOT** combine these two search types within the same search effort.

Each Search must be separated by a binary logical operator such as AND, OR, or NOT. OR is the implicit default operator. For example, `ProductType=Desktop [OR] MalwareType=VIRUS`. The system retrieves the records where the MalwareType is VIRUS, or the ProductType is Desktop.

Note: All operators must be entered in uppercase characters. For example, AND, OR, IS NULL, IS NOT NULL, RANGE FROM ... TO ..., and so on.

1. For Free Form Searches, you can search logs using a keyword that utilizes partial matching. For example, when searching for the keyword "Quarantined." The guideline is as follows:
   - A keyword is a term used with or without spaces. A single-quoted search keyword is required to allow for any literal spaces you want to include such as when searching for a phrase or title such as 'Trend Micro.' This keyword limits your search to only that particular literal phrase, and skips other similar results such as "Trends," "Trendy," or "Trended."
   - Keywords are NOT case-sensitive (meaning the keyword 'Virus' is the same as 'virus').
   - Keywords that are "system reserved" must be single-quoted. They are AND, OR, NOT, IS, NULL, RANGE, FROM, and TO.
   - Wildcards are NOT supported.
   - Reserved characters included within a keyword search phrase must be escaped using the backslash "\" character. The five reserved characters are *, %, ?, ', and \. For example: `C:\\system32\\malware.html`.
   - Keywords must be single-quoted when they contain at least one of the these three characters: =, (or). For example, 'Detected Terminal Services (RDP) Server Traffic'.
   - Double-byte values are supported in Free Form searches, but they must match exactly.
2. For a Name-Value Pair Search, you can search logs using a FieldName that is associated with a value using the format of `FieldName=Value`, as long as it matches exactly. For instance, with the `ProductName=OfficeScan` example, refer to the following:
   - A value is a term with or without spaces. Values containing spaces must be single-quoted.
   - The value used in the `FieldName=Value` paring is case-sensitive. For example: `DeviceNTDomain=workgroup` is different from `DeviceNTDomain=Workgroup`.

- Values that are "system reserved" must be single-quoted. They are AND, OR, NOT, IS, NULL, RANGE, FROM, and TO.
- Wildcards are supported and can be used for expressing various values. Note that no leading wildcard is supported. Wildcards can only appear in the middle or at the end of a value. Multiple character wildcards are denoted by either an asterisk (*) or the percent sign (%). For example: `MalwareName='TROJ*'` or `MalwareName='TROJ%'`. The system will retrieve logs with malware names starting with 'TROJ.' For a single-character wildcard, these are denoted by a single question mark (?). The respective reserved character rules for unquoted and quoted strings, mentioned previously, must be observed.
- Reserved characters included within a keyword search phrase must be escaped using the backslash "\" character. The five reserved characters are *, %, ?, ', and \. For example: `FilePath=C:\\system32\\malware.html`.
- Keywords must be single-quoted when they contain at least one of the these three characters: =, (or). For example: `RuleName='Detected Terminal Services (RDP) Server Traffic'`.
- Double-byte values are supported in Name-Value Pair searches.

3. The search feature also supports relational expressions such as "IS NULL," "IS NOT NULL," "RANGE FROM … TO …" and so on. Relational expressions can be enclosed by parentheses or not. For example:
   - (RequestURL IS NULL)
   - (RequestURL IS NOT NULL)
   - (RuleID RANGE FROM 100 TO 200)

Note: The "RANGE FROM" operator only applies to certain fields such as RuleID and Severity.

4. Searches using a negation operator such as (NOT) in front of any of the previously described search terms will be treated as a single search term. For example, if your search string is NOT 'OfficeScan' and 'Detect Only: Deny,' the system retrieves the logs that do not contain 'OfficeScan' and still includes the term 'Detect Only: Deny.' NOT is only applicable in Free Form and Name-value Pairs searches.

5. IP Address Wildcard Support

   IPv4 subnet wildcard support is allowed. But, IPv4 wildcard support is only applicable to the values of the Name-Value Pair Search using the asterisk (*).

   For example:

   - SourceIP=127.1.* (allowed)
   - SourceIP=127.1.1* (is not allowed)

   Classless Inter-Domain Routing (CIDR) Support

   The format is A.B.C.D/N, A.B.C.D is represented a IPv4 addresses, N is denoted by a number between 0 and 32.

   For example:

   - SourceIP=10.202.132.0/25 matches the first 25 bits of the address.
   - SourceIP='10.202.132.0/25' (Allowed)
   - SourceIP='10.202.132.0'/25 (is not allowed)

   Subnet Mask Support

   For example:

   - SourceIP=10.202.132.14/255.255.0.0
   - SourceIP='10.202.132.14/255.255.0.0'
   - SourceIP='10.202.132.14'/255.255.0.0 (is not allowed)

6. Searches can also be grouped together using parentheses. Parentheses can be nested. The conventional precedence for nested parentheses is observed. For example: MalwareType=VIRUS AND (SourceIP=127.0.0.1 OR DestinationHostName=myhome)

Tip: Queries with more than two operators could use parentheses to set execution priorities to avoid the ambiguous result.

Auto-complete

There are two kinds of auto-complete. The first is the Name-Value Pair (Field_name=<suggestion>) search. The other is the Free Form search (only a keyword with no field name). The system uses two types of auto-complete to suggest possible terms and some fields in the recommendation box to help you input your search conditions. The two types are described as follows:

- Field Names that match fields already in the database. These fields are ordered alphabetically. The field matching is NOT case sensitive.
- Possible terms that match the top five values in the total logs. The possible terms are case sensitive.

Note: The system dynamically filters the possible terms and field names based on the user-typed strings **without considering the time range**.

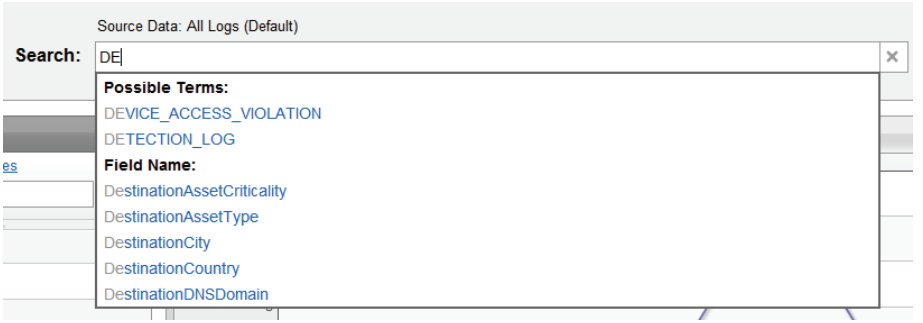


FIGURE 3-8 Auto-complete Search Feature

The following details the rules - how the system will display the recommendation box. Only the following scenarios include auto-complete. In other words, there are some

situations where the system will not include the auto-complete feature such as when the query string includes NOT, parentheses, rational expressions, and so on.

TABLE 3-2. Search Scenarios

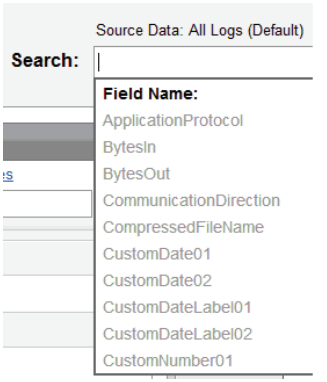
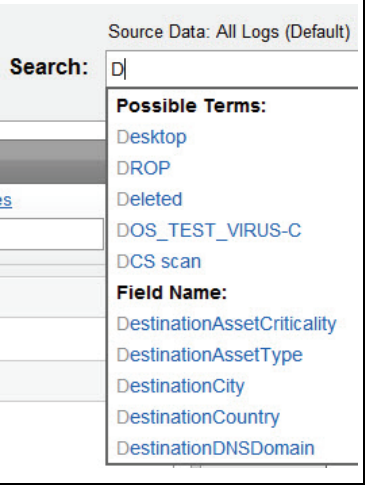
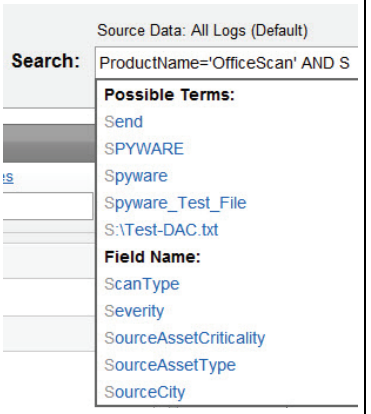
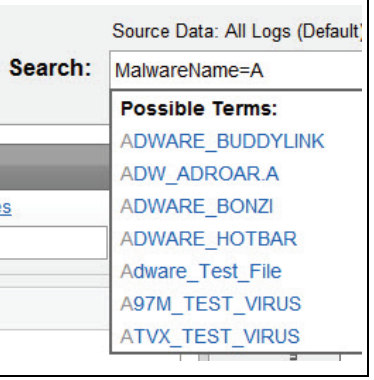
SCENARIOS	CONTENTS OF THE RECOMMENDATION BOX	EXAMPLE
Empty	Provide the field name that is in the database. • Field Name: 10 records.	
Letter	Provide the related field name and possible terms. • Possible Terms: 5 records. • Field Name: 5 records	

TABLE 3-2. Search Scenarios (Continued)

SCENARIOS	CONTENTS OF THE RECOMMENDATION BOX	EXAMPLE
Operator (AND,OR, NOT)	Provide the related field name and possible terms. • Possible Terms: 5 records. • Field Name: 5 records	
Equal Sign	Provide the related possible terms that belong to this field. • Possible Terms: 10 records.	

Note: There is a field that is an exception, the date field. The system only supports the Name-Value Pair suggestions. It does not support Free Form suggestions. For example: LogTime=2011 will provide you with suggestions, but simply typing 2011 will not show you the values from any date fields.

Filter

The feature provides your filtering conditions found under the Search bar. Think of it as a bread crumb that helps you narrow down your data scope based on your current searches. See Smart Events on page 3-20 for additional information.

"X" Icon

Click the "X" icon to clean or remove all search conditions. The system will return to its default settings. In so doing, the system retrieves the logs created within the last 24 hours without the use of any keywords, bread crumbs, and user-selected fields. For user-selected fields, see Smart Events on page 3-20 for more information.

Time Range Drop-Down List

If no query strings have been entered, by default, the investigation scope will include all event logs after you determine the investigation log duration. This duration could be over the last four hours, the last 24 hours, the last seven days, the last 30 days, the last 90 days, or within a customized range. When no duration period has been selected, the default configuration of 24 hours will be used.

Note: All search time ranges indicate the server time of the Threat Intelligence Manager server.

Go

You can execute a query based on the current search conditions. For example, see Figure 3-7. The system retrieves logs wherein the FinalAction was 'Cleanup failure' and the logs originated from OfficeScan within the last 7 seven days.

New Alert

You can directly save a query string as an Alerting Rule from the Search bar. Refer to Adding Alerts on page 4-3 for additional information.

Log View

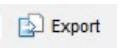
The Log View window is designed to show queried event logs that can be displayed together within the Investigation page. On the Investigation page, you can define the raw data of the returned logs that you want to appear in the Log View. If no other data is provided, the system default values will be used. When you save the investigation results, only the graphs will appear in the Investigation Basket.

In the Log View, you can:

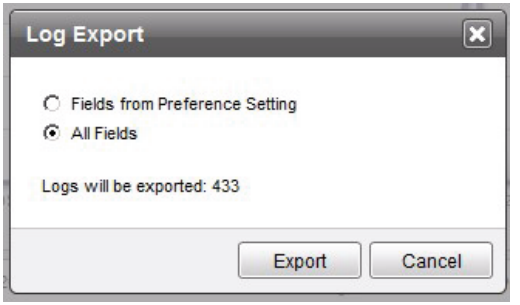
- Configure a display showing the items that will appear in the Log View panel.
- Click on an item and then select **New Search**, **Add as a keyword**, or **Free Form Search** to launch a new search or to narrow down your original search scope. "Free Form" searches allow you to launch new searches using a value as a search keyword.
- You should be able to see a Search Within tab in the Log View panel that is integrated with all other visualization tools (For example: Click one bar on the Bar Chart).
- Enter a utility from an IP/URL field.

Export:

1. From the Log View window, click Export as shown in the following figure.



The Log Export page appears where you can send log data to a CSV file.



2. Choose to export logs through the "Fields from Preference Setting" or the "All Fields" setting. When exporting logs by Preference Settings, Threat Intelligence Manager only exports the data regarding preference settings.

Note: You can only export 40,000 logs. If your exported logs number over 40,000, only 40,000 of them will be exported.

Panel Sizing:

1. Using the View buttons, change your panel view size from Chart View (full), Hybrid View (half), and Log View (minimum).
2. Click the Hybrid View option as shown in the following figure.

Interaction with tools:

1. When you click the visualization tool, the related logs are highlighted on the view. For example, click any bar on the Bar Chart and see the associated data highlighted

in the Log View as shown in the following figure. All chart types support this process similarly.

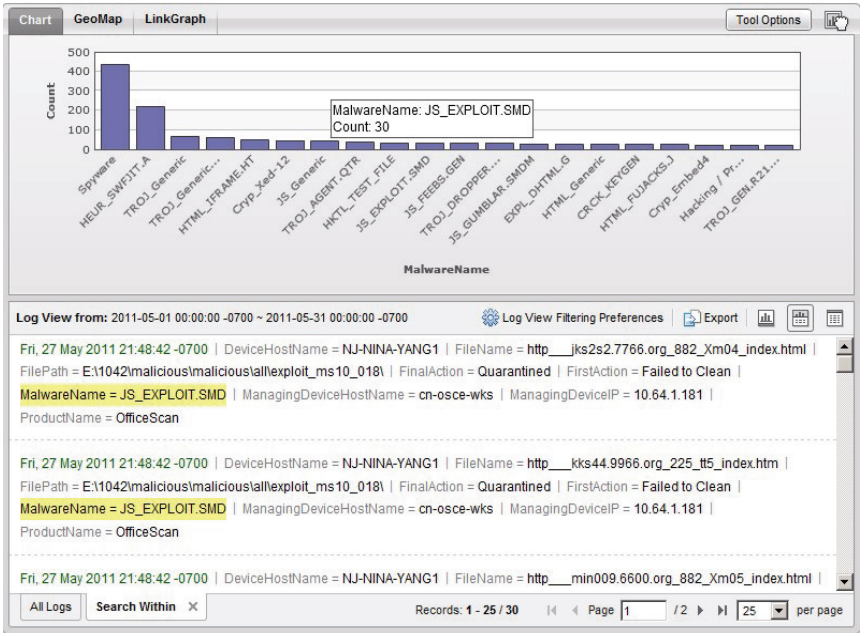
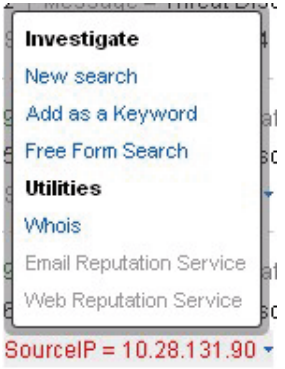


FIGURE 3-9 Search Within Log View Tab

2. Go to a desired utility from a IP or URL in the event logs by clicking the log entries with the blue arrows.



Log View Filtering Preferences

To access the Log View Filtering Preferences shown in the following figure.

1. Click **Investigation > Log View > Log View Filtering Preferences**.

The Filtering Preferences page appears.

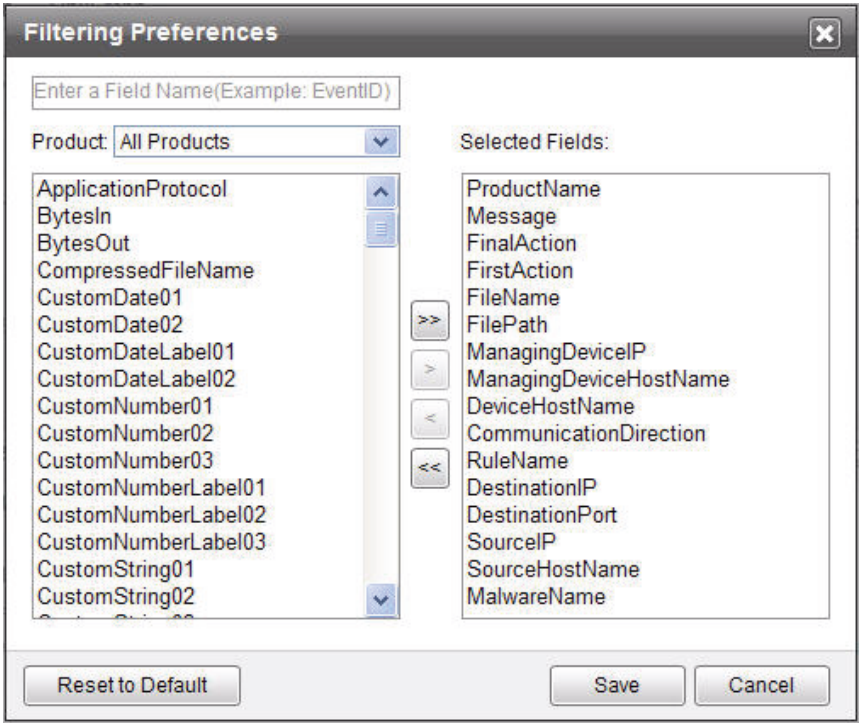


FIGURE 3-10 Filtering Preferences

2. Configure the fields based on your needs. Use the arrow buttons to move the variables in and out of the right column.
3. Selected fields in the right column are the fields you want to display by default. If you want to restore the default settings, click **Reset to Default**.

4. Use the Field Name filtering field to narrow results quickly. For this example, when you type 'dest,' Filtering Preferences filters other options and only displays the fields that contain 'dest,' as shown in the following figure.

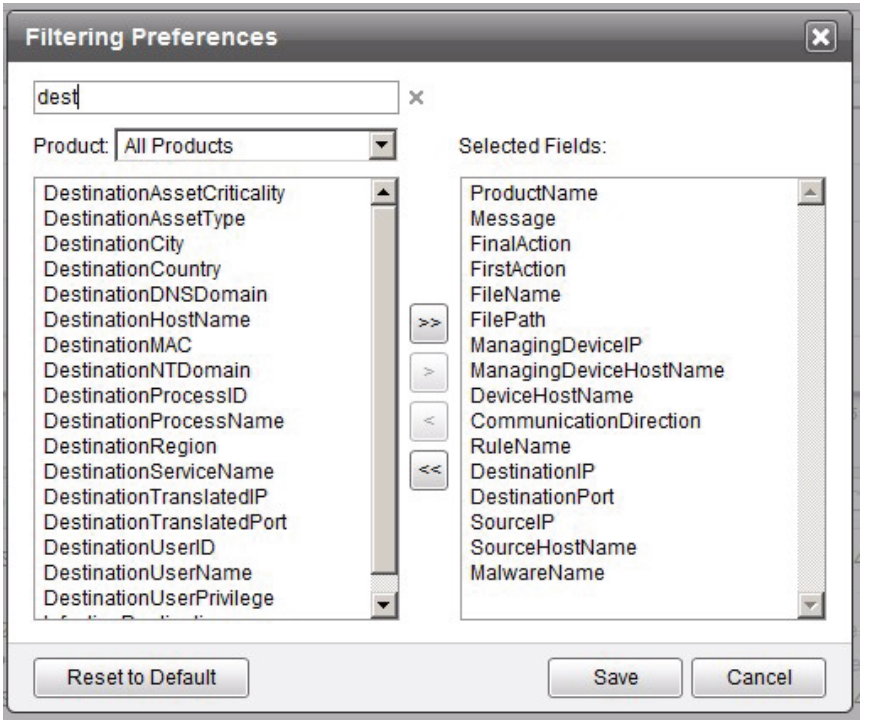


FIGURE 3-11 Filtering Preferences with Narrowed Results

Smart Events

Smart Events are designed to categorize queried event logs for all investigation tools and assist you in narrowing down the data. Using data fields, such as event types and product names, you can automatically categorize the queried event logs and show the actual log numbers of each field. For example, based on statistics provided by Smart Events, you can discover the names of the most detected virus events from the last 24 hours.

Tip: Drag your mouse over any of the field titles to see a field name description as a Tool Tip.

The Smart Events panel along with some sample event data are shown in the following figure.

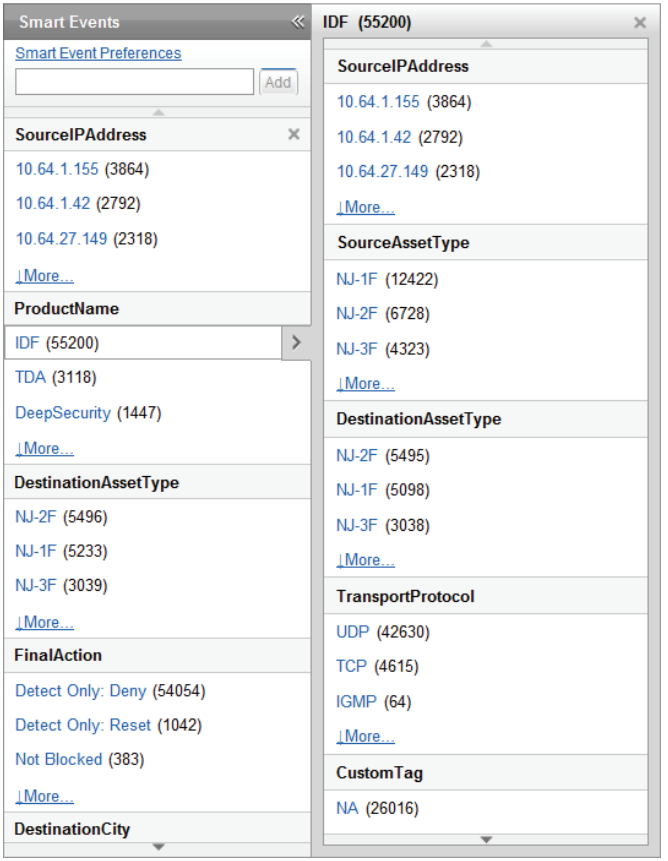


FIGURE 3-12 Smart Events Panel

Smart Events are separated into three fields in the Smart Events Panel.

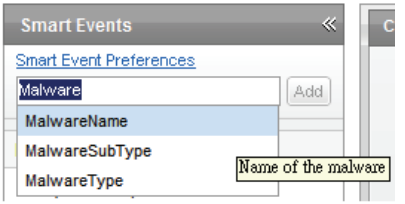
- The Smart Events Preferences field: Use the Smart Event Preferences to configure the fields that you want to appear by default. This means that every time you log in to Threat Intelligence Manager, you will see that field listed as a Smart Event. For additional information see Smart Event Preferences.
- The "Add" field: Add or remove this user-selected field (see To add a user-selected field:) during run-time and without limitation by clicking **Add** and selecting from the available options. User-selected fields can be removed by clicking the "X" next to the field name.
- The system-suggested fields: Threat Intelligence Manager will recommend fields that you might be interested in using according to your recent operation. If you have not added any user-preference or user-selected fields, the Smart Events panel default will show system-suggested fields for your reference.

