Trend Micro™ Deep Discovery™ Analyzer 7.6

Administrator's Guide

Breakthrough Protection Against APTs and Targeted Attacks

Document Part No.: APEM769913/240703

Release Date: August 2024

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

https://www.trendmicro.com/privacy

Table of Contents

Chapter 4: Virtual Analyzer

Chapter 5: Alerts and Reports

Chapter 6: Administration

Chapter 7: Technical Support

Appendices

Preface

Preface

This guide contains information about product settings and service levels.

Documentation

The documentation set for Deep Discovery Analyzer includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Analyzer, and explanations on Deep Discovery Analyzer concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Analyzer.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Analyzer to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.

Document	Description
Online Help	Web-based documentation that is accessible from the Deep Discovery Analyzer management console. The Online Help contains explanations of Deep Discovery Analyzer components and features, as well as procedures needed to configure Deep Discovery Analyzer.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: https://success.trendmicro.com

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

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

Audience

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

- Network topologies
- Database management
- Antivirus and content security protection

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

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

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

Terminology

Terminology	Description
ActiveUpdate Server	Provides updates for product components, including patterns and engines. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.
Active primary appliance	Clustered appliance with which all management tasks are performed. Retains all configuration settings and allocates submissions to secondary appliances for performance improvement.
Administrator	The person managing Deep Discovery Analyzer
Clustering	Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.
Custom port	A hardware port that connects Deep Discovery Analyzer to an isolated network dedicated to sandbox analysis
Dashboard	UI screen on which widgets are displayed
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.
Management console	A web-based user interface for managing a product.
Management port	A hardware port that connects to the management network.
Passive primary appliance	Clustered appliance that is on standby until active primary appliance encounters an error and is unable to recover. Provides high availability.

Terminology	Description
Role-based administration	Role-based administration streamlines how administrators configure user accounts and control access to the management console.
Sandbox image	A ready-to-use software package (operating system with applications) that require no configuration or installation. Virtual Analyzer supports only image files in the Open Virtual Appliance (OVA) format.
Sandbox instance	A single virtual machine based on a sandbox image.
Secondary appliance	Clustered appliance that processes submissions allocated by the active primary appliance for performance improvement.
Standalone appliance	Appliance that is not part of any cluster. Clustered appliances can revert to being standalone appliances by detaching the appliance from its cluster.
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.
Virtual Analyzer	An isolated virtual environment used to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.
Widget	A customizable screen to view targeted, selected data sets.
YARA	YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

About Trend Micro

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

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

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

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

Chapter 1

Introduction

This chapter introduces Deep Discovery Analyzer and the new features in this release.

About Deep Discovery Analyzer

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other products. The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.

Deep Discovery Analyzer also provides a Web Services API to allow integration with any third-party product, and a manual submission feature for threat research.

What's New

TABLE 1-1. What's New in Deep Discovery Analyzer 7.6

FEATURE/ENHANCEMENT	DETAILS
New hardware model support	This release of Deep Discovery Analyzer supports the new Deep Discovery Analyzer 1300 appliance with UEFI support.
Sandbox as a Service integration	With Sandbox as a Service integration, Deep Discovery Analyzer can receive and analyze samples submitted to Sandbox as a Service.
Enhanced Virtual Analyzer	The internal Virtual Analyzer has been enhanced to include new image support for Windows 10 22H2, Windows 11, and Ubuntu 20.04.
Enhanced Trend Vision One integration	This release of Deep Discovery Analyzer includes STIX files in investigation packages sent to Trend Vision One for intelligence report generation and Auto Sweeping.
Enhanced network share scanning	The network share scanning feature has been enhanced to include configuration settings for the following: • Output folder per risk level • Cloud storage server address (AWS/Azure)

Feature/Enhancement	Details
VirusTotal integration	This release of Deep Discovery Analyzer integrates with VirusTotal to query analysis reports for detected samples.
Inline migration from Deep Discovery Analyzer 7.5	On hardware models 1100 and 1200, Deep Discovery Analyzer can automatically migrate the settings of a Deep Discovery Analyzer 7.5 installation to 7.6.

Features and Benefits

Deep Discovery Analyzer includes the following features:

Enable Sandboxing as a Centralized Service

Deep Discovery Analyzer ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any additional source of samples.

Custom Sandboxing

Deep Discovery Analyzer performs sandbox simulation and analysis in environments that match the desktop software configurations attackers expect in your environment and ensures optimal detection with low false-positive rates.

Broad File Analysis Range

Deep Discovery Analyzer examines a wide range of Windows executable, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing.

YARA Rules

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

Document Exploit Detection

Using specialized detection and sandboxing, Deep Discovery Analyzer discovers malware and exploits that are often delivered in common office documents and other file formats.