The priority of these three field types is:

- User-selected fields
- User-preference fields
- System-suggested fields

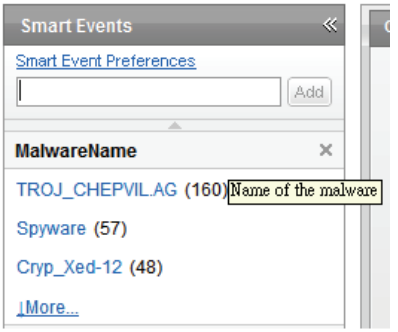
To add a user-selected field:

1. Type a string to search for the field name you want to add (such as Malware).



2. Upon a successful search, select the field name you want (such as MalwareName).
3. Press **Enter** or click **Add**.

See the following figure as an example.



Note: The newest fields always appear at the top of the Smart Event panel.

Narrowing Down Your Data

There are other procedures you can utilize to help narrow down your search results. These procedures include Bread Crumbs and Subpanels.

Bread Crumbs

When you click one of the field's values, it is added into the search string to help narrow down the investigation event logs. All relationships between bread crumbs use the "AND" variable. When you click the 'OfficeScan' value, its field name is 'ProductName,' based on the current scenario - such as the query string, bread crumbs, time range, and so on. This value will then be added to your search bar. In this case, the log only contains those logs in which the value of the `ProductName` field is OfficeScan. This will help you narrow down your Investigation event logs. The maximum number of bread crumbs is 10, and all bread crumbs can be deleted independently. When you move the mouse over a bread crumb or the "X" icon, the value displays under the search text

field and you can mouse-over the filter value to see the entire condition as a Tool Tip, as shown in the following figure.

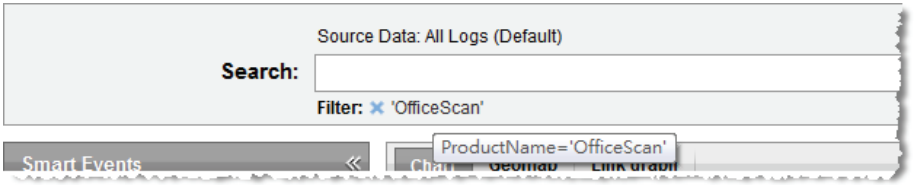


FIGURE 3-13 Bread Crumbs with Mouse-over

Note: After being added as a bread crumb, the field disappears from the Smart Events panel. In this case, it is `ProductName` that will disappear from the Smart Events panel.

Subpanels

Smart events can categorize, value, and sort values numerically. Subpanels provide a previewing mechanism that allows you to "peek" into your Smart Event results without changing your current search criteria.

For example, you can peek into the Smart Event results for `ProductName=TDA` or `ProductName=OfficeScan`. If you decide to narrow down your data using `ProductName=OfficeScan` and `FinalAction=DROP`, click "DROP" in the Smart Events subpanel. Then, your Investigation will add `ProductName=OfficeScan` and `FinalAction=DROP` into your search criteria. The Clear, or "X" button only appears after you input characters into the fields. Click the "X" at the top right corner of the Subpanel to close the panel.

Because the selected values are considered to be an anchor, the recommended fields that appear will change on the Subpanel. Click any of the values that appear to further

filter-down your search results. The following figure is an example of a Subpanel you might see for OfficeScan.

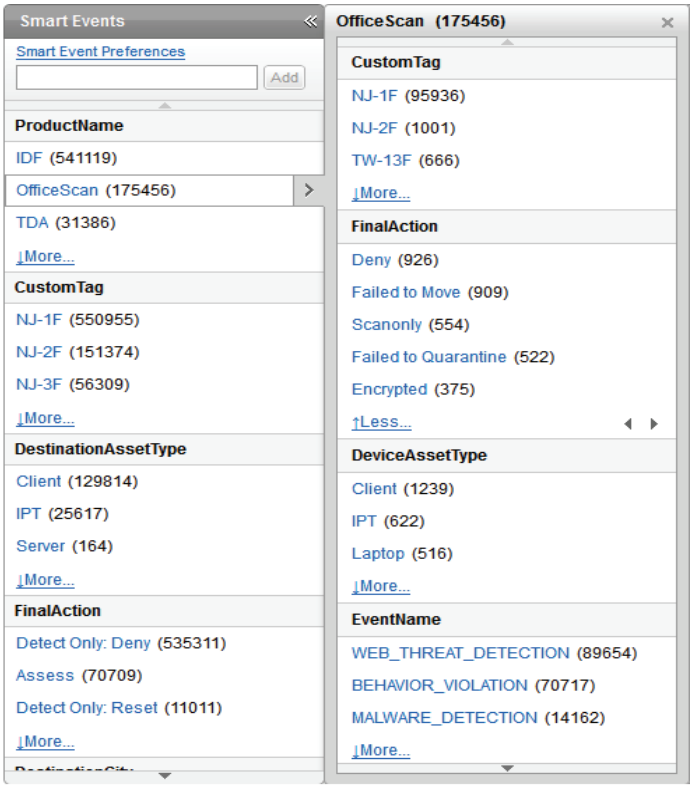


FIGURE 3-14 Smart Event Subpanel for OfficeScan

Pagination

Threat Intelligence Manger can display up to 10 fields per page. Click the "▲" and "▼" arrow icons to scroll up and down the panel. When the panel is at the bottom, the system displays the next 10 fields of the panel.

For the values in a field:

By default, the panel displays three values in a field at a time. Click **More** to view additional values. Click **Less** to reduce the space vertically, and return to the initial three

values. Use the right arrow icon to view the next five values and the left arrow icon to view the previous five values.

Smart Event Preferences

As mentioned in the previous section, Smart Event Preferences can be selected to further drill down returned results. Select a maximum of five fields to help you display results according to your requirements. Select to filter All Products, Deep Security Manager (DSM), Threat Discovery Appliance (TDA), Intrusion Defense Firewall (IDF), or OfficeScan products along with the filtering criteria you determine.

To access the Smart Event Preferences:

1. Click **Investigation > Smart Events > Smart Event Preferences**.

The Smart Event Preferences page appears.

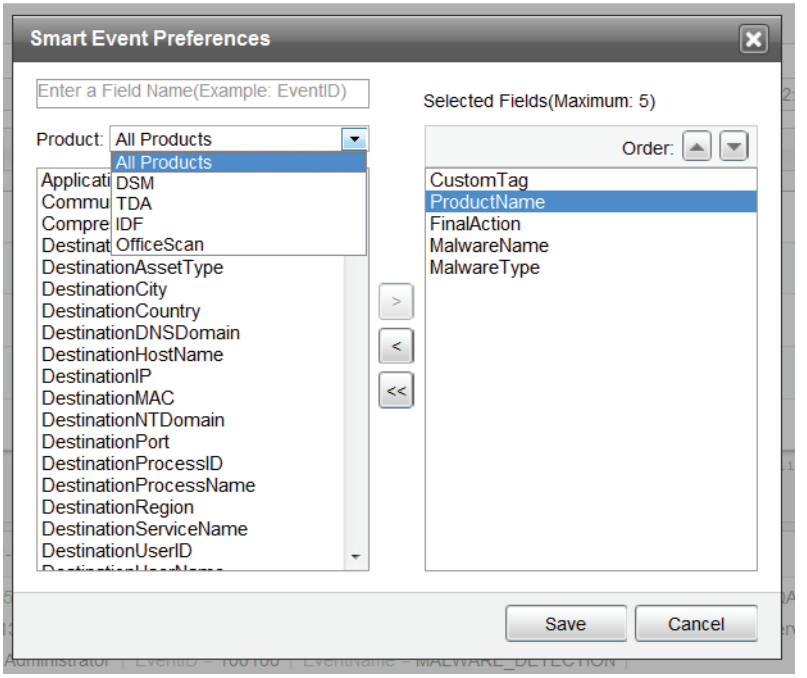


FIGURE 3-15 Smart Event Preferences page

2. Configure the fields based on your requirements. Use the arrows to move the variables in and out of the right column, and provide the following functions:
   - **Ordering** - Change the order of the field by highlighting it and pushing the Order arrow buttons on the top right up or down to the desired order.
   - **Filtering Text Fields** - At the top of the page, enter a Field Name such as EventID to determine the source value with which you would like to begin filtering. You can click the "X" at anytime to clear the filtering string.
   - **Filtering Product List** - Under Product, sort depending on the criteria you select from a specific product such as TDA, or select to see the filtering options for All Products.
   - **Field List** - The Field List alphabetically displays all your filtering options from which you can choose. This list's contents are dependent on the Products you selected earlier and might change if you chose TDA before, then opted to filter for IDF instead. Dragging your mouse over any of the titles will provide a field name description for each field as a Tool Tip.
   - **Selected/Deselected Fields** - Using the buttons in the center of the page, you can move deselected field names to the selected side by clicking the right arrow. Move it back by clicking the left arrow. To remove all selected fields, click the double left arrow.
   - **Save/Cancel button** - Click **Save** to maintain the settings you have selected or **Cancel** (X) to remove all preferences without saving.

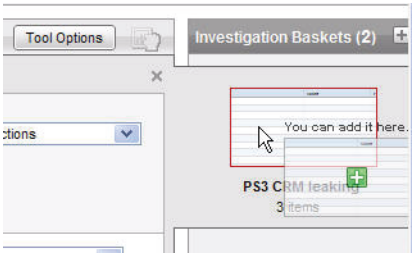
Note: In the Smart Events panel, you might see RuleIDs with product names associated with TDA that include no details or rule descriptions. For more information about TDA Rules, see TDA Rules in the Online Help.

Investigation Baskets

This area is designed to contain the unsaved investigation results of your reports.

You can drag the 'Drag Me' icon  next to the Tool Options button to save your investigation results to the Investigation Baskets. After right-clicking the 'Drag Me' icon, hold and drag it near the basket icons you want to save until you see a small green "plus"

icon at the center of the preview image and then release the mouse button as shown in the following figure.



The new basket result will appear similarly to the following figure.

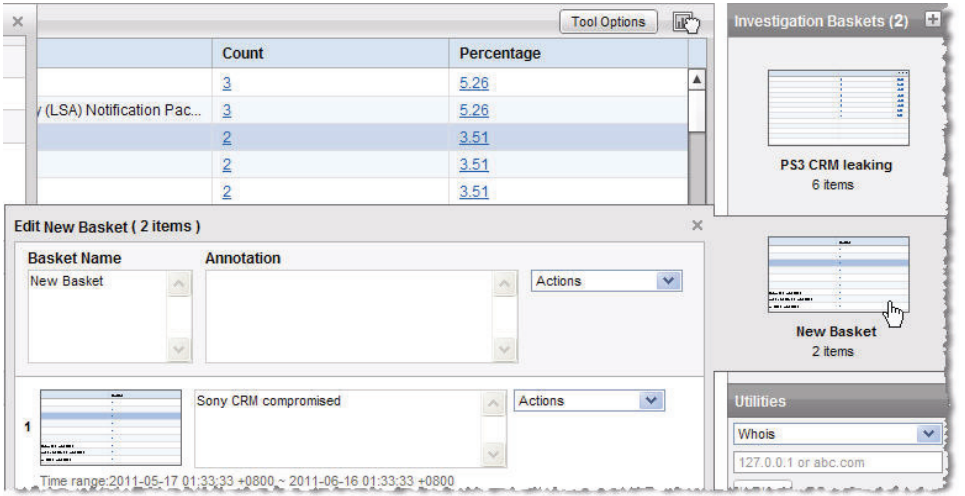


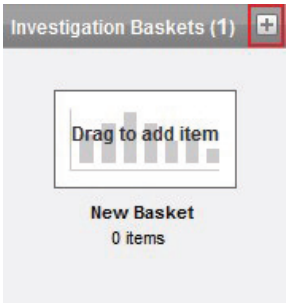
FIGURE 3-16 Editing Investigation Baskets

The Investigation Basket can contain a maximum of 15 baskets that contain 30 saved investigation items in each basket. You can create or delete these baskets at any time. However, when a basket is deleted, all saved investigation results will be deleted as well.

Adding a New Investigation Basket

To add a New Investigation Basket:

1. Click **Add** at the top right side of the Investigation Baskets title bar (+ symbol) as shown in the following figure.



The "Add a New Investigation Basket" pop-up appears.

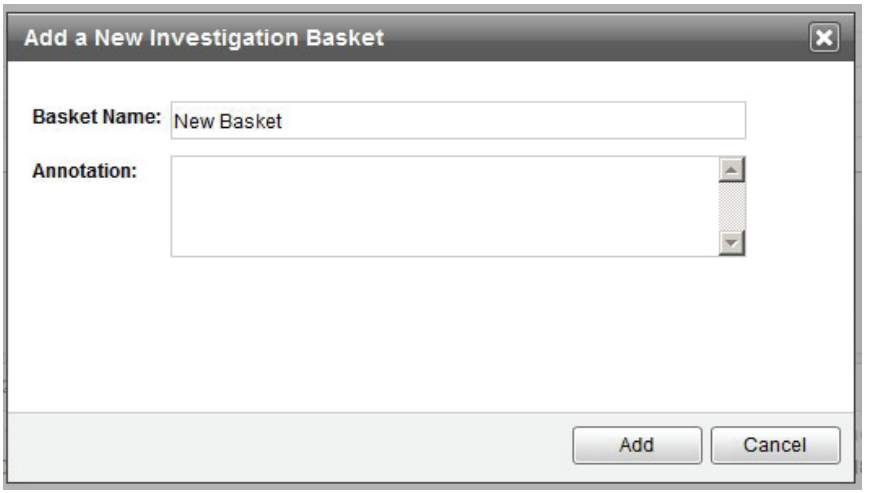


FIGURE 3-17 Adding a New Investigation Basket

2. In Basket Name, you can name the report basket something that will help you identify its contents.

3. Enter an "Annotation" if you believe further explanation is necessary to identify the contents of this particular basket.
4. Click **Add** to create the new report basket, or **Cancel** if you no longer wish to create the new basket.

Editing Investigation Baskets

Edit the title and annotation for a basket or items within a basket.

To edit an Investigation Basket:

1. Open an Investigation Basket by clicking the basket you would like to edit.
2. Place your cursor in the Basket Name or Annotation text fields.

   The **Save** and **Cancel** options will only display when your cursor is in a text field as shown in the following figure.

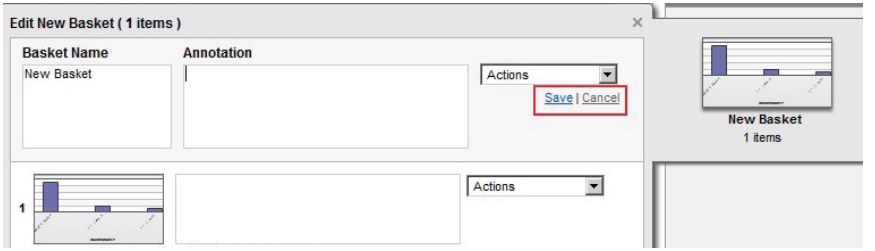


FIGURE 3-18 Editing an Investigation Basket

3. Enter or change the text in the text field.
4. Click **Save** to preserve your settings or **Cancel** to start over.

Basket Actions

You can access the Basket Actions (the first tier basket displayed) by clicking an Investigation Basket. The Edit Basket page appears. Click **Actions** and the associated actions will appear as shown in the following figure.

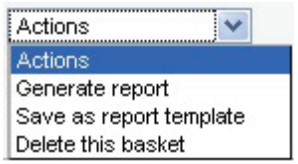


FIGURE 3-19 Available Basket Actions

- From the Actions drop-down menu choose **Generate report** to generate a report from the investigation results. This will generate the report that contains all the items in the basket.
- From the Actions drop-down menu choose **Save as report template** to save the investigation results as a report template. This will save all the items in the basket into a report template.
- To delete a basket, from the Actions drop-down menu choose **Delete this basket**.

Note: Different login users have different stored baskets and different investigation results stored within those baskets.

Item Actions

You can access the Item Actions (the second tier by clicking any of the Investigation Baskets). Click **Actions** for the saved item and the associated actions will appear as shown in the following figure.

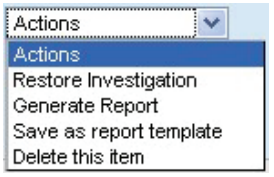


FIGURE 3-20 Available Item Actions

- From the Actions drop-down menu choose **Restore Investigation** to return to the current state of the investigation tool. Restore Investigation can be used to restore your investigation to the state of a stored basket item. Then you can perform further analysis on those logs.
- From the Actions drop-down menu choose **Generate Report** to generate a report from a Report Basket item.
- From the Actions drop-down menu choose **Save as report template** to save the search criteria, log duration data, and so on as a report template.
- From the Actions drop-down menu choose **Delete this item** to delete Report Basket items.

Note: Different login users will have different stored baskets as well as different investigation results within those baskets.

Utilities

Utilities provide additional information regarding the values you selected in the Log View or for the values you are interested in learning more about. If your values are not compatible with the selected tool, the system will remind you with an error message or gray out the tool from the Log View.

The utility options are shown in the following figure.

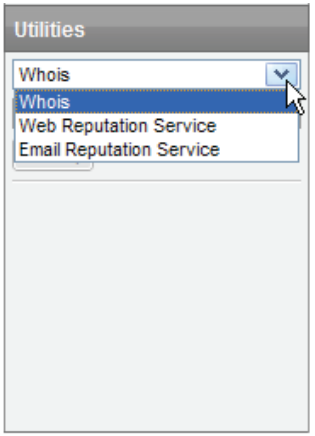


FIGURE 3-21 Utilities

The utilities include:

- **Whois**

Use the Whois utility to query information about to whom the IP address (such as 127.0.0.1) or the domain name (such as trendmicro.com) is associated. By default, Whois will query from the ARIN Web-service, so the system will dependably help you find exact information about the provided address.

- You can execute the Whois service in one of the following three ways.
  - Execute Whois from the Utilities panel directly.
  - A value with a field name such as `SourceIP\DestinationIP` in the Log View panel.
  - A node with a value such as `SourceIP\DestinationIP` in LinkGraph.

Note: The Whois service needs to connect to the ARIN Web-service trough TCP port 43.

- **Web Reputation Service (WRS)**
  - Threat Intelligence Manager provides URL/domain reputation feedback from the Trend Micro Smart Protection Network-WTP database. The results contain four safety ratings and eight content ratings. The following represents the Safety and Content Ratings page.

FIGURE 3-22 Safety and Content Ratings Description page

- Execute the Web Reputation Service in one of the following two ways:
  - Execute in utilities panel directly.

    Select Web Reputation Service (WRS) from the drop-down list and manually enter a URL and press **Look Up**.

- A value with the field name RequestURL can also execute a WRS query from the log view panel.

Note: Make sure the proxy settings are correct if the proxy is necessary in your network environment. For more information about Proxy Settings, see Proxy Settings on page 5-34.

- **Email Reputation Service (ERS)**
  - The sender of spam-email can be identified by query through the Trend Micro Smart Protection Network-ERS database. The returned data can be returned in one of two types, one is safe - the other dangerous. See Figure 3-23. The returned data can only come from the log view panel, and only values with the field name of `SourceIP` and this log's `DestinationPort = 25` can be executed in the ERS query.

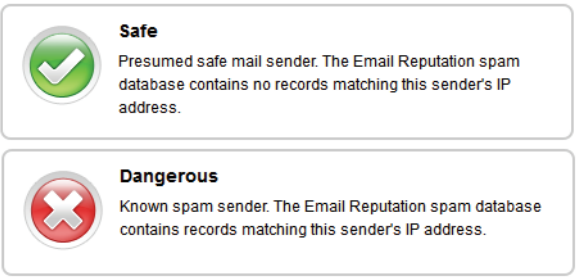


FIGURE 3-23 Email Reputation Service Results

Chart Tools

The Investigation tab provides a chart view option to help you view your queried logs, however, Threat Intelligence Manager can only display one chart view at a time. You can select a bar chart, line chart, pie chart, or a table.

Whether you decide to investigate through a widget or directly from the Investigation tab, use the preferred chart type for that widget or Investigation page.

Note: The chart does not render all search results because the required fields do not exist in some of the queried logs. That means the result might be different between the chart and Smart Events/Log View panel.

Generally, the chart tools include the following options:

- The capability of switching between different chart tools.
- Default settings are applied when you log in for the first time. After the chart tool settings have been changed and applied, the next time you click on the data set presented in the chart tool, the related logs will be highlighted in the Log View. The chart displays with the last applied settings.
- When logging out or closing the browser, the configuration of each tool will be maintained for future use.
- When you click on a chart tool, the related logs in the Log view are highlighted.
- The capability of saving your charts into the Investigation Basket.

Tip: As part of a chart's percentage calculation, the common denominator is the number of logs that contain a certain specified field. For example, if there are a total of 100,000 logs in the log system, and 80,000 logs contain values in the "Malware Type" field, but the other 20,000 logs do not. When displaying the Malware Type chart, Threat Intelligence Manager uses the 80,000 logs as the common denominator to calculate each item's percentage. The item percentage displayed on the UI on a Table and Pie chart are calculated differently. Currently, the max items for each chart can only display 200 items. When there are more than 200 items, Threat Intelligence Manager can only recalculate it as a Pie Chart with each item's percentage with the sum of the displayed items counting as the denominator. Table keeps the original percentage without recalculating it.

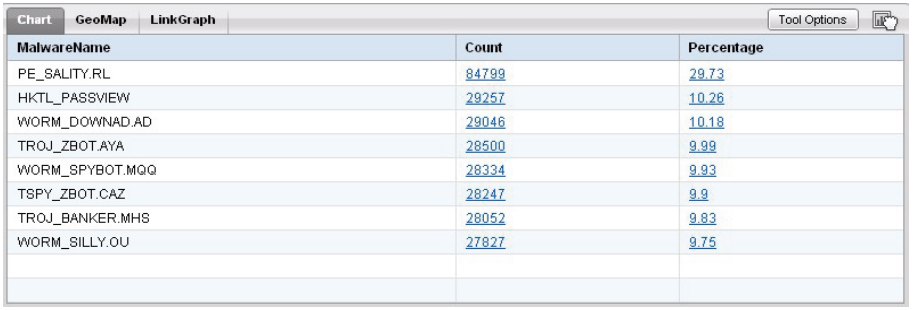
Continuing with this example, there are 80,000 logs that contain the "Malware Type" field and the first 200 Malware Type items correspond to 65,000 logs (items are sorted by count before calculation). Threat Intelligence Manager uses 65,000 as the common denominator to calculate the displayed item percentages so the whole pie always represents 100 percent.

When displaying the Top N or N% items, the settings use the same calculation.

Chart Types

The following are examples of the types of charts from which you can choose.

- Table



MalwareName	Count	Percentage
PE_SALITY.RL	84799	29.73
HKTL_PASSVIEW	29257	10.26
WORM_DOWNAD.AD	29046	10.18
TROJ_ZBOT.AYA	28500	9.99
WORM_SPYBOT.MQQ	28334	9.93
TSPY_ZBOT.CAZ	28247	9.9
TROJ_BANKER.MHS	28052	9.83
WORM_SILLY.OU	27827	9.75

FIGURE 3-24 Table Chart Example

- Bar

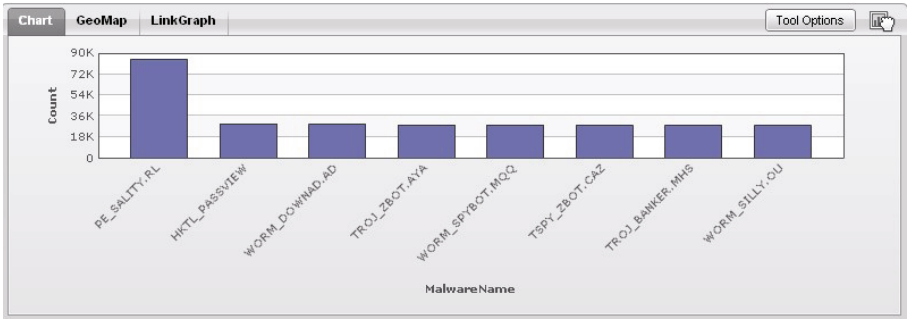


FIGURE 3-25 Bart Chart Example

- Pie

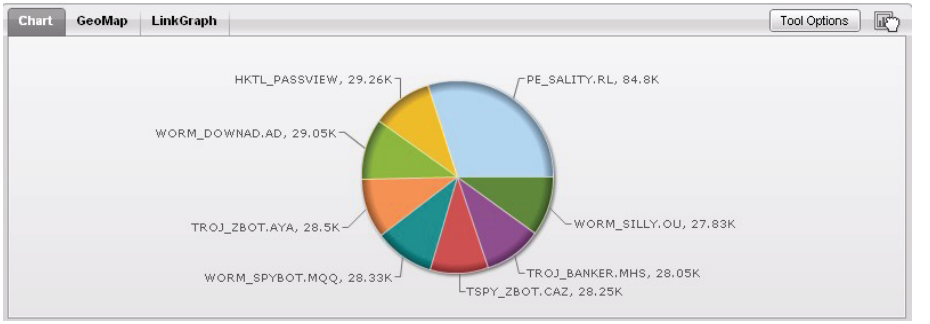


FIGURE 3-26 Pie Chart Example

- Line

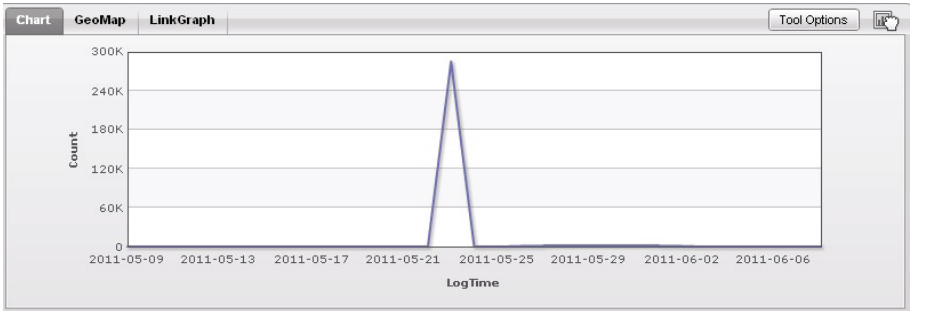


FIGURE 3-27 Line Chart Example

Table Tool Options

There are three columns available for you use in the Table option. The columns will show field names, log numbers, and the percentages of the total queried logs. Tables allow you to sort by FieldNames, Counts, or Percentages when you click the column name.

The following are descriptions of the options you can set for the Table Chart shown in the following figure.

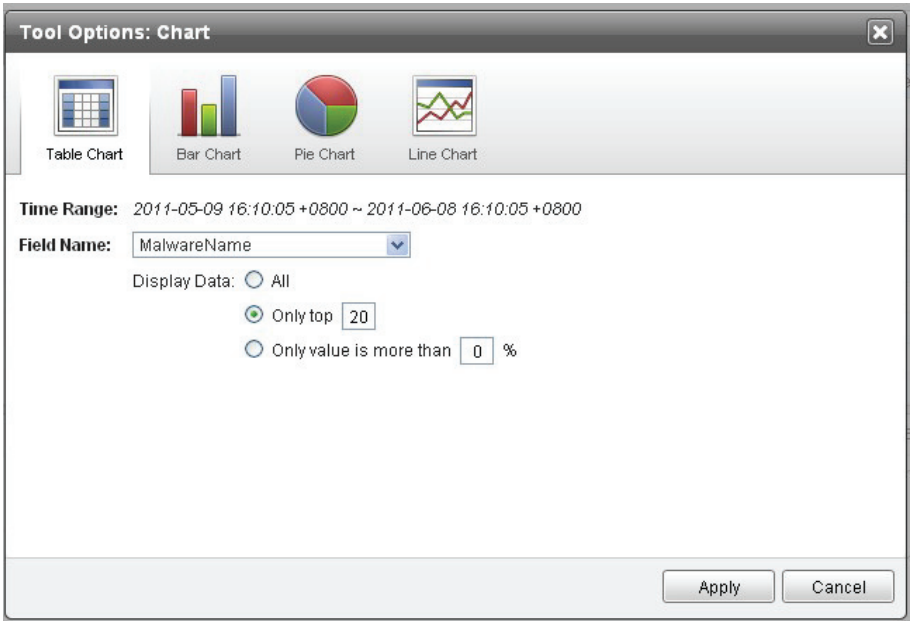


FIGURE 3-28 Tool Options: Table Chart

Time Range - Displays the date and time period you chose for the search range.

Field Name - When selecting the Table Chart option, label a Field Name row by selecting a heading from the Field Name drop-down to display predefined items that will render in the row of the event log (in the case of Figure 3-28, LogTime will be the heading.)

Note: When selecting a time field such as "LogTime" from the Field Name drop-down menu, the "Display Data" option will be hidden.

Display Data:

- **All** - Displays all queried data.
- **Only top N** - Only displays the top N values of the queried data.
- **Only values more than N%** - Displays the values where the percentage of queried data is over N%.

Note: Charts can only display a maximum of 200 values. Data beyond the 200th value cannot be displayed.

Bar Chart Options

The Bar chart provides the view to compare the height of each bar and identifies the most important event needing your attention. When using the Bar Chart display, by default, you can determine the name of the label for the chart's horizontal axis. The Y-axis uses an event count. Next, you can decide the data input of the X-axis. The item is predetermined by the fields of the event logs.

Choose **Switch Axis** to display the bars horizontally, or choose "Draw in 3D" to display the bars in 3D. These options are not available at the same time.

The following are descriptions of the options available to setup your Bar Chart as shown on the figure.

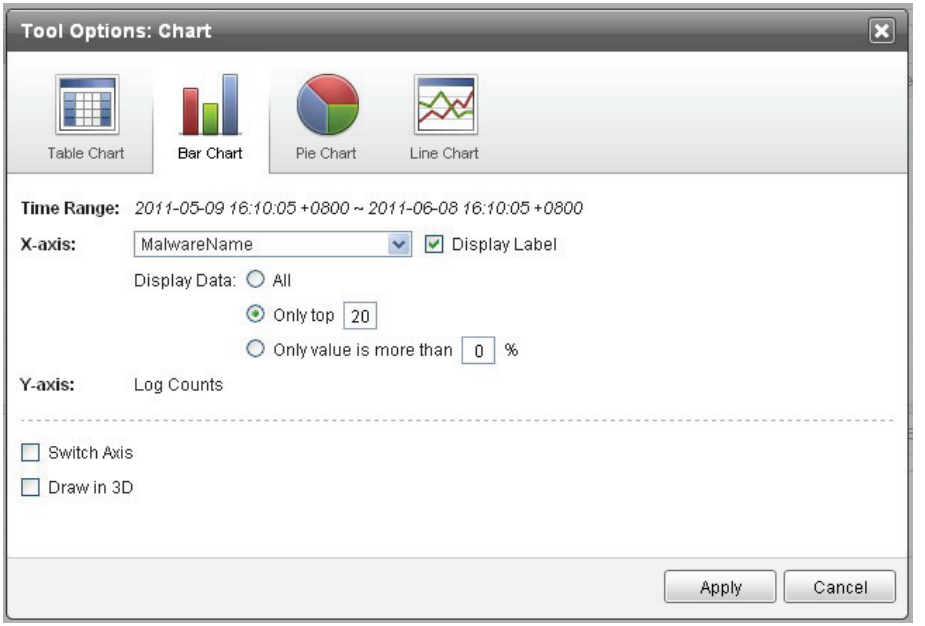


FIGURE 3-29 Tool Options: Bar Chart

Time Range - Displays the date or time period you chose for the report range.

X-axis - Label the name of the x-axis by selecting a heading from the Field Name drop-down to display predefined items that will render on the x-axis row of the event log.

Note: When selecting a time field such as "LogTime" from the X-axis drop-down menu, the "Display Data" options will be hidden.

Display Label - Select to show the display label on the X-axis of the bar chart rendering.

Display Data:

- **All** - Displays all queried data.
- **Only top N** - Only displays the top N values of the queried data.
- **Only values more than N%** - Displays the values where the percentage of queried data is over N%.

Y-axis - Fixed as the log counter when the Switch Axis option has been disabled.

Switch Axis - Switches the X and Y axis.

Draw in 3D - Select to render the bar chart in 3D.

Note: Charts can only display a maximum of 200 values. Data beyond the 200th value cannot be displayed.

Pie Chart Options

When using the Pie Chart display, you first determine the name of the pie chart and whether to show a data number or percentage on the chart. Next, determine how to render the data distribution. The pie chart's color is predetermined and cannot be changed. The pie chart can be displayed in 3D.

The following are descriptions of the options available to setup your Pie Chart as shown in the figure.

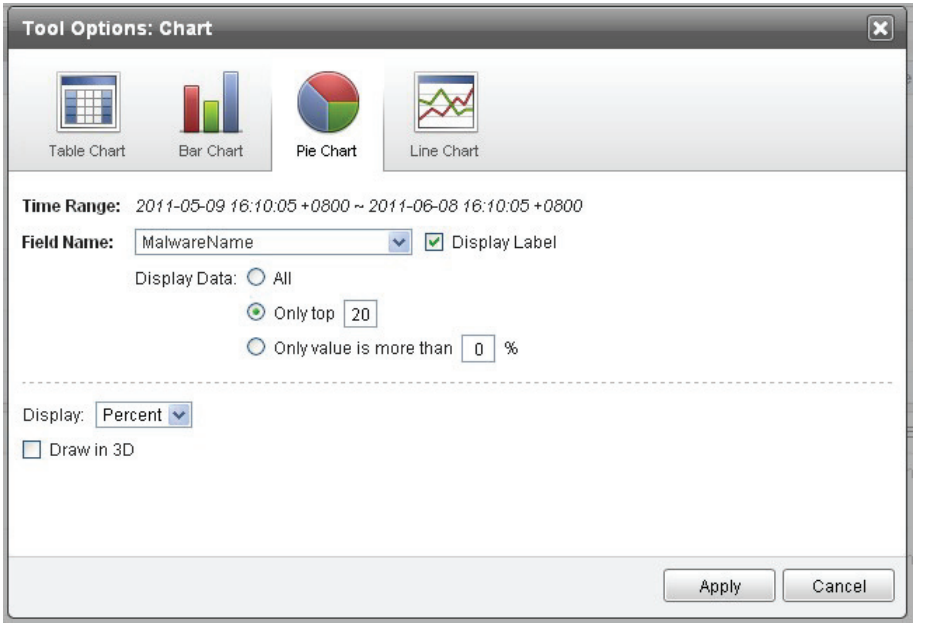


FIGURE 3-30 Tool Options: Pie Chart

Time Range - Displays the date or time period you chose for the report range.

Note: When selecting a time field such as "LogTime" from the Field Name drop-down menu, the "Display Data" option will be hidden.

Field Name - Label the Field Name by selecting a heading from the Field Name drop-down to display predefined items that will render on the Field Name row of the event log.

Display Label - Select to show the display label in the pie chart rendering.

Display Data:

- **All** - Displays all queried data.
- **Only top N** - Only displays the top N values of the queried data.
- **Only values more than N%** - Displays the values where the percentage of queried data is over N%.

Display - Select to render the pie slices in terms of percentages or a physical data count.

Draw in 3D - Select to render the pie chart in 3D.

Note: Charts can only display a maximum of 200 values. Data beyond the 200th value cannot be displayed.

Line Chart Options

The Line Chart tool is the initial display (default) of the Chart tool that plots your log counts over a time-line. When using the Line Chart, you can determine the name of the label for the chart's horizontal axis. The vertical axis always uses an actual event count for labeling. LogTime is a suggested field used to present log trends. You can decide the line area to be used.

The following are descriptions of the options available to setup your Line Chart as shown in the figure.

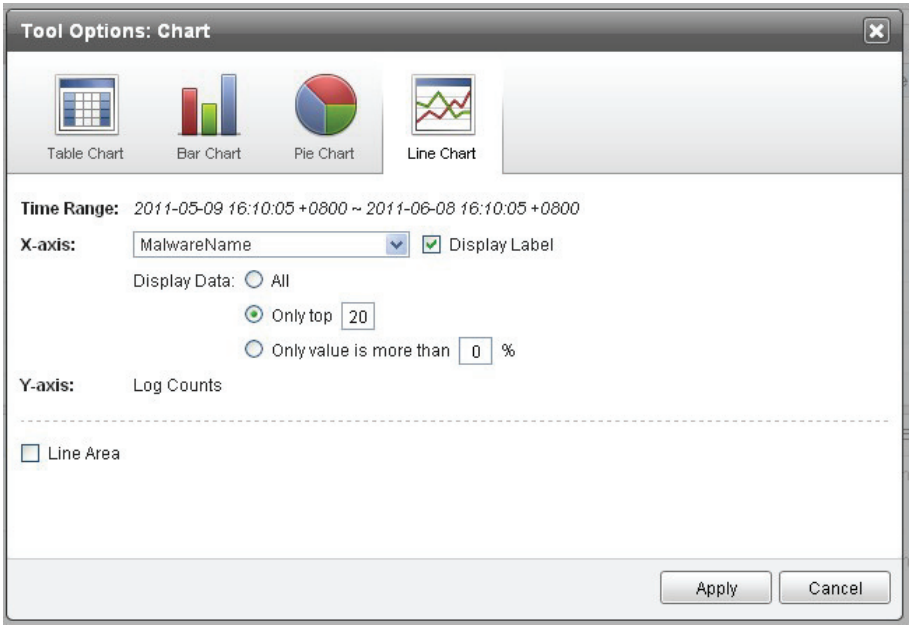


FIGURE 3-31 Tool Options: Line Chart

Time Range - Displays the date or time period you chose for the report range.

X-axis - Label the name of the x-axis by selecting a heading from the Field Name drop-down to display predefined items that will render on the x-axis row of the event log.

Note: When selecting a time field such as "LogTime" from the X-axis drop-down menu, the "Display Data" option will be hidden.

Display Label - Select to show the display label in the line chart rendering.

Display Data:

- **All** - Displays all queried data.
- **Only top N** - Only displays the top N values of the queried data.
- **Only values more than N%** - Displays the values where the percentage of queried data is over N%.

Y-axis - The vertical axis is always going to show an event count.

Line Area - Use the line area size to highlight the variation of a line.

Note: Charts can only display a maximum of 200 values. Data beyond the 200th value cannot be displayed.

Smart Interval and Smart Label

The Smart Interval and Smart label are the mechanism to automatically choose the proper time interval and display label. They are ONLY available for the LogTime as the

X-axis or FieldName. When choosing the LogTime as the X-axis or FieldName, all of the original options of Display Data will be hidden.

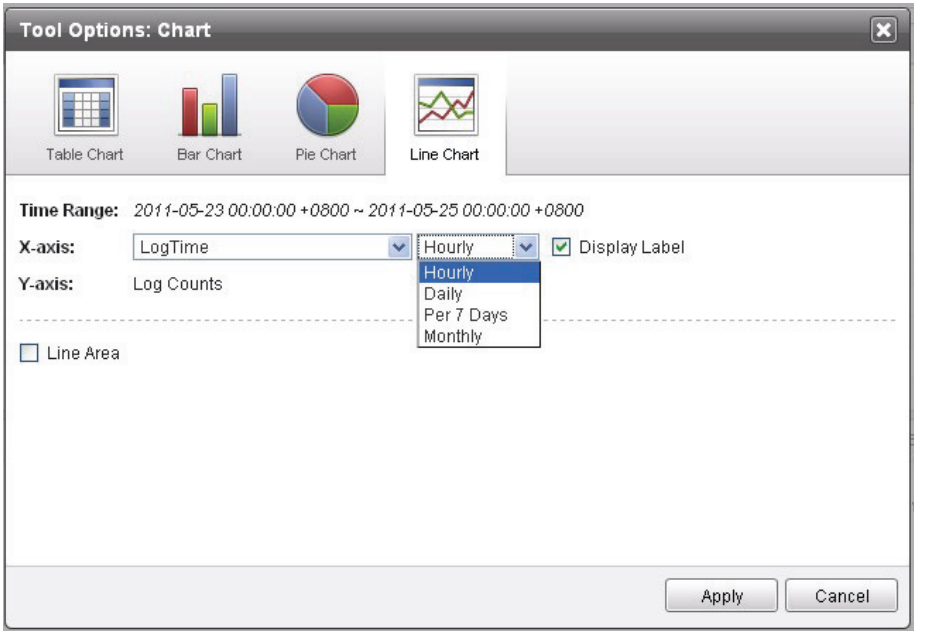


FIGURE 3-32 Tool Options: Line Chart with LogTime

Smart Interval

The Chart tool automatically chooses the proper time interval to display a chart according to your search Time Range. It also chooses the proper time interval options you can use. The available time interval options include Hourly, Daily, Per 7 Days, and Monthly. When the search time range is for the Last 30 days, the available time interval options will be Daily, Per 7 Days, and Monthly. The Hourly option is not available for the Last 30 days.

Smart Label

The Chart tool automatically chooses the proper time format and displays an interval at which to show the chart with LogTime.

GeoMap Tool

GeoMap provides a world map to display information based on queried logs. Before using GeoMap to display your data, you will need to enable Geo Information tagging. See GeoIP Tagging on page 5-19 for more detail.

GeoMap Options

When you use GeoMap (shown in Figure 3-33) to view information from varying events, you can change the following options.

FIGURE 3-33 GeoMap Events

Scale

The present information from the geographic scale view that appears includes:

- Log data
- Linear data

Select the option that best suits your requirements.

Display label

Select this option to add location labeling to your GeoMap rendering.

Category List

You can discover event counts through the following four categories:

- Source
- Destination
- Device
- Managing Device

Show by Different View

Show information based on one of the following:

- **Country** - Select to show a map rendering by country name. For example, China, United States, Japan, and so on.
- **City** - Select to show a map rendering by city name. For example, Beijing, Los Angeles, Tokyo, and so on.

The following table describes the meaning between the combination of categories and different views.

TABLE 3-3. Category Combinations

CATEGORY	VIEW	DESCRIPTION
Source	City	Displays by city the number of events from a Source IP.
	Country	Displays by country the number of events from a Source IP.
Destination	City	Displays by city the number of events from a Destination IP.
	Country	Displays by country the number of events from a Destination IP.
Device	City	Displays by city the number of events from a Device.
	Country	Displays by country the number of events from a Device.

TABLE 3-3. Category Combinations (Continued)

CATEGORY	VIEW	DESCRIPTION
Managing Device	City	Displays by city the number of events from a Managing Device.
	Country	Displays by country the number of events from a Managing Device.

Note: The map does not render all search results because the required associated geographical locations cannot be found in some queried logs. That means the number of results might be different between the chart and Smart Events/Log View panel.

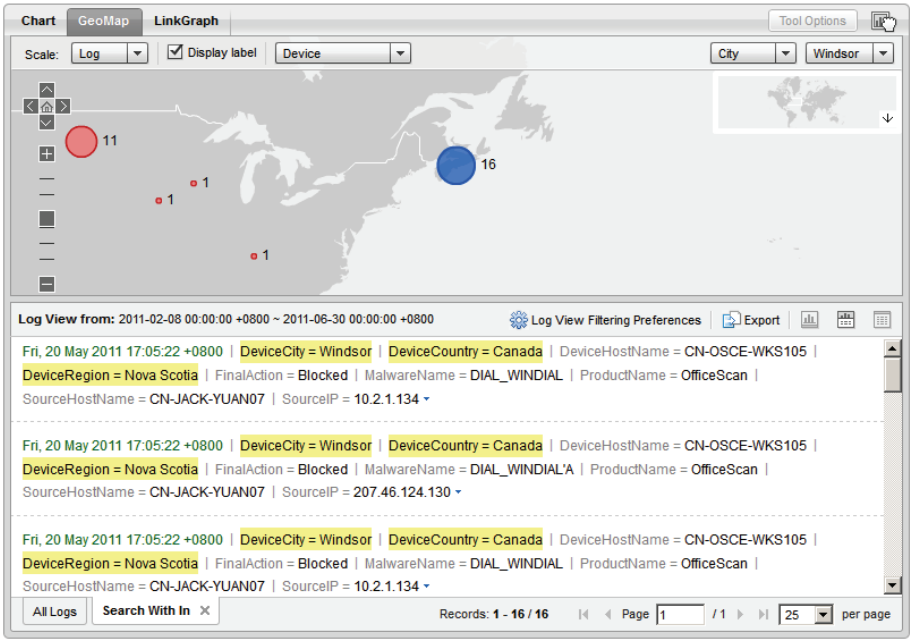
Location List

The items in the location drop-down represent events that have occurred in the cities or countries (depending on your previous selection) and have been pinned on the map. By selecting a city or country name from the list, Threat Intelligence Manager will do the following:

- Zoom-in on the selected city or country
- Highlight the pin of the selected city or country
- Execute the "Search Within" feature. "Search Within" displays the result of the selected city or country name on the tab.

You can also click a location on the map to achieve the same results. This example shows how GeoMap displays the distribution of a device to different cities in the world.

In the following example, the figure focuses on the city of Windsor, so the logs in the Search Within tab will narrow results to only the city of Windsor.



Context Menu

The Context Menu appears on the GeoMap rendering when you right-click on an event city or country (See Figure 3-34) and features the following:

New Search - Limits the search scope to the selected location.

Add as Keywords (AND) - Adds a new location to further narrow the search scope.

For example, if your original query string was to retrieve logs that included the `ProductName` filtered by TDA within the last seven days, and you then right-clicked to open the Context Menu on say "Tokyo," and then clicking **New Search** would retrieve the logs of the `SourceCity` (Tokyo) within the last seven days. Clicking **Add as**

Keywords (AND) retrieves the logs generated by `ProductName` filtered by TDA, and the `SourceCity` filtered by the Tokyo example within the last seven days.

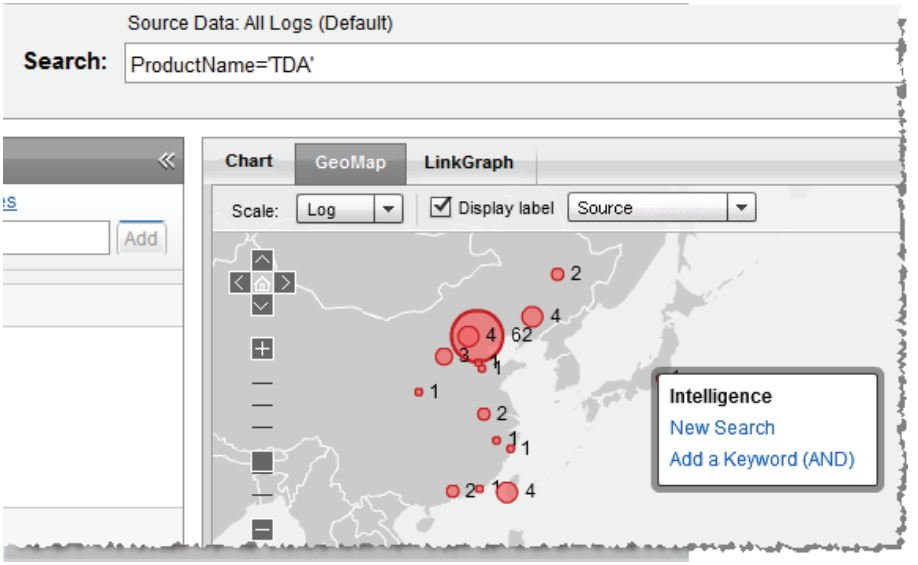


FIGURE 3-34 Context Menu

Operator

The Operator can also zoom-in, zoom-out, as well as save the investigation result to the Investigation Basket. You also can mouse-over the pin to see a detailed description in the Tool Tip.

Note: GeoMap has a limitation on the number of the pins it can utilize at any one time. This means that when the result contains more than 1000 cities or countries, the rendering time could be more than 30 seconds. The system returns a warning message asking you to narrow your search scope.

LinkGraph Tool

LinkGraph is designed to present the visual interactions between the source IP and a destination IP with the ports between them within the queried event logs. With regard to the search results, Threat Intelligence Manager creates a relationship between the SourceIPAddress, a Port Number, and the DestinationIPAddress and provides you a look into the topology of your threat-attacked network as shown in the following figure.

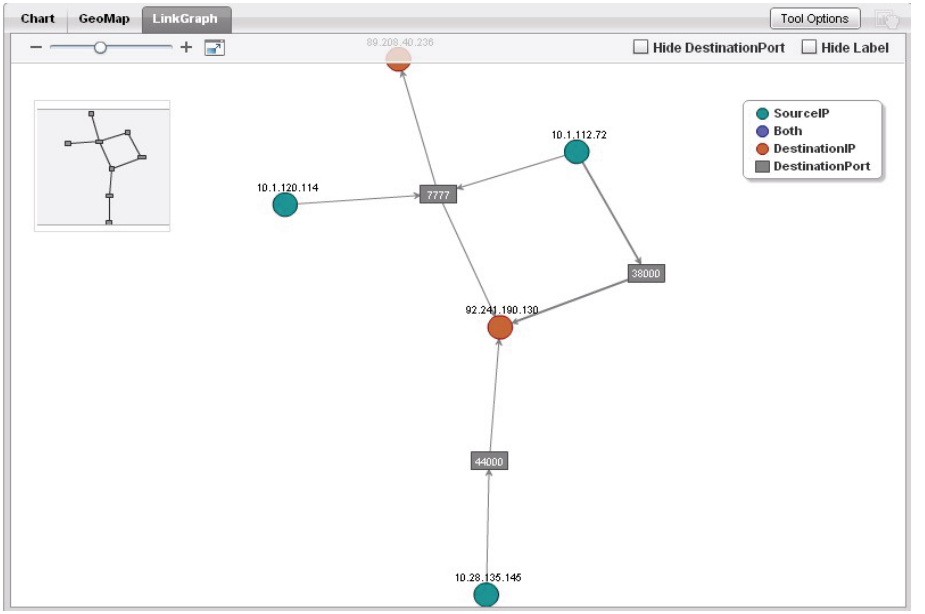


FIGURE 3-35 LinkGraph Example

LinkGraph features the following four primary functions:

- Display Panel
- Tool Options
  - Node Settings Configuration
- Tool Bar
  - Zoom In/Out
  - Hide Label or Port

- Context Menu
  - New Search
  - Add as Keywords (AND)
  - Add as Keywords (OR)
  - Interaction with Utilities (Whois)

LinkGraph Tool Options

When configuring the Tool Options, the SourceIP and DestinationIP are already fixed. You can, however, configure the Mediate port setting to use None, the SourcePort, or the DestinationPort.

Select Display Legend on the Tool Options screen if you would like a chart Legend to appear on the LinkGraph.

To access the LinkGraph Tool Options:

1. Click **Investigation > LinkGraph > Tool Options**.

   The Tool Options: LinkGraph window appears.

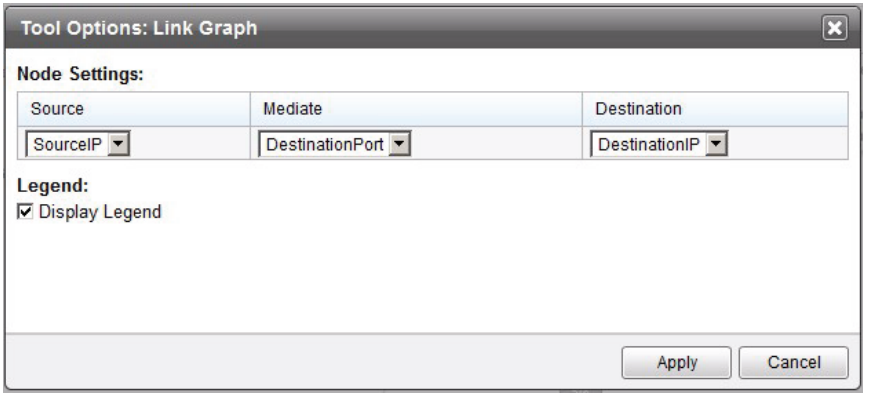


FIGURE 3-36 LinkGraph Tool Options Settings page

2. Assign the setting using the criteria defined in the paragraphs that follow.

Node Settings

Source

Fixed by the SourceIP address.

Mediate

Choose to perform mediation on the DestinationPort, the SourcePort, or None.

Destination

Fixed by the DestinationIP address.

Legend

Display Legend

Select **Display Legend** on the Tool Options screen if you would like a chart Legend.

Context Menu

From the Context Menus, you can select from the following options:

- New Search
- Add as Keywords (AND)
- Add as Keywords (OR)
- Whois (Only for the IP node)

New Search

Available for the IP, the Port node, or both. When using a "New Search" option on the IP node, the new search string will be (DestinationIP='xxx.xxx.xxx.xxx' OR SourceIP='xxx.xxx.xxx.xxx'). This search is for querying whether there are other logs that only include the DestinationIP or SourceIP data.

Add as Keywords (AND):

Available for the IP, the Port node, or both. When using the "Add as Keyword (AND)" option on the IP node, it will append the search string behind the original string with the OR operator. The new search string will be the Original string AND (DestinationIP='xxx.xxx.xxx.xxx' OR SourceIP='xxx.xxx.xxx.xxx'). This search is for querying whether there are other logs that only include the DestinationIP or SourceIP data.

Add as Keywords (OR):

Available for the IP, the Port node, or both. When using the "Add as Keywords (OR)" option on the IP node, it will append the search string behind the original string with the OR operator. The new search string will be the Original string OR (DestinationIP='xxx.xxx.xxx.xxx' OR SourceIP='xxx.xxx.xxx.xxx'). This search is for querying whether there are other logs that only include the DestinationIP or SourceIP data.

Whois:

Used only for the IP node. It interacts with the Whois utility.

Tool Bar

Zoom In/Out

Use the Zoom feature to zoom in and out using the slider bar as shown in the following figure.

You can zoom in or out with this tool bar or by using your mouse wheel. You can also drag a LinkGraph to change its position.

Hide Port / Label

Quickly hide a label or port using one of these two options.

When you check the box to hide a destination port, the LinkGraph will be rerendered.

Note: The Hide DestinationPort label will be reflected with a Mediate setting. If you configure the Mediate setting as None, the Hide DestinationPort option will not display.

Operations

When the tool cannot render all event logs in the graph, you will see a warning message to help reduce the investigation log scope. Use Smart Events or a Search string to help narrow down the log scope. You can also expand your search scope through a new

search of a selected node. When you click the graph nodes or a port, the related logs should also be highlighted as shown in the following figure.

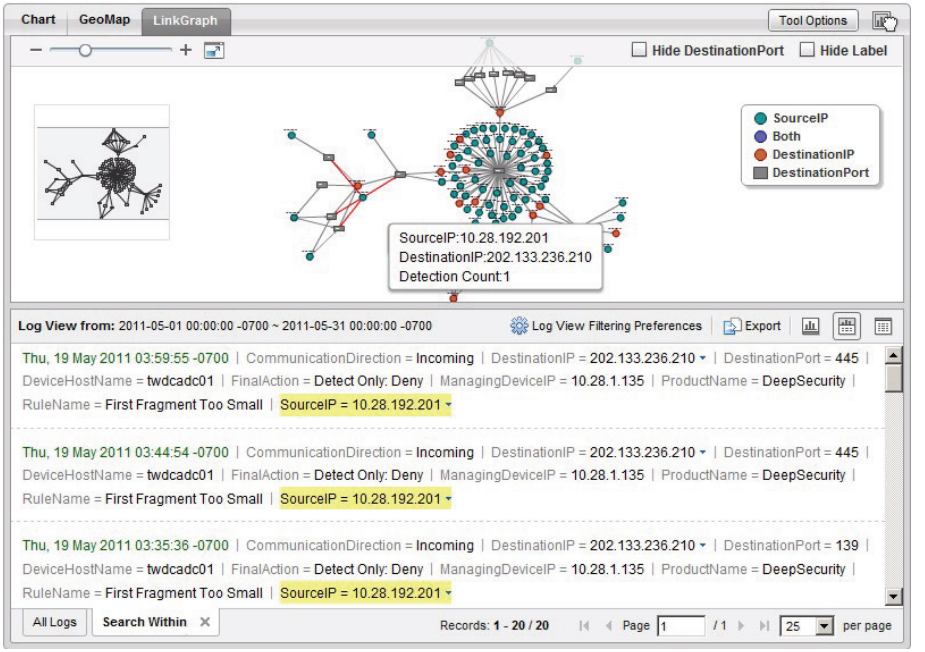


FIGURE 3-37 LinkGraph Search Within Highlighting

Additionally, you can zoom in or zoom out of the graph, or save the investigation results to your Investigation Basket. When you add a LinkGraph into the Investigation Basket, you could generate a report or save your results as a report template for the LinkGraph.

For details on how to save your search results into an Investigation Basket, see Investigation Baskets on page 3-27.

Chapter 4

Alerts and Reports

The features of the Trend Micro™ Threat Intelligence Manager Alerts and Reports tab are discussed in this chapter.

Topics include the following:

Alerts

Alerts are generated when a search query returns a certain number of results during a specific time period. Given the enormous amount of information flowing over the Intranet, you might like a simple way to learn when events of interest occur. Rather than periodically running reports or constantly monitoring events as they occur, you can be notified when a particular type of event occurs.

The Alert mechanism is designed to do just that. You can set the criteria to notify you when a particular type of event occurs, or access an alert results page where you can then go and analyze the set of events that triggered the alerts. The paragraphs that follow describe the details, rules, and management of these alerts.

Requirements for Creating Alerts

In order to generate alerting mechanisms you will need to configure the following:

- A search query
- A number of logs to generate as a ceiling (<=, <, =, >, >=)
- The log duration (days, hours, minutes.)
- The frequency of the checks (days, hours, minutes.)

Adding Alerts

Click the **New Alert** button located in the top right corner as shown in the following figure.

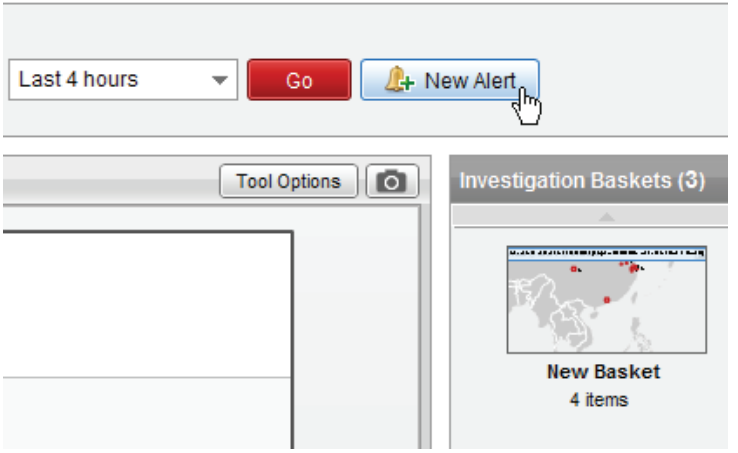


FIGURE 4-1 New Alert button

The Alert Rule Builder page appears.

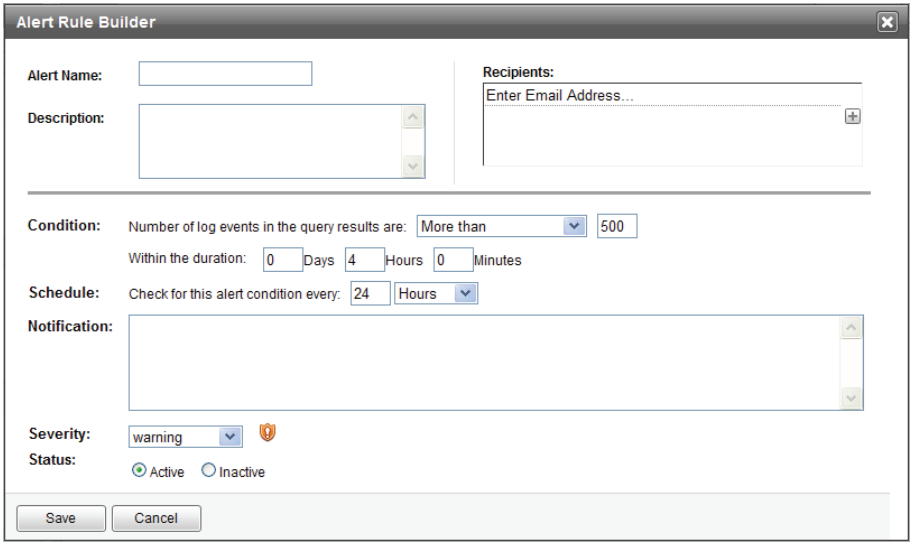


FIGURE 4-2 Alert Rule Builder page

To configure the Alert Rule Builder:

1. Enter a name you would like to call this particular alert rule. Something like "Recently Triggered Logs."
2. Enter a description to help identify the contents. You could enter something like "Triggered Logs for the Month of June, 2011."
3. Type a valid email address to which the alerts are sent.

> **Note:** Input only one email address. Do NOT enter multiple emails separated by commas. To send copies of this log to other individuals, enter the email addresses of your recipients, separated by commas.

4. For "Condition," select the number of log events you would like to require before triggering the alert.
5. Set the duration range for this log accumulation time to have transpired.
6. Schedule the frequency for alert checks in minutes, hours, or days.

7. Indicate the severity level that best describes the alert you are creating. The Severity level choices include informational, warning, or critical.
8. Mark the Alert Rule as active or inactive.
9. Click **Save** to preserve your settings.

   Your Alert Rule will appear under Alerts/Reports > Alerts > Alerting Rules as shown in the following figure.

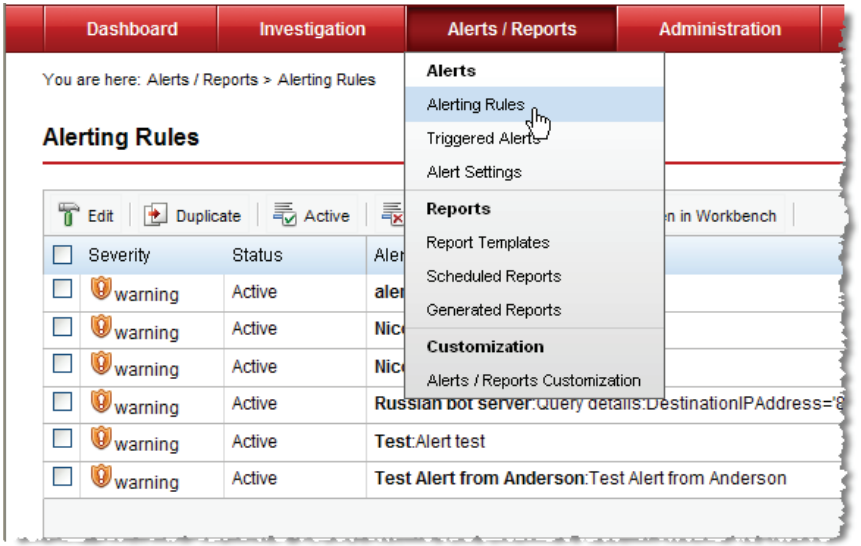


FIGURE 4-3 Accessing Alert Rules

Alerting Rules

From the **Alerts/Reports > Alerts** menu, select **Alerting Rules**. The Alerting Rules page appears.

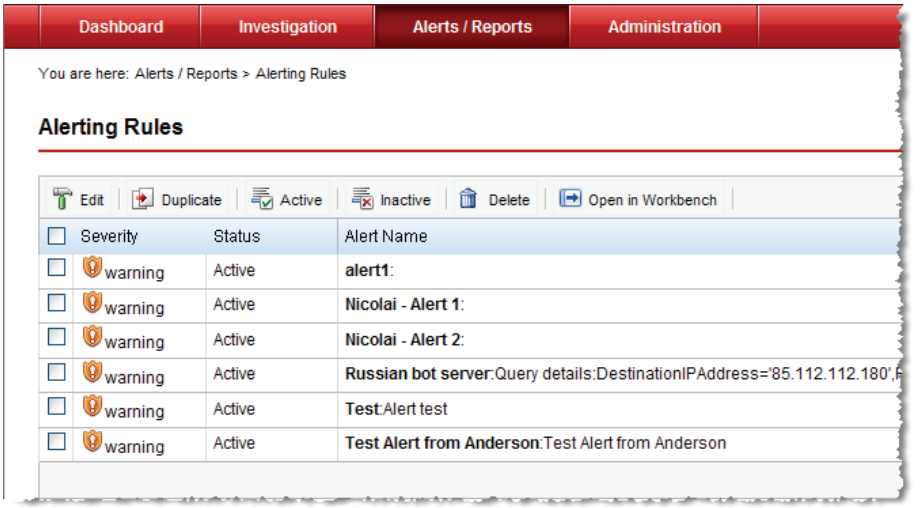


FIGURE 4-4 Alerting Rules page

- Alert Configuration Management
  - Create alerts from the Investigation page.
  - Modify or delete custom alerts.
  - Activate (schedule) an alert configuration and deactivate (unschedule) a scheduled alert.
  - Search for alert configurations based on the alert priority, alert category, and the alert title.
  - Alert configurations are global for all users.
- Alert Subscription
  - Triggered alerts are broadcast only to those users who subscribe to them.
- Alert Notification
  - Console on screen notification (on Status Bar, see 2.3.25)

    - Email notification
- Triggered Alert Management
    - See triggered alert details, including statistics and raw logs.
    - Investigate triggered alerts on the Investigation page.
    - Mark triggered alert status as:
        - Resolved
    - Attach a report or upload external attachments to the triggered alerts to use as evidence.
    - Send triggered alert detail and attachments to email recipients.
    - Search triggered alerts by case status, priority, category, and alert title.
    - Triggered alert management is global to all users.
- Alert Suppression and Aggregation
    - Multiple triggered alerts of the same rule should be consolidated into one.
        - If you have marked an alert as read, a newly arrived alert of the same type should update the case status from read to unread.
        - If you have marked the same alert (triggered earlier) as resolved, a newly arrived alert should change the case status to reoccurring.
    - Alert suppression configuration is global.

Triggered Alerts

From the **Alerts/Reports > Alerts** menu, select **Triggered Alerts**. The Triggered Alerts page appears.

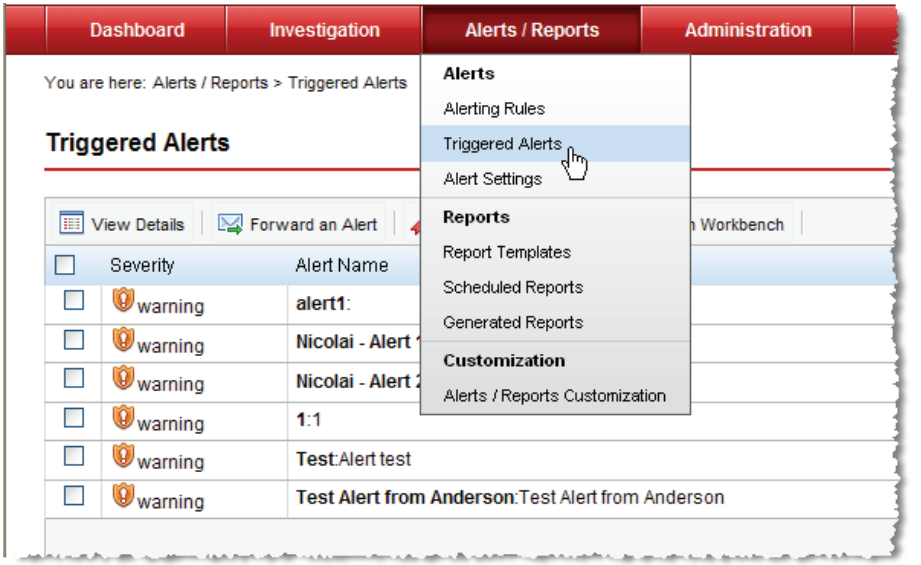


FIGURE 4-5 Triggered Alerts page

Triggered Alert Management

Through triggered alerts, you can see all the alert details, including informative statistics and raw logs. You can investigate and mark these triggered alerts on the Dashboard to increase alert awareness.

Mark triggered alert status as any one of the following:

- **Mark as Resolved** – The alert has been investigated and closed

You can add annotations to triggered alerts, attach a report, or upload external attachments to triggered alerts as evidence. You can also send triggered alert details and attachments to email recipients, or search triggered alerts by case status, priority, category, and the alert title. Triggered alert management is globally available to all users.

Alert Settings

All alert configurations are stored within the Threat Intelligence Manager database. The alert configuration specifies the alert settings that will be triggered and create the actual alert events.

Alert Event Information

The core information about the alert is stored within the platform database. All configured alerts are sent through the notification system based on the notification criteria configured when the alert was created.

Alert Configuration

The GUI and email alerts can be configured on the Threat Intelligence Manager GUI where you can set up the information that will appear in your alert. When evaluating the notification rules that you would like to apply to the alert, the rules should be arranged in order of the evaluation. The first match to an evaluation rule executes the notification based on its configuration, and the evaluation stops there.

Alert Notification

The supported severity levels are Informational, Warning, and Critical. Alert notification can be sent to subscribers through a variety of mechanisms, such as email. Alert notification is also available when you log in through a Web GUI, but you will only see the notifications sent to you that are marked unread. You can attach notes to the alert notification, and the notification mechanism automatically informs others that the alert has been updated.

To create alert notifications:

1. Go to **Alerts/Reports > Alert Settings**.
2. There are three severity levels from which you can choose the frequency of your alert notifications; Critical, Warning, and Informational.
3. Depending on your requirements, when one of your alerting rules has been critically breached, set the notification response cap to notify you per number of hours, days or weeks.
4. Make additional alerts for instances of Moderate alerts as well as any Informational only alerts you might want to see.

5. Save your settings to preserve your requirements.

Adding Attachments

You can add reports and other external files to your alerts.

To add an attachment to your triggered alerts:

1. From the **Alerts/Reports > Alerts** menu, select **Triggered Alerts**. The Triggered Alerts page appears.
2. Select an Alert Name and click **View Details**. The Triggered Alert Details page appears.
3. On the right side of the Triggered Alert Details page, you can see the Add Attachment option.
4. Click **Add**.

   The Add Attachments page appears.

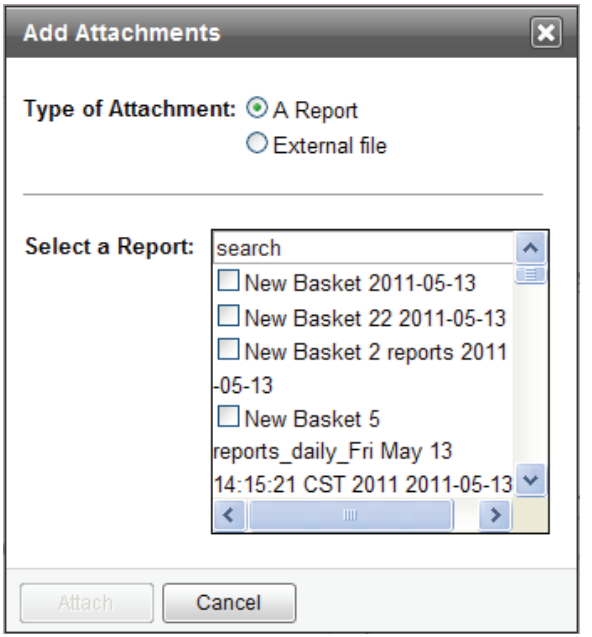


FIGURE 4-6 Add Attachments page

5. Select to add a report or an external file.
6. If you select to add a report, use the Search feature to locate a specific report name, or use the scroll button to scroll to the appropriate report.
7. If you select to add an external file, browse to the file's location and click **Attach**.
8. The attachment will appear in the Alert Details.

Reports

A graphical chart (such as a Line Chart, a Pie Chart, Bar Chart, Table Chart, GeoMap or a LinkGraph along with four types of visualization types) representing the data in one report. The graphical layout was inherited from the Investigation page. An optional log data table containing query results matching the query criteria. You can configure company logs, company names, fonts, and font sizes that are universal to all generated reports.

The following figure is representation of the six types of visualization from which you can view data.

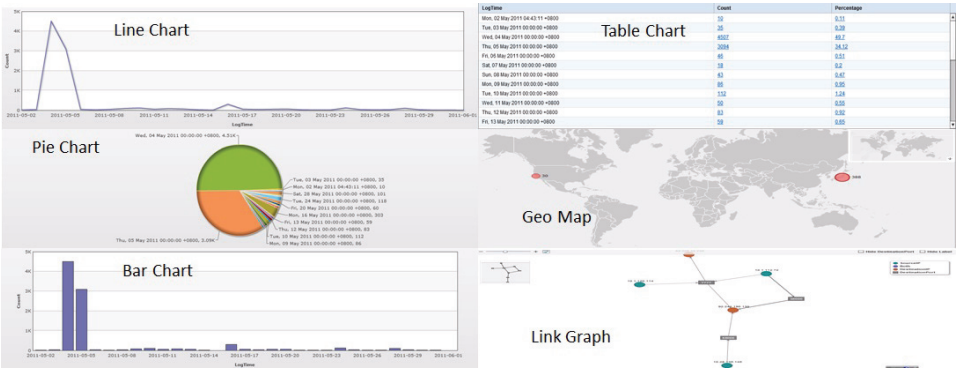


FIGURE 4-7 Six Visualization Types

A Threat Intelligence Manager Report can contain:

- A graphical chart that represents the data found in the report. The graphical layout was inherited from the Investigation page.
- An optional log data table that contains query results that match your query criteria.

- Company logs, header, and footer logos, and some annotations for each visualization type.

Report Templates

You can retrieve a list of report templates from the Investigation Basket on the Investigation page as shown in the following figure.

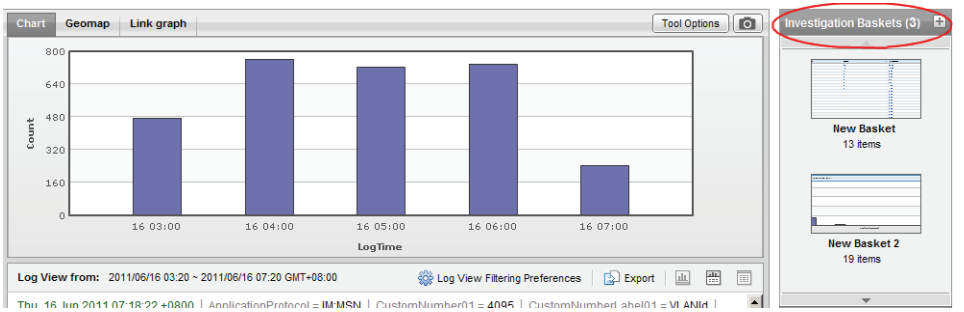


FIGURE 4-8 List of report templates from the Investigation basket

After selecting a Report Basket, select the "Save as report template" option from the Actions drop-down list for that report basket or one of the report items under this report basket.

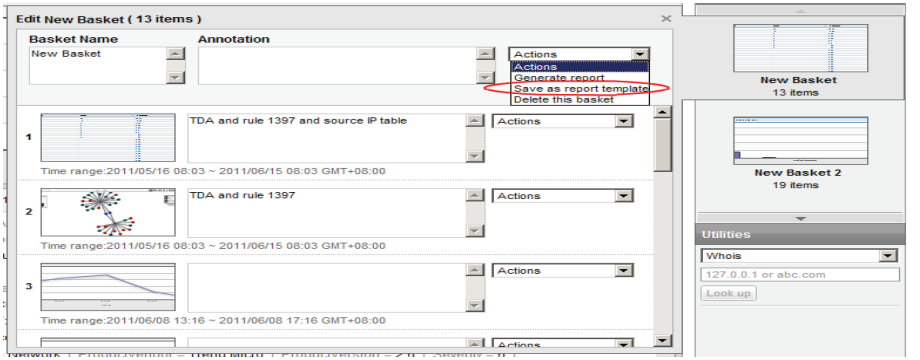


FIGURE 4-9 Generate a Report Template from a Report Basket

Threat Intelligence Manager will pop up the "Report Template Builder" dialog box to generate a report template as shown in the following figure.

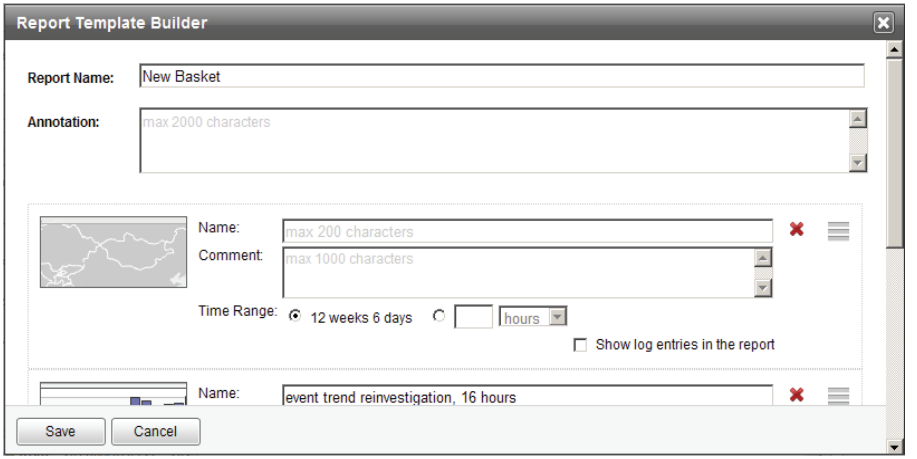


FIGURE 4-10 Report Template Builder

You will need to input some information such as the "Report Name" on the report template builder. The "Name" field is also mandatory. The others fields, including the "Annotation" and "Comment" fields are optional.

Use the Report Template Builder to create report templates based on saved queries and searches you created on the Investigation page. You can configure report names, report annotations, time ranges, and you have the option of including your query results. You can also consolidate multiple reports into one manageable report.

The Report Template Builder acquires its report basket data from the Investigation page by accessing the Investigation Basket. The Report Template or Group Reports pop-up displays, containing one or more report items. Edit the report template information in the template builder. Click **Save** to store the Report Template.

From the **Alerts/Reports > Reports** menu, select **Report Templates**. The Report Template page appears.

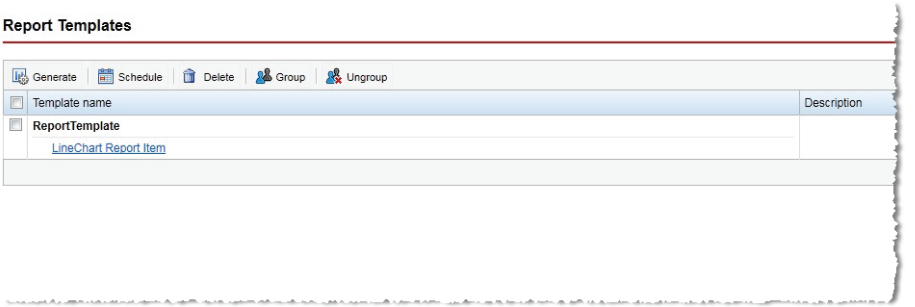


FIGURE 4-11 Report Templates

Complete any of the following actions:

- Choose one or more of the following check boxes to generate reports that meet your needs:
  - Click the **Delete** option to delete the selected report template(s).
  - Click the **Group** option to group selected templates into one report template group.
  - Click the **Ungroup** option to ungroup one report template group into more than one report template.
- For any single report template, select one of the following options from the Actions buttons:
  - All actions including "Generate" and "Schedule" can be configured under the Report Template page. Only one check box can checked at a time.
  - "Generate" allows you to generate one report from a report template. Threat Intelligence Manager provides three entry points including the Dashboard, Report Basket, and the Report Template page for generating a report. After you have generated your report from a report template, you can go to the "Generated Report" page to verify your results.
  - "Schedule" allows you to schedule one report from a report template. You can schedule one report for a Daily, Weekly and Monthly status. After generating one scheduled report, you can go to the "Scheduled Report" page to verify your results.

- If necessary, return to the Investigation page by clicking the report item as shown in Figure 4-12.

You can return to the Investigation page from a Report Template as shown in the following figure.

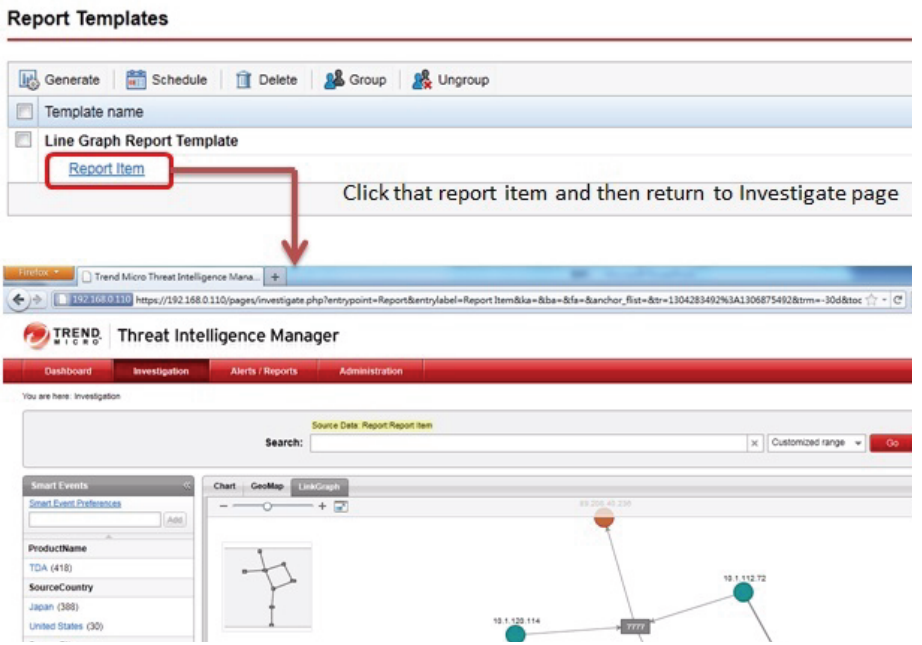


FIGURE 4-12 Returning to the Investigation Page from a Report Template

Scheduled Reports

There are two ways you can schedule a report. First, schedule your report from the Report Templates page found at **Alerts/Reports > Reports > Report Templates > Schedule** as shown in the following figure.

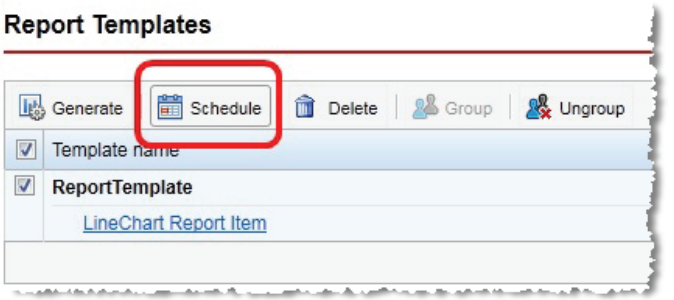


FIGURE 4-13 Scheduling Reports through Report Templates

Note: You must select one of the templates before you can schedule it.

Setup up daily, weekly, or monthly reporting to be done at a specific time for a Scheduled Report and Threat Intelligence Manager will base the generated final report on that time stamp and then send the results to the recipients you enter in the format (PDF, HTML or Excel spreadsheet) you choose. Click **Save** to preserve your settings.

Secondly, you can go to the Scheduled Reports page found at **Alerts/Reports > Reports > Scheduled Reports** and click **Add** at the top of the page as shown in the following figure.

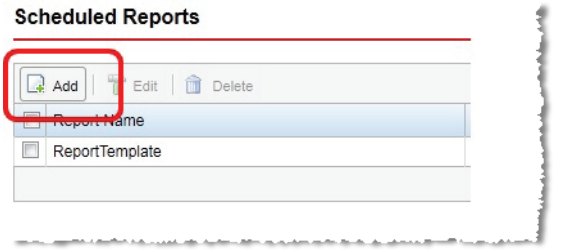


FIGURE 4-14 Scheduled Reports

Just as with Report Templates, you can schedule daily, weekly, or monthly reporting to be done at a specific time for a Scheduled Report and Threat Intelligence Manager will base the generated final report on that time stamp and then send the results to the recipients you enter in the format (PDF, HTML or Excel spreadsheet) you choose as shown in the following figure.

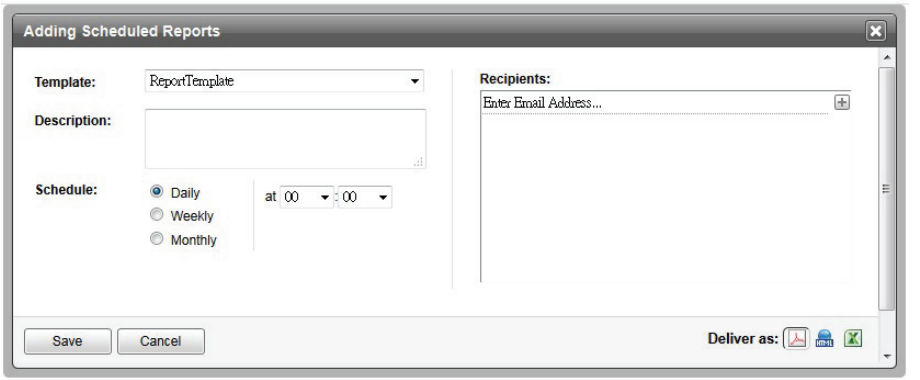


FIGURE 4-15 Adding Scheduled Reports

After making your selections, click **Save** to preserve your settings.

Next to the **Add** button, there are two other actions including **Edit** and **Delete**. You can change the scheduled time using **Edit** and **Delete** to remove a Scheduled Report.

Use Scheduled Reports to add a new report schedule from the Report Template. Edit and delete existing report schedules using the following settings:

- Schedule frequency – daily, weekly, monthly, at hh:mm
- Report annotation
- Email recipients
- Report formats

Search report schedules by either their title or description.

To add a scheduled report:

1. Go to **Alerts/Reports > Reports > Scheduled Reports**.

   The Scheduled Reports page appears.
2. Click **Add** and complete the page with the details to fit your requirements.

3. Click **Save**.

To delete a scheduled report:

1. Go to **Alerts/Reports > Reports > Scheduled Reports**.
   The Scheduled Reports page appears.
2. Select the check box for one or more scheduled reports:
3. Click **Delete** to delete the selected scheduled report.

Generated Reports

The Generated Reports page allows administrators to use previously generated reports.

About Generating Reports

Generate a report from the Actions in the Investigation Baskets of the Investigation page, Report Templates, or Dashboard. Before generating a report, the system pops up the "Report Builder" window for setting up additional information including the "Report Name" on that report as shown in the following figure.

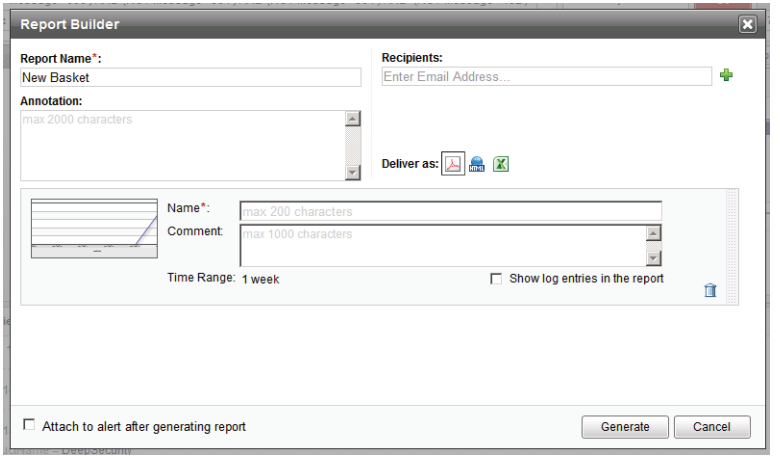


FIGURE 4-16 Report Builder

Report Name and the names of each item are required input fields. The other fields, including the Annotation and Comment, are optional.

Select the **Generate Report** option from the Actions drop-down menu that follows the Report Builder usage case. Select the **Save Report as a Template** option that follows the Report Template or Group Builder usage case.

Using Generated Reports

Under the Generated Reports page, you can accomplish the following three actions:

- **Attach to an Alert** - Attach a specified generated report to an alert after clicking this button.
- **Send Report** - Deliver a generated report using this button. Before sending a report, you should first setup your SMTP information under System Settings on page 5-34.

  Note: Reports are available approximately five minutes after clicking **Send Report**.

- **Delete** - Delete one generated report by clicking **Delete**.

To attach an alert, send a report, or delete a report:

1. Go to **Alerts/Reports > Reports > Generated Reports**.

   The following page appears.

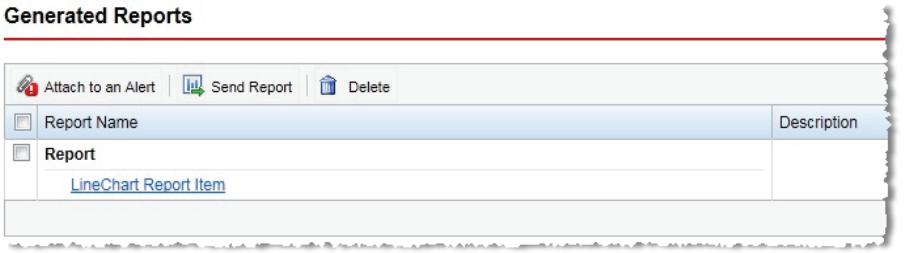


FIGURE 4-17 Generated Reports

2. Select a generated Report Name and choose to either attach it to an alert, send it as a report, or delete it.

3. Click any report item to return to the Investigation page as shown in the following figure.

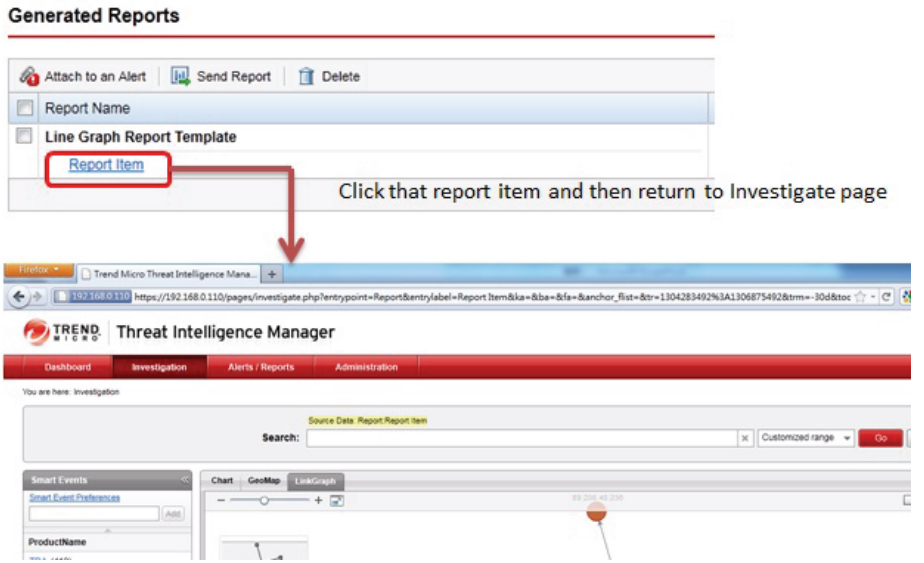


FIGURE 4-18 Returning to the Investigation page from Generated Reports

Alerts and Reports Customization

You can setup your "header" logo, "footer" logo, Company Name, Footer Name, and Font size / type / color on this page for your final report.

1. From the **Alerts/Reports > Reports** menu, select **Customization > Alerts and Report Customization**.

The Alerts / Reports Customization page appears.

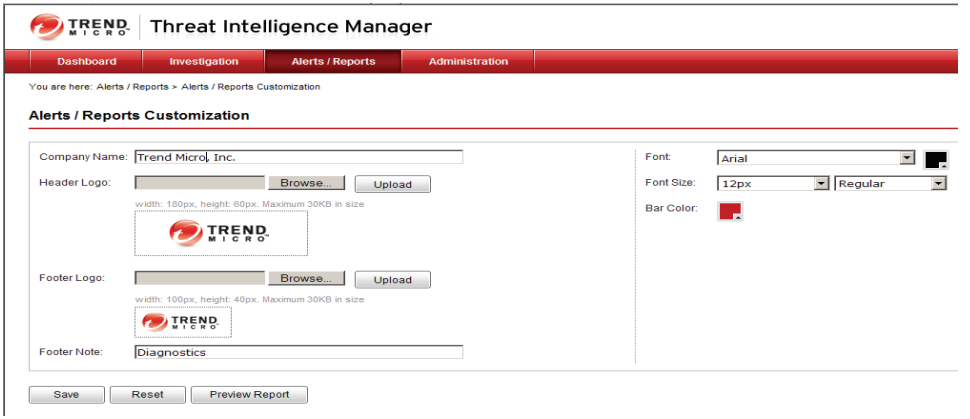


FIGURE 4-19 Alerts/Reports Customization

2. Edit the report settings to your required configuration.
3. Browse to the path of your company logo image.
4. Click **Upload** to initiate the Upload Company Logo feature.
5. Click **Save** to initiate the **Save Report Settings**.

With Threat Intelligence Manager, you will configure your own company logs, company names, fonts, and the font sizes that are universal to all your generated reports.

Chapter 5

Administration

The features of the Trend Micro™ Threat Intelligence Manager Administration tab are discussed in this chapter.

Topics include the following:

Log Collection

Through Log Collection, you can manage both your logging sources, and the settings that apply to those sources. The sections that follow explain the details on how to accomplish both.

Log Sources

With all your agents installed during the Installation and Deployment phase, you are prepared to begin identifying the sources of the logs you would like to collect. You can collect logs from agent-based clients, syslog clients, and Webservices depending on your requirements and server configuration.

Note: The Threat Intelligence Management server does not support using double type characters in host names. Instead, you should enter the IP values whenever necessary in the Management Console.

To view the Log Sources page or to begin identifying your available log collection resources:

1. Click **Administration > Log Collection > Log Sources**.

   The Log Sources page appears.

2. Choose to collect log information from Agent Based sources, Syslog sources, or a Webservices source.

3. Continue by following the information discussed in the appropriate sections that follow.

Agent Based

This section explains how to collect log data through agent-based sources. The various icons located in front of the Server Names indicate the various agent types. See the following table for the descriptions of each icon. See Figure 5-1 as an example.

TABLE 5-1. Server Name Icons

ICON	DESCRIPTION
	Icon indicates the concentrator is located on the Threat Intelligence Manager server.
	Icon indicates the source is an agent with concentrator functionality.
	Icon indicates the source is an agent installed with an OfficeScan server.

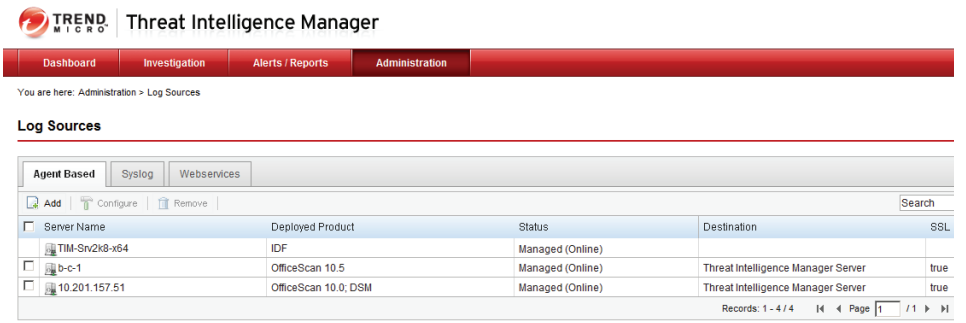


FIGURE 5-1 Agent Based Log Sources

Adding a New Agent

From the Log Sources screen:

1. Define your Agent-based clients by clicking **Add**. (See Figure 5-1.)
   The **Adding New Agent** window appears.

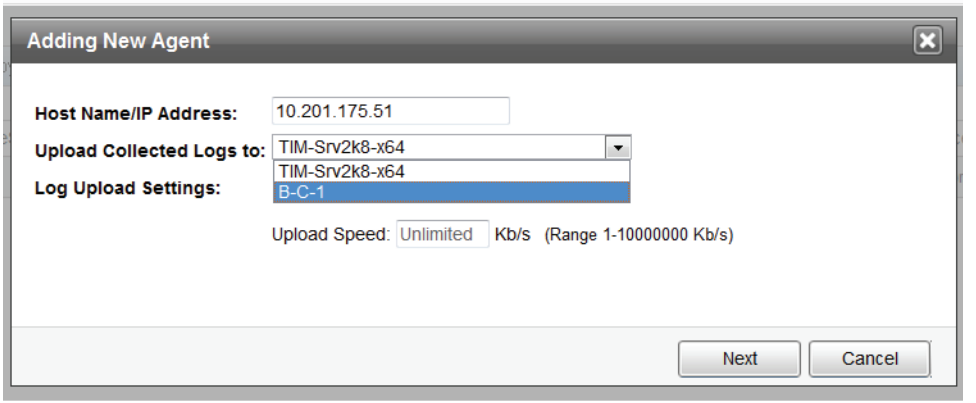


FIGURE 5-2 Adding New Agent Window

2. Enter the Host Name or IP Address of the agent client you would like to include. For example, enter a (hostname) or xxx.xxx.xxx.xxx (IP address).

Note: Do not use double-byte host names for the agent name. Use the IP address.

---

3. If an agent is also installed as a concentrator, after you have added that agent into the Agent Based list, it appears in the collector list for you to choose after you add the next agent.
4. You can set the maximum upload speed to restrict the bandwidth allowance for the uploading of files. The default upload speed is unlimited. You can also enable SSL protocol while uploading.

5. Click **Next**.

   Threat Intelligence Manager attempts to connect with the server you entered, and if successful, return the following message:

   > "Connection was successfully established with the server: 'xx.xxx.xx.xx.' The Agent has been activated and will send logs to this server."

6. Click **Close** to complete the connection.
7. The connected Server Name will appear as an available log source, and include the deployed product and version as well as the server's status. If there are deployed products on an agent, the log collection will be started by a scheduler.
8. Repeat these steps for all agent-based servers in your network to complete your log collection requirements.

Configuring an Agent

You need to configure or edit any of the agent-based server sources added to Log Sources. To use multiple agents, select all the agents necessary, then assign and deploy them using the same settings.

To configure or edit an existing agent:

1. Select the boxes of the servers you wish to edit, and then click **Configure** on the Agent Based action tab.

   The **Editing Agents** screen appears.
2. Change the name of the collector to which you want to upload logs.
3. Enable or disable the SSL protocol.
4. Change the maximum upload speed restriction.
5. Click **Next** to verify the connection.
6. Click **Close** to complete the connection.

Removing an Agent

Remove or delete any unnecessary agent-based server sources added to Log Sources by selecting the box of the server you wish to remove, and then clicking **Remove** on the Agent Based action tab. Logs will no longer be collected from the servers you remove.

If removing an agent fails because of the agent status: "Deactivation Failed," you can check the "Remove the agent even if deactivation fails" option and remove that agent again. The agent will be removed successfully.

Syslog

You can collect logs through from syslog clients by selecting either UDP or TCP protocol sources (depending on your configuration) and entering the client port number of 8514 (the default port). (See Figure 5-3.) Click **Save** to create the connection.

When collecting logs with Syslog, use a concentrator located in the same time zone as where the syslog sender to normalize the syslog log time with the correct UTC time.

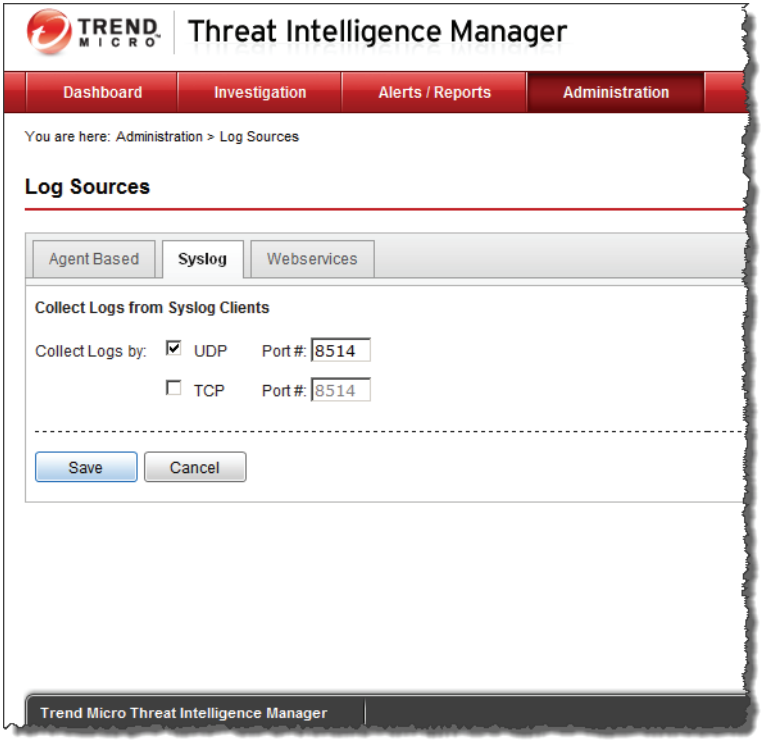


FIGURE 5-3 Syslog Log Source Settings

Search

You can also enter a **Keyword Search** to help narrow results when searching for a specific server IP or hostname.

Webservices

Use the Webservices tab to define the DSM and IDF servers.

Enabling Webservices on the IDF and DSM

Before adding the web service, you must enable web services first on the DSM and/or IDF server.

To enable the IDF webservice:

1. Open a command prompt window.
2. **cd** to the IDF Add-on installation folder at: `OfficeScan\Addon\Intrusion Defense Firewall`
3. Use the command line to enable IDF Web service.

```
idf_c -action changesetting -name configuration.webserviceAPIEnabled
-value true
```

> **Note:** APIE must be capitalized in the ".webserviceAPIEnabled" portion of the command.

4. Use the username and password under the registry key for the web service.
5. Do the following:
   a. Run: **regedit.**
   b. **HLM > SOFTWARE > TrendMicro > OfficeScan > Addon > IDF**
   c. Value of **IDFUSER** as username.
   d. Value of **IDFPASS** as password.

To enable the DSM webservice:

1. Go to the DSM web console at **System > System Settings > System > Web Service API**.
2. Check the **Enabled** radio button.
3. Click **Save**.

Adding a Webservice

To add a Webservice:

1. Define your Webservices clients by clicking **Add**.

   The **Adding New Webservice** window appears.
2. Enter the type of the agent you would like to include whether DSM 7.0 or IDF 1.2.
3. If you select DSM, enter the following URL in the URL window:

   `https://<hostname or IP address>:4119/webservice/Manager`

   Note: The default port is 4119. "Manager" must be capitalized. Administrators can configure the DSM port as needed.
4. Add the user name and password you use with your Deep Security Manager. The Deep Security role should be configured as a Web Service API user.
5. If you have a collector installed, you can select the location of the collector, and upload your collected logs to that location. The collector concentrator shows the products deployed with DSM.
6. Click **Save**.

7. The connected Webservice Name will appear as an available server source, and include the deployed product, version, and collector used as well as the Webservices status as shown in the following figure.

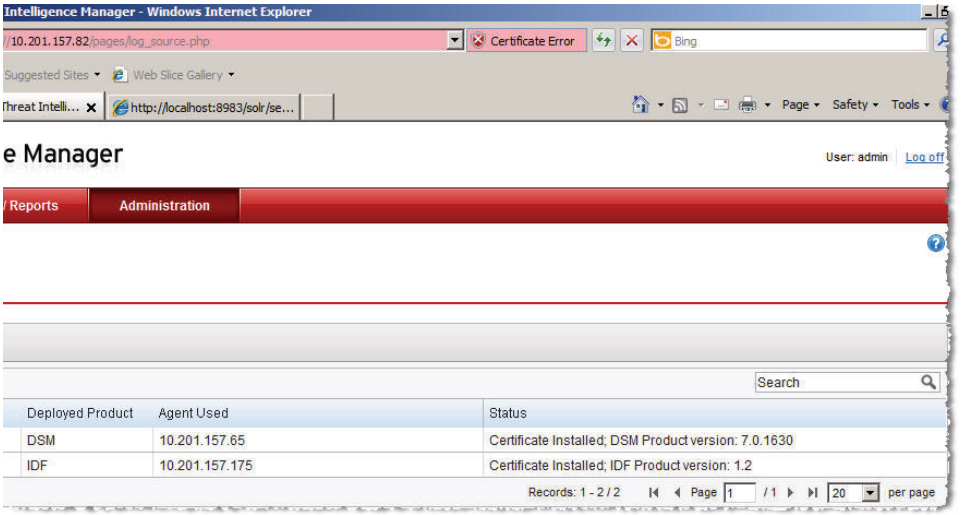


FIGURE 5-4 Successful Webservice Additions

8. Repeat these steps for all Webservice servers in your network to complete your log collection requirements.

To unlock the account of DSM and IDF:

If you are locked out of the DSM or IDF accounts because the login failed too many times, use the following commands to unlock the accounts.

1. To unlock the DSM account:
   a. Edit the locked out user from the DSM console.
   b. Uncheck the lock out option.
   c. Save.

2. To unlock the IDF account:
   a. Use the command prompt to open the IDF installation folder.
   b. Run the unlock command:

```
idf_c -action unlockout -username Administrator
```

Note: Log collection retrieves the latest DSM logs. For IDF, however, there is a one-hour delay. For example, if the time of log collection from IDF is 18:00, IDF only supplies the logs up to 17:00.

Search

You can also enter a **Keyword Search** to help narrow results when searching for a specific Web service host name or IP Address.

Log Settings

Through these settings, you can maintain, delete, or archive your outdated logs under the conditions you determine. In the Log Forwarding sections, you can also forward all logs to another Syslog server.

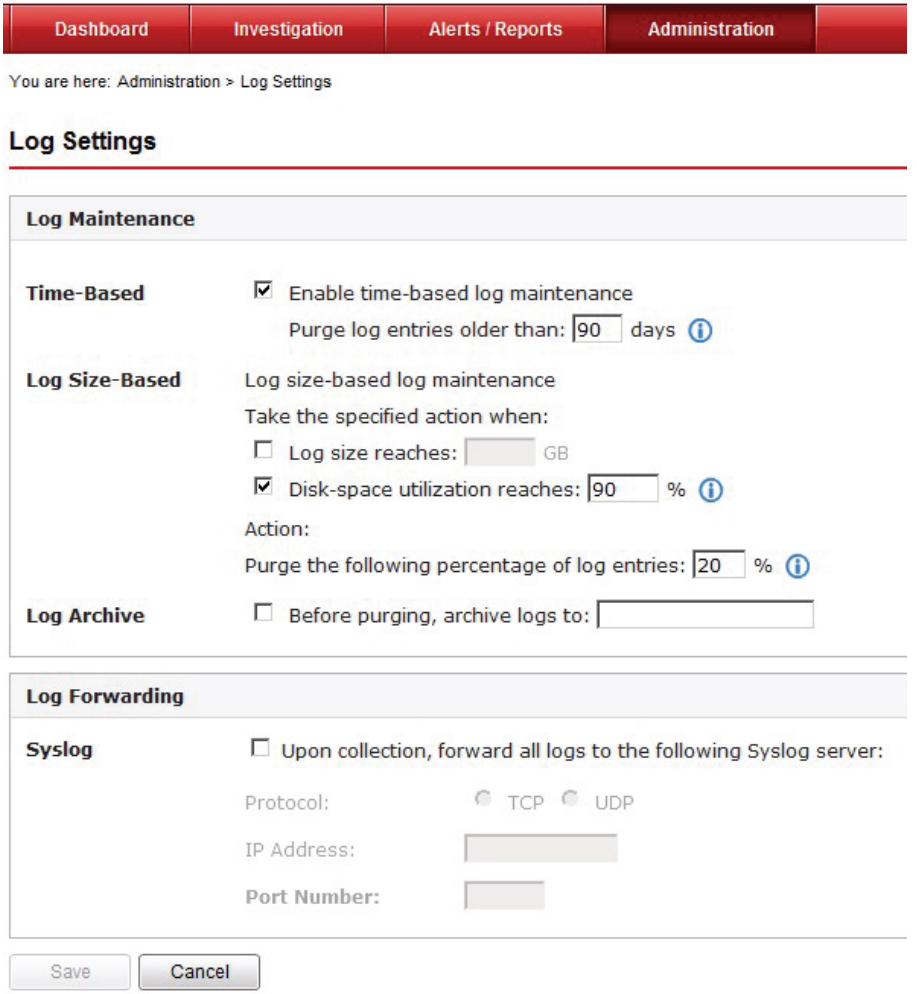


FIGURE 5-5 Log Settings Page

Note: Log Forwarding only forwards the logs generated after enabling the Log Forwarding setting. Historic logs will not be forwarded.

Log Maintenance

Maintain your log settings by adjusting the maintenance features as described in the paragraphs that follow.

Time-Based

By enabling the time-based log maintenance feature, you can set Threat Intelligence Manager to either purge or purge with archive outdated logs based on the number of days you determine. The default is 90 days to take the action as shown in the following figure. Click **Save** to preserve your settings.

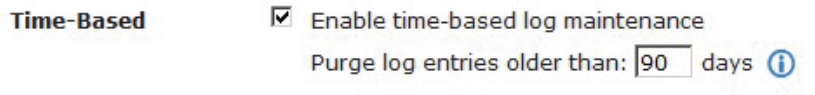
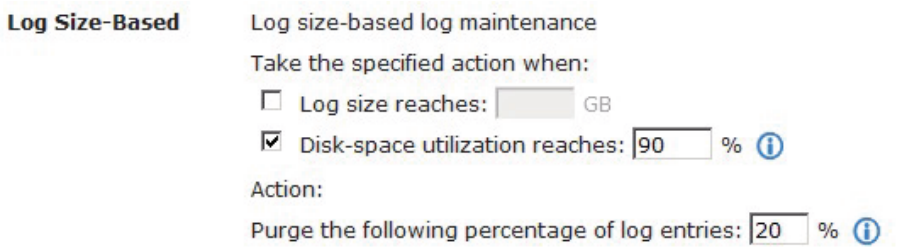


FIGURE 5-6 Enabling Time-based Log Maintenance in the Log Setting Page

Log Size-Based

By enabling the log size-based log maintenance feature, you can set Threat Intelligence Manager to either purge or archive outdated logs based on their file sizes or by the percentage of disk space in use. Enter a disk storage allowance maximum in Gigabytes so when the log size reaches a certain GB size, or an integer from 1 to 100 percent for when a log size reaches a certain percentage and Threat Intelligence Manager will

perform the action you have specified under "Action" after those conditions have been met as shown in the following figure. Click **Save** to maintain your settings.

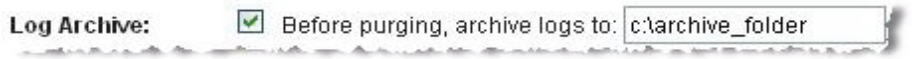


Action - Action allows you to set what percentage you would like to purge after reaching this Log Size-based condition.

Select an option to either purge or archive logs based on the conditions you have specified on the previous options. If you choose to purge your logs, whether based on time or file size, the outdated logs will deleted from the data center. If you opt to archive your logs, you will need to enter a file folder location. Click **Save** to maintain your settings.

Log Archive

The Log archive is to set archiving before purging and setting the archive destination as shown in the following figure.



Note: Make certain the archive folder actually exists before assigning this feature or the logs will not be archived before being purged.

Log maintenance is scheduled to execute at 00:00 every day.

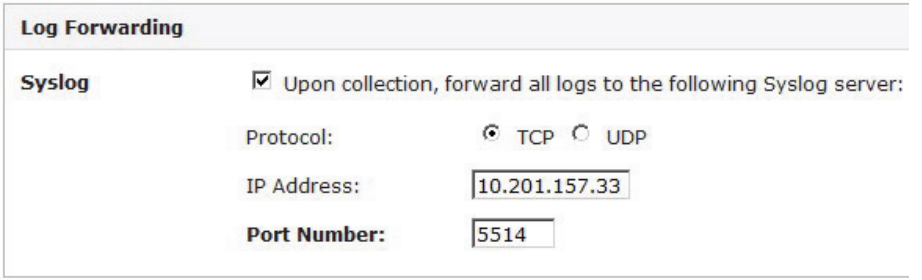
Log Forwarding

You can also forward and store your newly defined logs to another location (after they have been saved to the Threat Intelligence Manager server database), such as a Syslog server.

Syslog

Select the option to "Forward all logs upon collection to the following Syslog server" and enter the Syslog server's IP address and the appropriate port number of the Syslog server as shown in the following figure. (Contact your system administrator for these details if you are not certain.) Click **Save** to preserve your settings.

Note: Log Forwarding forwards the logs created after enabling this setting. Previous logs will not be forward.



Common Components

The Common Components of the Threat Intelligence Manager include Contact Management, Custom Tagging, Account Management, and System Settings. You can learn more about these components in the sections that follow.

Contact Management

Through Contact Management, you can develop and maintain a list of personnel contact information. You are essentially creating an Address Book to help you maintain a list of the people interested in the data your logs collect.

To access the Contact Management page:

1. Click **Administration > Common Components > Contact Management**.

   The Contact Management page appears.
2. Populate the page by completing the directions offered in the sections that follow.

Adding a New Contact

From the Content Management screen:

1. Define your contacts by clicking **Add Contact**.

   The **Add Contact** window appears.
2. Enter the individual's Name, Email Address, Phone number, and a description of their role that you might want to include and then click **Save**.
3. The contact you defined appears on the Contact Management page.
4. Repeat these steps for all necessary contacts in your network to complete your contacts database.

Editing a Contact

You can edit any of the contacts added to Contact Management by selecting the box of the contact you wish to edit, and then clicking **Edit** on the Contact Management action tab, and then adjusting the contact data as necessary. Click **Save** when complete.

Deleting a Contact

Remove any unnecessary contacts added to Contact Management by selecting the box of the contact you wish to remove, and then clicking **Delete** on the Contact Management action tab. Contacts removed will no longer be available in Contact Management.

Search

You can also enter **Search** criteria to help narrow results when searching for a specific contact, email address, phone number, or description.

Custom Tags

Custom Tags can be used in both Asset Tagging as well as Geo Tagging. The custom tag identifies individual event logs by tagging them with a customized name. All servers, agents, terminals, and laptops make up your system ASSETS. Each asset should be identified, defined, and tagged as such. Those tags are then customizable for use with Threat Intelligence Manager.

To define custom tags:

1. Access the Custom Tagging page in one of three places:
   - **Administration > Common Components > Custom Tags**
   - **Administration > Log Tagging > GeoIP Tagging > Custom Tags**
   - **Administration > Log Tagging > Asset Tagging > Custom Tags**
2. Do one of the following:
   - From the Custom Tags page, enter a descriptive tag name in the field provided and click **Add**.
   - From the GeoIP and Asset Tagging pages:
     - Click **Custom Tags.**
     - Enter a descriptive name in the Custom Tags dialog box.
     - Click **Add**. Then click **Close**.

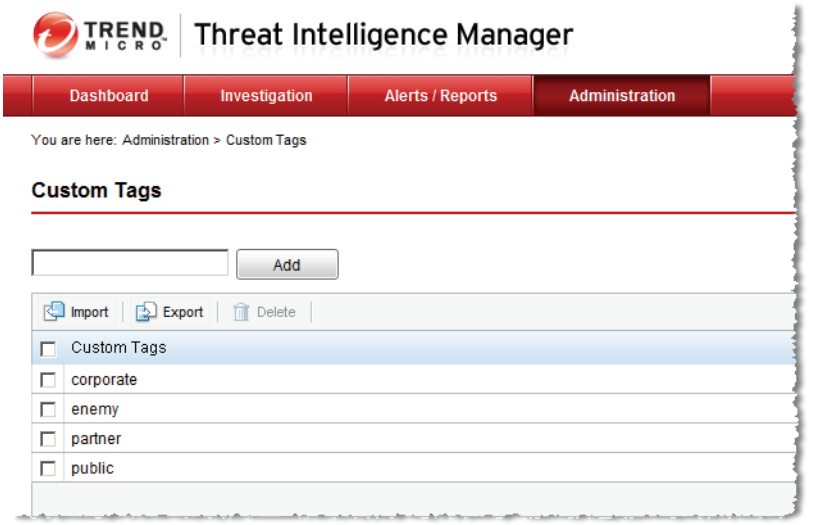


FIGURE 5-7 Custom Tags .CSV Files

To delete a Custom Tag:

1. Remove unused or unwanted custom tags by selecting the check box of the custom tag you want to remove.

2. Click **Delete** on the Custom Tags page.

To import Custom tags:

The Import feature allows a list of custom tags to be created externally with a .CSV file, and then imported into Threat Intelligence Manager. Any duplicate tags are ignored during the import process.

1. Go to **Administration > Log Tagging > Custom Tagging**.
2. Click **Import** from the Custom Tagging action tab to import a comma separated value (CSV) file that you want to add into asset tagging or geo tagging. (See how to access sample files in Figure 5-7 to create a custom tag .CSV file of your own.)
   a. To access a sample file, click **Import**, then click **here** from the Custom Tags Import window (see Figure 5-8) to get the sample file.
   b. Another way to create a sample file is to click **Export** from the Custom Tagging table.

Note: From the Custom Tags dialog box accessed when adding **GeoIP Tagging > Custom Tags** and **Asset Tagging > Custom Tags**, a here link (Figure 5-8)on the Custom Tags dialog box takes you to the Custom Tags dialog box shown in Figure 5-9.

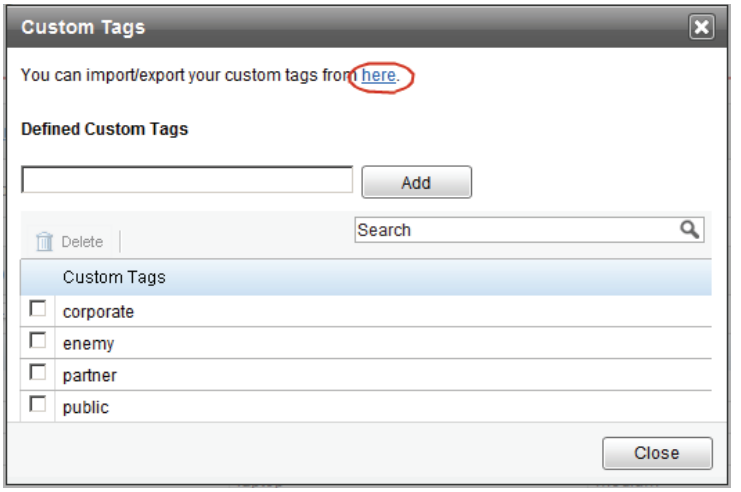


FIGURE 5-8 Importing Custom Tags

Select the here link to access the Custom Tags screen as shown in the following figure.

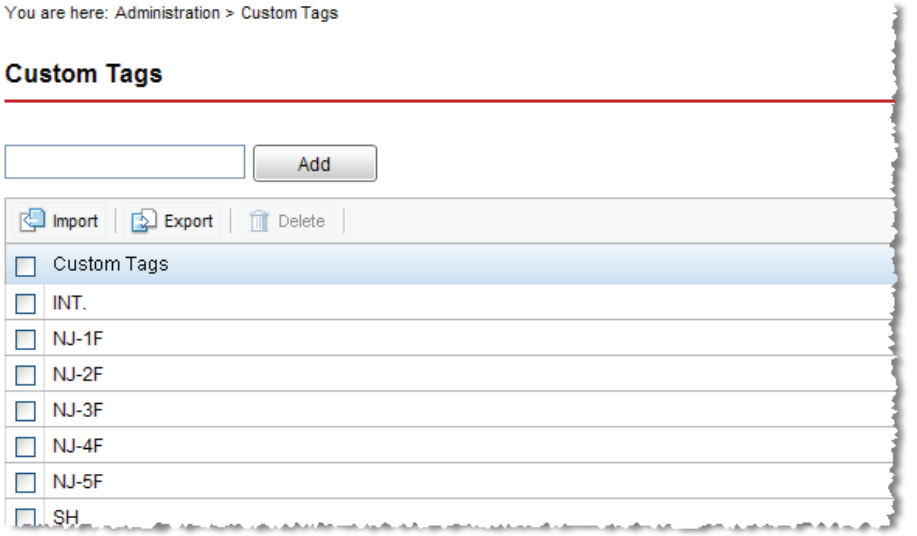


FIGURE 5-9 Custom Tags

3. From the **Custom Tags** screen, click **Import** and browse to the location of your custom tags where the .CSV file resides.
4. Complete the action by clicking **Import** on the Import: Custom Tags screen.
5. After importing the Custom Tags file, the new information replaces the original custom tags.

To export custom tags:

1. The Export feature creates a list of custom tags in the .CSV file format. You can backup your previously created custom tag files by clicking **Export** and saving the files to another location.

To delete a custom tag:

1. Select the custom tag you would like to delete from the Custom Tags list.
2. Click **Delete**.
3. The Remove Custom Tags dialog box appears with the name of the Custom Tag listed. You will need to confirm the deletion by clicking **Yes** or **No**.

4. If the tag is still in use, you will receive a warning error message indicating you will need to replace that tag with either a new one, or an existing tag from the remaining Custom Tags list.

Log Tagging

Log tagging helps to improve the reliability of the collected data. The tagging mechanism will search tags from the hostname table and then the IP table. If matching tags are found in the hostname table, the mechanism no longer searches the IP table. This searching process applies to both GeoIP and Asset tagging.

Threat Intelligence Manager allows the administrators to perform three forms of log tagging:

- Custom Tags on page 5-15
- GeoIP Tagging on page 5-19
- Asset Tagging on page 5-25

GeoIP Tagging

GeoIP Tagging provides corporate GeoIP mapping information so you can tag virtual location data in your collected logs. You can also optionally add physical location information to your event logs by using GeoIP Tagging. GeoIP Tagging is used to standardize the naming of locations from around the world for use and consumption while identifying your asset locations through City, Region, Country, and Custom tags.

Note: If you would like to import GeoIP locations using special alphabet or extended characters for locations such as Köln or München, your .CSV file must be UTF8-encoded.

Define

The Define: Custom Tags tab provides the following option to help you create Custom Tags.

Enabling GeoIP Tagging During Event Log Collection:

Enable GeoIP tagging by clicking "Add location to event logs during collection." This feature enables the auto-tagging of all event logs that have been collected by Threat Intelligence Manager. If you check the option without defining the Geo Tagging IP range or the host name tables, only the external IP addresses will be tagged with geographic information. That means only public IP addresses are tagged. Click **Save** to preserve your settings.

Host Name

The Host Name tab provides a list of host names with their corresponding City, Region, Country, and Custom Tags. Each host name can include a host name prefix or an actual host name. The host name prefix can be indicated with a wildcard "*." The wildcard indicates that any host name with a similar prefix could be considered a match.

For example, "tw-*" is created as a hostname. "tw-web1" is matched with the "tw-*" host name rule. "tw-web1" is tagged with the City "Taipei," Region "Taipei," Country "Taiwan," and Custom Tag "partner."

Note: The "*" wildcard is only allowed at the end of a host name. You cannot type a * in the front or middle of a host name.

Import - The Import feature automatically creates Custom Tags that do not exist within their respective Custom Tag tables. Import also verifies the validity of the City, Region and Country identities. The Country field is mandatory, but the City and Region are optional.

Create a CSV file that consists of a host name with corresponding City, Region, Country, and Custom Tags.

Note: Not all .CSV files can be imported. The " character, for example, is not supported and cannot be imported as a .CSV file. If you want to define the " character as a Custom Tag, you will need to use the Add function to add the " character into the list.

Export - Export the existing geotagging data to a CSV file in another location as a backup file.

IP/IP Range

The IP/IP Range tab provides a list of IPs or IP Ranges with their corresponding City, Region, Country and Custom tags. The IP/IP Range field can be an individual IP or an IP range such as 1.1.1.1 to 1.1.1.255.

Import - The Import feature automatically creates Custom Tags that do not exist within their respective Custom Tag tables. Import also verifies the validity of the City, Region, and Country identities. The Country field is mandatory, but the City and Region are optional.

Create a CSV file that consists of a host name with corresponding City, Region, Country, and Custom Tags.

Export - Export the existing geotagging data to a CSV file in another location as a backup file.

See the following links for additional standardized information on over 300,000 cities available for tagging:

- Worldwide: http://www.maxmind.com/GeoIPCity-534-Location.csv

Use the following files to reference the mapping of region codes to region names:

- World: http://www.maxmind.com/app/fips10_4
- US and Canada: http://www.maxmind.com/app/iso3166_2

Administrators can define the Geo Tagging IP/Hostname table two ways:

- Click **Add** and type in the geo information with auto-complete options.
- Import a CSV file. The import mechanism replaces all the original data in the table.

To add Host Name entries into the GeoIP table:

1. Click **GeoIP Tagging > Host Name > Add**. A window named **Add** displays.

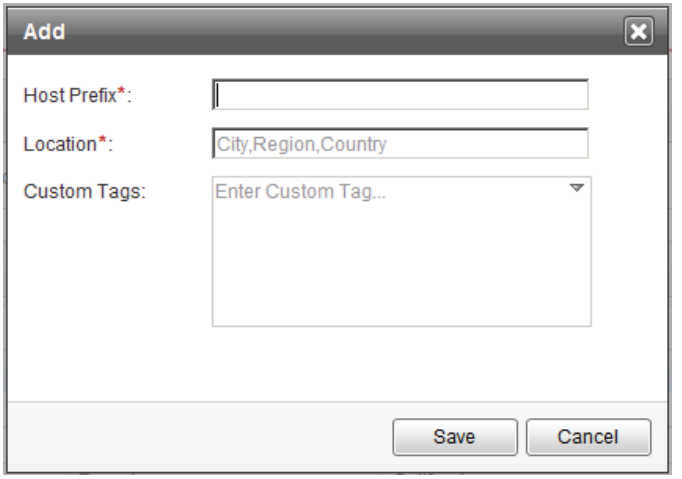


FIGURE 5-10 Add GeoIP Table Entries

2. Input the Host Prefix name and specify valid geo location information.
3. Enter any custom tagging information you would like.
4. Click **Save**. The first entry will be added to the background of the table.
5. The **Edit GeoIP Tagging** window remains open, without values, until you input the next IP address with geo information.
6. Repeat these steps for the IP/IP Range table.

To add IP/IP Range entries into the GeoIP table:

1. Click **GeoIP Tagging > IP/IP Range > Add**. A window named **Add** displays.

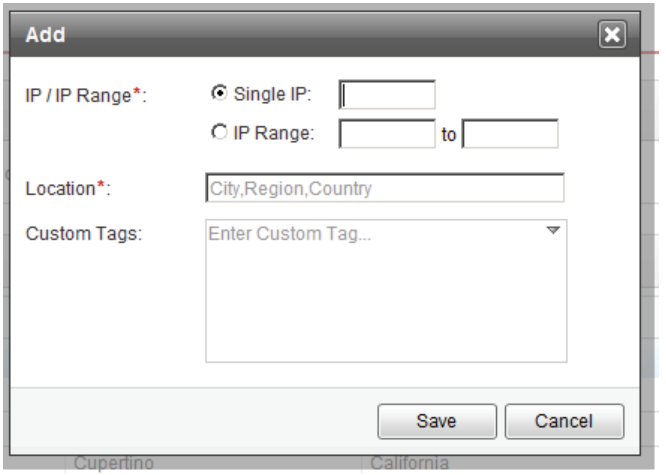


FIGURE 5-11 Add GeoIP Table Entries

2. Input a single IP address or an IP address range and specify valid geo location information. You can use the auto complete feature to help you choose geo locations.
3. Enter your customized tags.
4. Click **Save**. The first entry will be added to the background of the table.

   You could choose multiple custom tags in one entry. Duplicated host names or IP/IP Ranges will not be allowed in the list, but they can replace old files with the same host name or IP.IP Range files.
5. The **Edit GeoIP Tagging** window remains open, without values, until you input the next IP address with geo information.

To import valuable Geo Tagging CSV files:

1. Click **Import**. The **Import: Geo Tagging Information** screen appears.

Note: Use the import process to add geo information. You can import the customized corporate Geo information based on an IP address range or hostname. To get the sample file, click **Import** and download the sample file.

2. Enter the file name and path or Browse to the location of the .CSV file.
3. Select the file and click **Import**.
4. To import a file, the geo information must follow the correct format, which is:
   - **City**—Use the complete city name. Example: San Jose
   - **Region**—Use the complete region name. Example: California
   - **Country**—Use the country code. Example: US

corporate_geoip_sample.csv

```
1  beginIP,endIP,cityName,regionName,countryCode2,customTag
2  10.2.0.0,10.2.255.255,Cupertino,California,US,
3  10.0.0.0,10.0.255.255,Pasadena,California,US,Sales
4  10.1.0.0,10.1.255.255,Ottawa,Ontario,CA,Human Resource
5  192.168.1.0,192.168.1.255,Cupertino,California,US,
```

corporate_geoip_hostprefix_sample.csv

```
1  hostPrefix,cityName,regionName,country,customTag
2  us-cup*,Cupertino,California,US,
3  us-pas*,Pasadena,California,US,Research
4  ca-*,Ottawa,Ontario,CA,Human Resource
5  tw-*,Taipei,T'ai-pei,TW,
6  B-C-*,Cupertino,California,US,
7  BBB,Munich,Bayern,DE,Data Center
```

FIGURE 5-12 Sample Geo IP Address (top) and Geo Prefix (bottom) Files

Note: Not all countries have region information. For those regions, enter -„ in the column to mark the column as empty. GeoIP Tagging on page 5-19 describes how to obtain a valid list of region formation.

Search

You can also enter **Search** criteria to help narrow results when searching for a specific IP address range, Hostname, City, Region, Country, or Custom Tag.

Asset Tagging

Asset Tagging identifies your corporate assets to help you add asset-type and criticality information to your collected logs. As an additional option, you can add selected Asset-Tags to your event logs during collection that include an asset type, an asset criticality, or your asset tags.

Define

Depending on the asset criteria you would like to track, click the Asset Types, Asset Criticality, or the Custom Tags underlined titles. Depending on your requirements, you can import the CSV file tags of the assets that fit your requirements by clicking **Import** and browsing to a predefined CSV file. Click **Import** to complete the requirement. Click **Save** to preserve your work.

You can define the Asset Tagging IP address/hostname table one of two ways - Auto Complete or Drop-down:

- Click **Add** and type the asset information with auto-complete options.
- Import a CSV file. The import mechanism will replace all the original data in the table.

Asset Types

Asset Types identify and categorize each physical asset within your company. Define your particular assets such as corporate, server, laptop, and branch office types.

The defined Asset Types can either be created manually or imported through a CSV file that includes a list of your company asset types. View the sample CSV file format before creating your own CSV file by clicking the page link shown in the following figure:

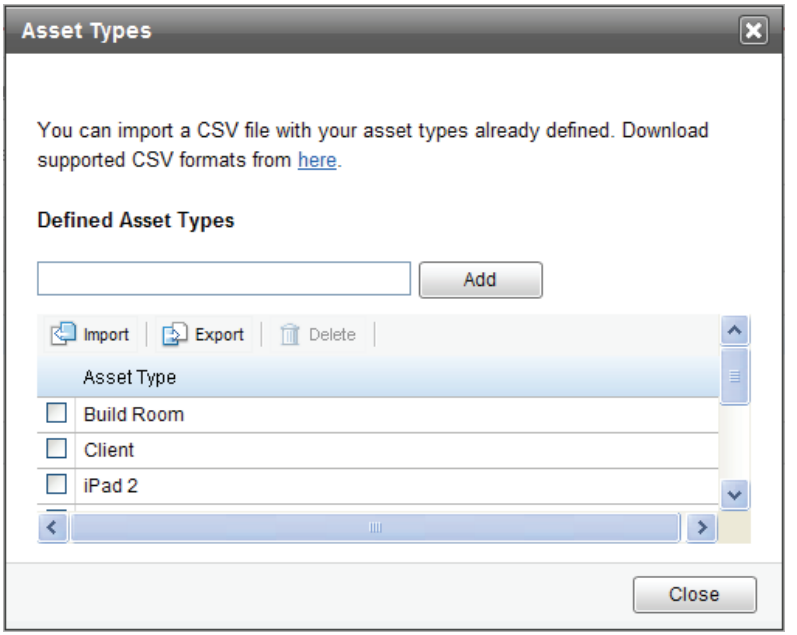


FIGURE 5-13 Asset Types with a CSV File

To add entries into an Asset table:

1. Click **Add**. A window **Edit Asset Tagging** displays.
2. Input the IP address or IP address range and other asset information.
3. Click **Save**. The first entry will be added into background of the table.
4. The "Edit Asset Tagging" remains open (without any value) to allow you to input the next IP address with asset information.
5. Repeat these steps for the Hostname table.

To import valuable Asset Tagging CSV files:

1. There are two CSV formats, under the IP/IP Range and Host Name tabs that you can use to import .CSV files. To import files through Host Name, choose **Host Name > Import**. The Import: Asset Tagging Information dialog box appears.

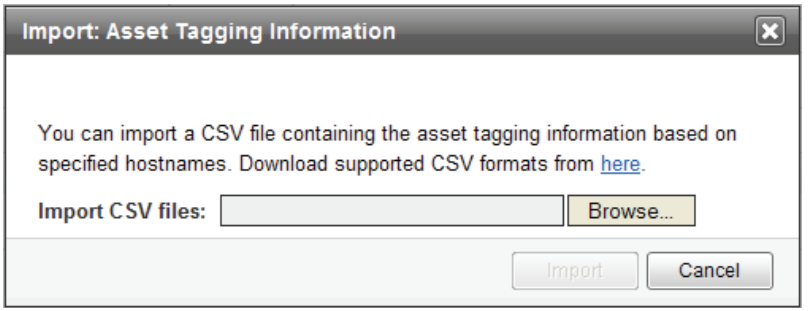


FIGURE 5-14 Import: Asset Tagging Information through Host Name

2. Browse to your .CSV file and select it.
3. Click **Import**.
4. Use the "here" link to obtain a sample file.

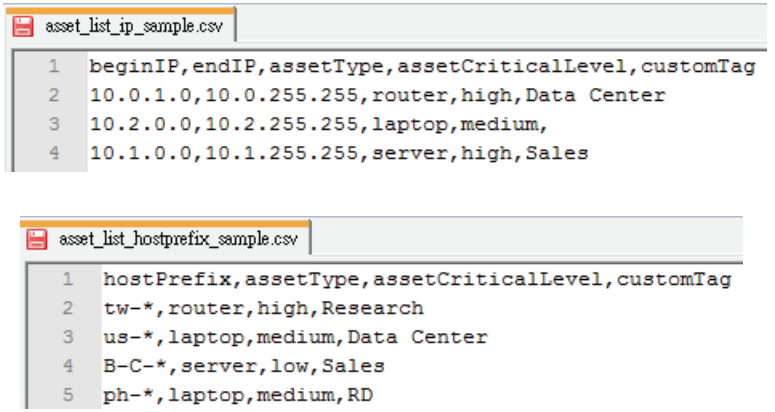


FIGURE 5-15 Sample Files for Asset IP Address (top) and Asset Prefix (bottom)

To add a Host Name:

1. Click **Host Name > Add**.

   The Add dialog box appears.

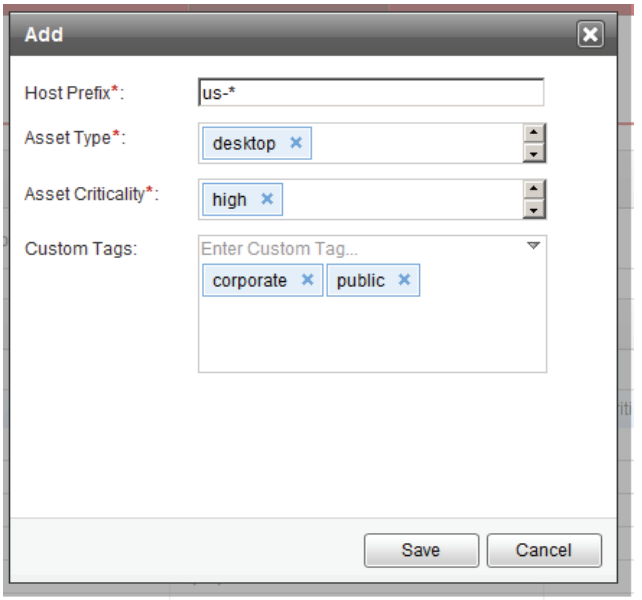


FIGURE 5-16 Add dialog box for a Host Name

2. Complete the fields similarly to those shown in Figure 5-16. You can choose multiple Custom Tags for one entry. Duplicated Host Names are not allowed.
3. Click **Save** to preserve your settings.

To import valuable Asset Tagging CSV files:

1. Under the IP/IP Range tab, you can also use **Import** to import .CSV files. To import files through IP/IP Range, choose **IP/IP Range > Import**. The Import: Asset Tagging Information dialog box appears.

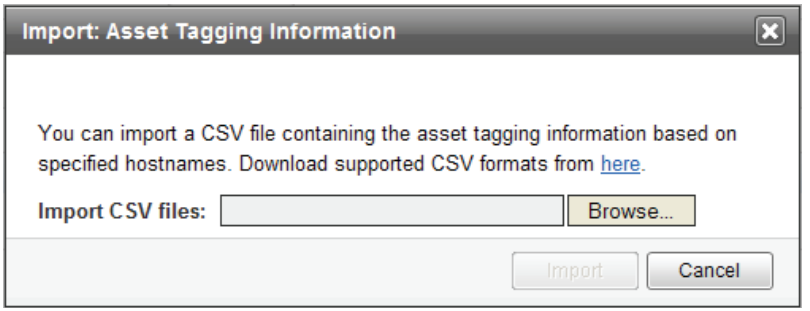


FIGURE 5-17 Import: Asset Tagging Information through Host Name

2. Browse to your .CSV file and select it.
3. Click **Import**.

Use the "here" link to obtain a sample file.

To add an IP or an IP Range:

1. Click **IP/IP Range > Add**.

The Add dialog box appears.

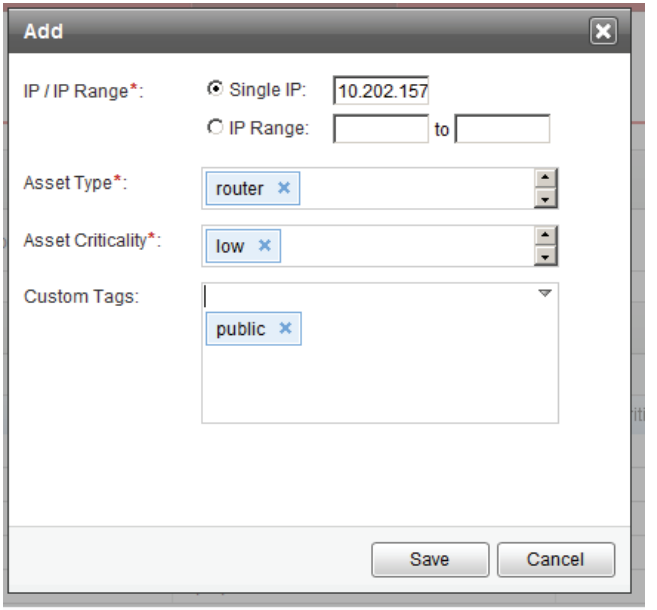


FIGURE 5-18 Add dialog box for an IP/IP Range

2. Complete the fields similarly to those shown in Figure 5-18. You can choose multiple Custom Tags for one entry. Duplicated Host Names or IP/IP Ranges are not allowed.
3. Click **Save** to preserve your settings.

To export valuable Asset Tagging CSV files:

The Export feature creates a list of asset types in the CSV file format. Backup your asset types to another location by clicking **Export**.

Asset Criticality

The asset criticality identifies the level of severity for each event log that has been tagged. For example, you can assign asset criticality such as severe, informational, warning, and critical. The following is an example of the Asset tagging Criticality page.

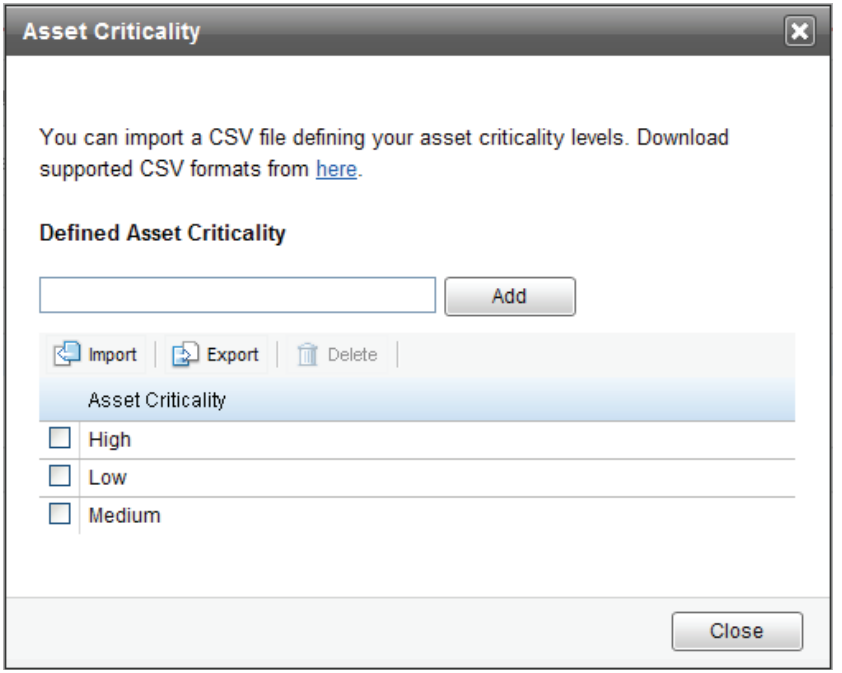


FIGURE 5-19 Asset Criticality Definition page

Import

The Import feature allows a list of asset criticality tags to be created previously. Any duplicate tags are ignored during import process.

1. Create a comma separated value (CSV) file that includes a list of asset criticality tags.
2. Click **Import** from the asset criticality action tab to import the CSV file you created.
3. From the Import: Asset criticality Tag screen, browse to the location of your asset criticality tags. Complete the action by clicking **Import**.

Export

The Export feature creates a list of asset criticality in the CSV file format. You can backup your asset criticality files and saving them to another location by clicking **Export**.

Host Name

The Host Name tab shows a list of host names with their corresponding Asset Types, Asset Criticality, and Custom tags. Each hostname can include a host name prefix or an actual hostname. The host name prefix is indicated with the wildcard "*." The wildcard indicates that any host name with a similar prefix would be considered a match.

For example, "tw-*" is created as a host name. "tw-web1" is matched with the "tw-*" host name rules. "tw-web1" is tagged with the Asset Type "router," Asset Criticality "High," and Custom Tag "corporate."

Add - Create new host prefixes by clicking **Add**.

Import - The Import feature automatically creates asset types, asset criticality, and custom tags that do not exist within their respective tables. Create a CSV file that consists of a hostname with corresponding asset types, asset criticality, and custom tags.

Export - The Export feature creates a CSV file that contains a list of host names, asset types, asset criticality, and custom tags.

IP/IP Range

The IP/IP Range tab reveals a list of IPs/IP Ranges and their corresponding Asset Types, Asset Criticality, and Custom tags. The IP/IP Range field can include an individual IP or an IP range such as 1.1.1.1 to 1.1.1.255.

Import - The Import feature automatically creates Asset Types, Asset Criticality, and Custom Tags that do not exists within their respective tables. Create a CSV file that consist of an IP/IP Range with corresponding asset types, asset criticality, and custom tags.

Export - The Export feature creates a CSV file that contains a list of IP/IP Ranges, asset types, asset criticality, and custom tags.

Search

You can also enter **Search** criteria to help narrow customized tag results when searching for a specific customized tag.

System

The system section of Threat Intelligence Manager contains information about:

Account Management

Through Account Management, you can develop and maintain a list of usernames, their access passwords, and contact information. You are essentially adding additional layers to your Address Book to help you maintain a list of the people involved in your data collection.

Adding a New User

From the Account Management screen:

1. Define your users by clicking **Add User**.

   The **Add User** window appears.
2. Enter the individual's Username, an eight-character password, password confirmation, Name, Email Address, and a description of their role that you might want to include and then click **Save**.
3. The user you defined appears on the Account Management page.
4. Repeat these steps for all necessary users in your network to complete your account database.

Editing a User

You can edit any of the users added to Account Management by selecting the box of the user you wish to edit, and then clicking **Edit** on the Account Management action tab, and then adjusting the user data as necessary. Click **Save** when complete.

Deleting a User

Remove any unnecessary users added to Account Management by selecting the box of the user you wish to remove, and then clicking **Delete** on the Account Management action tab. Users removed will no longer be available in Account Management.

Search

You can also enter **Search** criteria to help narrow results when searching for a specific user, email address, or description.

System Settings

System Settings can include both proxy settings as well as SMTP Settings. Learn more about these system settings in the sections that follow.

Proxy Settings

You can enable the use of a proxy server for the Web Reputation service and the Whois utilities by selecting the box to the left of the "Enable the use of HTTP proxy server." After selecting the box, enter the name of the server or it's IP address and port number. Click the box to the left of "Enable proxy server authentication" if you would like to enter the proxy server authentication username and password. Click **Save** to preserve your settings.

SMTP Settings

You can also configure SMTP settings by entering the SMTP URL or the SMTP from email account. Select the box for "SMTP server requires authentication" if you would like to require a username and password of SMTP users. Click **Save** to preserve your settings.

Password Policy

Set your password policy to require strong, complex passwords. Strong passwords usually contain a combination of both uppercase and lowercase letters, numbers, and symbols, and are at least eight characters or more in length.

When using a strong password policy, a user submits a new password, and the password policy determines whether the password meets your company's established requirements.

You can set very complex password requirements; but, strict password policies sometimes increase costs to an organization when they obligate users to select passwords too difficult to remember. Users are forced to call the help desk when they forget their passwords, or they might write them down and make them vulnerable to threats. So when you establish a password policy, you need to balance your need for strong security against the need to make the policy easy for users to follow.

The following parameters allow you to configure your password's strength. This is a system-wide feature.

The system administrator enables or disables the password strength setting by clicking the **Administration > System Settings > Password Policy > Enable Password Policy** check box.

Internally, the Enable Password Policy check box enables or disables the following features:

- `administratorPasswordMinimumLength - integer`
- `administratorPasswordRequireMix - boolean`
- `administratorPasswordRequireCase - boolean`
- `administratorPasswordRequireSpecial - Boolean`

Account State

When a user exceeds the number of retries allowed while entering incorrect passwords, the Threat Intelligence Manager server eventually sets their user account to inactive (locked out). The administrator must use this feature then to unlock that user account.

Note: This unlock feature applies to all user accounts, with the exception of the "root" administrator.

Resetting User Passwords

In order to reset a lost user password (including the Administrator password), you will need command line access to the machine where Threat Intelligence Manager is installed.

There is a "`tmcore_cli.bat`"command line utility that can be used to reset a user account password. This utility is located in the bin directory of the installation path, such as: `C:\Program Files\Trend Micro\Threat Intelligence Manager\bin>`

Access the utility using the following syntax:

```
tmcore_cli -action unlockout -username USERNAME [-newpassword
NEWPASSWORD]
```

To reset the administrator's account password, use the command:

```
C:\Program Files\Trend Micro\Threat Intelligence Manager\bin>
tmcore_cli -action unlockout -username admin -newpassword
AdminPassword
```

Note: - Passwords cannot be recovered. They can only be reset for a given username.
- Passwords can be reset for any user account, not just the admin account.
- The password accepted by the command line utility depends on the password strength configuration. For example, if your configuration is set to only accept strong passwords, the command line utility only accepts strong passwords. See Password Policy for more information.

Unlocking an Account

Threat Intelligence Manager includes a security feature where an account can be disabled in cases where the user has typed an incorrect password 10 times in a row. This feature is enabled by default and cannot be disabled through the user interface. You can, however, use the same "`tmcore_cli.bat`" file to unlock locked user accounts. This utility is located in the bin directory of the installation path, such as `C:\Program Files\Trend Micro\Threat Intelligence Manager\bin>`.

Access the utility using the following syntax:

```
tmcore_cli -action unlockout -username USERNAME
```

To unlock the administrator's account use:

```
C:\Program Files\Trend Micro\Threat Intelligence
Manager\bin>tmcore_cli -action unlockout -username admin
```

Session Length

During login to the Management Console, admins are allowed to choose between the default session period or an extended session period. A longer session length might be less secure if user forgets to log out from the session and leaves the console unattended.

The value for the default session length is 10 minutes and for an extended session length is 30 minutes at install time. After installation, administrators can change these values from a selected drop-down menu by going to the **Administration > System Settings** and clicking the Session tab. You can change either default or extended session time out values from this page and save the changes. New values take effect on the next login.

Licensing

This section explains how to view licensing information, manage your license, and register and activate your Threat Intelligence Manager product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's most current Maintenance rate.

A Maintenance Agreement is a contract between your organization and Trend Micro. It establishes your right to receive technical support and product updates in return for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

Note: The Maintenance Agreement has an expiration date. Your License Agreement does not. If the Maintenance Agreement expires, scanning can still occur, but you will not be able to update the scan engine or program files (even manually), nor will you be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending discontinuation. You can update

your Maintenance Agreement by purchasing renewal maintenance from your Reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

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

Viewing Your Product Licenses

To view your existing licenses:

1. Choose **Administration > License**. A brief summary of your product and license details appears on the License screen.
2. For the license you want to view, click "**View details online**." The following information appears:
   - **Product Name:** Trend Micro Threat Intelligence Manager
   - **Version:** Full or Trial
   - **Build Number**:
   - **Operating System**: Windows
   - **Platform**: ---
   - **Language:** English
   - **Licenses**: Indicates how many (seats) or licenses for this particular Activation Code.
   - **Activation Code:** The actual Activation Code that the user entered.
   - **License expiration:** The date the license expires.

To check the status of your license agreement on the Trend Micro™ Online Registration Web site, click **View details online.**

Registering Your Product

You must activate your product to use it's features. To activate this product, you must have its Activation Code, which you can obtain after registering the product and receiving a Registration Code. To obtain a registration code, go to the Trend Micro online registration Web site:

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

To activate a product:

1. Choose **Administration > License** and click **Update Online**. The "**Enter a new Activation code"** window appears.

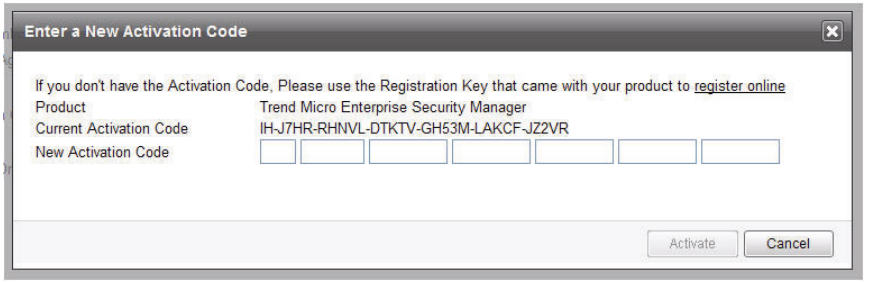


FIGURE 5-20 Enter a New Activation Code page

2. Type the new activation code in the spaces provided.
3. Click **Activate**. The Product Licenses screen reappears displaying the number of days left before the product expires.

Checking a License Status

You can also check the status of your license online by accessing Trend Micro™ Online Registration.

To check your license status online:

1. Click the **View Details Online** link.

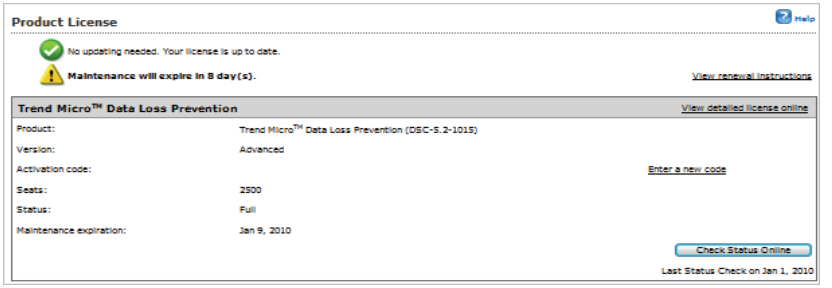


FIGURE 5-21 View Details Online link

2. The link accesses an online license home page that details all the information about your license.

About Threat Intelligence Manager

View your product version details and license agreement by clicking **Administration > About Threat Intelligence Manager**.

Version Details

You can locate the current version number of the installed software you are using simply by selecting About Threat Intelligence Manager from the Administration drop-down.

License Agreement

View the scope and other details of the Threat Intelligence Manger license agreement.

Glossary

This glossary describes special terms used in this document or the Online Help.

TERM	EXPLANATION
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.
“in the wild”	Describes known viruses that are actively circulating. *Also see* “in the zoo.”
“in the zoo”	Describes known viruses that are currently controlled by antivirus products. *Also see* “in the wild.”
(administrative) domain	A group of computers sharing a common database and security policy.
100BaseT	An alternate term for “fast Ethernet,” an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT. *Also see* 10BaseT.
10BaseT	The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024. *Also see* 100BaseT.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.
access (verb)	To read data from or write data to a storage device, such as a computer or server.

TERM	EXPLANATION
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Your products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate your products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session.
ActiveUpdate	ActiveUpdate is a function common to many products. Connected to the update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files through the Internet or the Total Solution CD.
ActiveUpdate	A utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.

TERM	EXPLANATION
ActiveX malicious code	An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as House-Call, a free online scanner. Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to “high.”
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to “system administrator” — the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of your product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
agent	A stand alone program that resides on the Trend Micro OfficeScan Servers and retrieves events from the OSCE server and then delivers them to the Threat Intelligence Server.
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.

TERM	EXPLANATION
anti-relay	Mechanisms to prevent hosts from "piggybacking" through another host's network.
antivirus	Computer programs designed to detect and clean computer viruses.
application	A Visualization application provides a specialized view into the data. An Application typically queries raw data from one or more sources, processes them and presents a specialized view of the data. An application could provide one or a collection of widgets, reports, or statistics.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.

TERM	EXPLANATION
bridge	A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address.
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
Common Vulnerabilities and Exposures (CVE)	Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (such as CVE Identifiers) for publicly known information security vulnerabilities.

TERM	EXPLANATION
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
dashboard	User interface screen in which Widgets are displayed.
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.

TERM	EXPLANATION
Deep Packet Inspection (DPI) Rules	Software vulnerabilities are shielded from attack through the use of deep-packet inspections that examine application data to and from the computer. DPI Rules allow, block, log, or edit data based on its content. DPI Rules protect vulnerabilities from known and unknown attacks by defining expected application data, and blocking malicious data based on its content. Ongoing DPI Rule updates automatically provide the most current, comprehensive protection against known and unknown attacks.
Deep Security Manager (DSM)	Deep Security Manager ("the Manager") is a powerful, centralized Web-based management system that allows you to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. All of this can be done in real-time from the desktop.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory on the C drive.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is: *C:\Programs\<your company>\ISVW\Quarantine*

TERM	EXPLANATION
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
DOS virus	Also referred to as "COM" and "EXE file infectors." DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a Web site through HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.

TERM	EXPLANATION
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.
ELF	Executable and Linkable Format—An executable file format for UNIX and Linux platforms.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.

TERM	EXPLANATION
EXE file infector	An executable program with an .exe file extension. *Also see* DOS virus.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

TERM	EXPLANATION
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
filtering, dynamic	IP service that can be used within VPN tunnels. Filters are one way GateLock controls traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. *Also see* tunneling and Virtual Private Network (VPN).
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
generated report	Displays the results of a TMQL query in a given visualization, such as a pie chart, table, line graph, and so on, in the form of a widget displayed on the Console user interface or printable form.

TERM	EXPLANATION
GeoMap	A method for mapping Internet protocol addresses to physical locations on a map of the earth.
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
Hibernate	Open source facility that provides relational database table to object mapping. It is the tool used by report management system to interact with the report database.

TERM	EXPLANATION
host	A computer connected to a network.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
hub	This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, crytography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, through a digital camera, or they may be generated by computer using graphics software.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install UNIX versions of your products.
integrity checking	*See* checksumming.

TERM	EXPLANATION
IntelliScan	IntelliScan is a scanning technology that optimizes performance by examining file headers using true-file type recognition, and scanning only file types known to potentially harbor malicious code. True-file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
Intrusion Defense Firewall (IDF)	The Intrusion Defense Firewall is an advanced, host-based intrusion defense system that brings proven network security approaches, including firewall and intrusion detection and prevention, down to individual networked computers and devices. Intrusion Defense Firewall has been architected for enterprises that recognize the need to further enhance their security posture to protect mission critical IT assets from known and zero-day attacks.
Investigation Basket	Collection of report baskets that are available to users from the console user interface.
IP	Internet Protocol—*See* IP address.

TERM	EXPLANATION
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IP gateway	Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java applets	Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality. Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to “high.”
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet’s code is transferred to your system and is executed by the browser’s Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.

TERM	EXPLANATION
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of memory.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
LDAP (Lightweight Directory Access Protocol)	An Internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name "Bob." An LDAP search would enable you to view the email addresses that meet this criteria.
license	Authorization by law to use a specific product.
license certificate	A document that proves you are an authorized user of a specific product.

TERM	EXPLANATION
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
LinkGraph	A method for displaying multiple data points on a graph form. Threat Intelligence Manager uses this method to display interconnecting source and destination IP addresses and destination ports.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
macro	A command used to automate certain functions within an application.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.

TERM	EXPLANATION
management console	The user interface for your particular product.
MB	Megabyte—1024 kilobytes of data.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the "Nimda" or "Code Red" threats.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

TERM	EXPLANATION
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
OSSEC	OSSEC is an open source HIDS tool that collects logs through an agent and correlates the data at the server. This software is meant to use this as its primary log collection infrastructure.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).

TERM	EXPLANATION
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
POJO	Acronym for Plain Old Java Objects that is one form of the database interface provided by Hibernate.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
protected network	A network protected by IWSA (InterScan Web Security Appliance).
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.

TERM	EXPLANATION
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a company customer, using a product Registration Key, on the company Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.

TERM	EXPLANATION
removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
report basket	Collection of reports maintained in the Investigation Basket user interface object.
report template	Object that contains the TMQL query and visualization information necessary to generate a report.
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
scheduled report	Generated report that is run at regular time intervals.
script	A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with "script" are "macro" or "batch file."
seat	A license for one person to use a particular product.
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)

TERM	EXPLANATION
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
server farm	A server farm is a network where clients install their own computers to run Web servers, e-mail, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.
signature-based spam detection	A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file. *Also see* rule-based spam detection. *Also see* false positive.

TERM	EXPLANATION
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
Solr	Apache solr is an enterprise search server based on Apache Lucene. This program intends to use Solr as its primary mechanism for retrieving data.
Solr Core	Multiple cores allow you to have a single Solr instance with separate configurations and indexes, with their own config and schema for very different applications, but still have the convenience of unified administration
Solr Shard	When an index becomes too large to fit on a single solr system, or when a single query takes too long to execute, an index can be split into multiple shards, and solr can query and merge results across those shards. A shard has its own instance of solr namely JVM and indexes, unlike core that share them within an instance.
spam	Unsolicited email messages meant to promote a product or service.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

TERM	EXPLANATION
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.
syslog	Syslog is an event-based messaging system that allows users to collect logs for analysis.
tagging	The process of adding additional identifying information to events.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

TERM	EXPLANATION
Threat Discovery Appliance (TDA)	Threat Discovery Appliance is a next-generation network monitoring product that uses a combination of intelligent rules, algorithms, and signatures to detect a variety of malware including worms, Trojans, backdoor programs, viruses, spyware, adware, and other threats.
TMQL	Trend Micro Query Language. Provides a unified query interface to Zero Gravity SOLR and DB data stores.
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your product detects a virus in an email message. This may *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true-file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

TERM	EXPLANATION
trusted domain	A domain from which your product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, because the messages are from a known and trusted source.
trusted host	A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.
tunnel interface	A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface. *Also see* Virtual Private Network (VPN).
tunnel zone	A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

TERM	EXPLANATION
tunneling	A method of sending data that enables one network to send data through another network's connections. Tunnelling is used to get data between administrative domains which use a protocol that is not supported by the Internet connecting those domains. With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a "Click Here for More Information" button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* JavaScript virus.

TERM	EXPLANATION
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions. By default, your company's GateLock supports two virtual routers: Untrust-VR and Trust-VR.
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same GateLock remote appliance; each one can be managed by its own virtual system administrator.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

TERM	EXPLANATION
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the virus pattern file. The scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
visualization platform	(VP) provides scalable log collection and application development framework. **Collect > Normalize > Store > Query > Visualize**. The platform can collect and store heterogeneous types of information such as logs, the Threat Encyclopedia, AD data, and so on.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
Web services	Web services describe a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol (HTTP).
Whois	A utility to allow users to look up domain names and owners of those domains with only an IP address.
widget	Visual renderings of the report templates. Widgets are contained in the Dashboard.

TERM	EXPLANATION
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.
workbench	User interface screens in which the product logs and event data are queried and analyzed.
working directory	The destination directory in which the main application files are stored, such as `/etc/iscan/iwss`.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
Zero Download	Technology enabling the decryption and reading of Private Post encrypted email messages using any modern Web browser.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).