Automatic URL Analysis

Deep Discovery Analyzer performs page scanning and sandbox analysis of URLs that are automatically submitted by integrating products.

Detailed Reporting

Deep Discovery Analyzer delivers full analysis results including detailed sample activities and C&C communications via central dashboards and reports.

Alert Notifications

Alert notifications provide immediate intelligence about the state of Deep Discovery Analyzer.

Clustered Deployment

Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.

Trend Micro Product Integration

Deep Discovery Analyzer enables out-of-the-box integration to expand the sandboxing capacity of Trend Micro email and web security products.

Sample Submissions

Deep Discovery Analyzer allows sample submissions using one of the following:

- Integrated security products through web services API
- Manual submissions on the management console

- Email submissions from permitted sender domains and SMTP servers
- ICAP clients
- Network share scanning
- Manual Submission Tool

Custom Defense Integration

Deep Discovery Analyzer shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products.

ICAP Integration

Deep Discovery Analyzer supports integration with Internet Content Adaptation Protocol (ICAP) clients. After integration, Deep Discovery Analyzer can perform the following functions:

- Work as an ICAP server that analyzes samples submitted by ICAP clients
- Serve User Configuration Pages to the end user when the specified network behavior (URL access / file upload / file download) is blocked
- Control which ICAP clients can submit samples by configuring the ICAP Client list
- Bypass file scanning based on selected MIME content-types
- Bypass file scanning based on true file types
- Bypass URL scanning in RESPMOD mode
- Scan samples using different scanning modules
- Filter sample submissions based on the file types that Virtual Analyzer can process.

Chapter 2

Getting Started

This chapter describes how to get started with Deep Discovery Analyzer and configure initial settings.

The Preconfiguration Console

The preconfiguration console is a Bash-based (Unix shell) interface used to configure network settings, view high availability details, ping remote hosts, and change the preconfiguration console password.

For details, see the *Deep Discovery Analyzer Installation and Deployment Guide.*

The Management Console

Deep Discovery Analyzer provides a built-in management console that you can use to configure and manage the product.

Open the management console from any computer on the management network using one of the following web browsers:

- Microsoft Edge™
- Google Chrome™
- Mozilla Firefox™

Note

Make sure Javascript is enabled in the web browser.

To log on, open a browser window and type the following URL:

`https://<Appliance IP Address>/pages/login.php`

You can log on to the Deep Discovery Analyzer management console using one of the following methods:

- *Logging On Using Local Accounts on page 2-3*
- *Logging On With Single Sign-On on page 2-3*

Logging On Using Local Accounts

Procedure

1. On the **Log On** screen, type the logon credentials (user name and password) for the management console.

   Use the default administrator logon credentials when logging on for the first time:

   - User name: `admin`
   - Password: `Admin1234!`

   Note

   Depending on your account, provide one of the following information in the **User name** field:

   - User name
   - UPN
   - Email address

2. (Optional) Select **Enable extended session timeout** to apply the extended session timeout for your logon session. The default session timeout is 10 minutes.

   To change the session timeout settings, navigate to **Administration** > **System Settings** and click the **Session Timeout** tab.

3. Click **Log On**.

4. If this is the first time you log on, change the account password before you can access the management console.

Logging On With Single Sign-On

If you configure the required settings for SAML integration on Deep Discovery Analyzer, users can access the Deep Discovery Analyzer management console using their existing identity provider credentials.

For more information, see *SAML Authentication Tab on page 6-35*.

Procedure

1. On the **Log On** screen, select a service name from the drop-down list.
2. Click **Single Sign-on (SSO)**.

   The system automatically navigates to the logon page for your organization.
3. Follow the on-screen instructions and provide your account credentials to access the Deep Discovery Analyzer management console.

Management Console Navigation

The management console consists of the following elements:

TABLE 2-1. Management Console Elements

SECTION	DETAILS
Banner	The management console banner contains: • Product logo and name: Click to go to the dashboard. For details, see *Dashboard Overview on page 3-2*. • Name of the user currently logged on to the management console. • **Change password** link: Click to change current user password. • **Log off** link: Click to end the current console session and return to the logon screen. • System time: Displays the current system time and time zone.
Main Menu Bar	The main menu bar contains several menu items that allow you to configure product settings. For some menu items, such as **Dashboard**, clicking the item opens the corresponding screen. For other menu items, submenu items appear when you click or mouseover the menu item. Clicking a submenu item opens the corresponding screen.

Section	Details
Scroll Up and Arrow Buttons	Use the **Scroll up** option when a screen's content exceeds the available screen space. Next to the **Scroll up** button is an arrow button that expands or collapses the bar at the bottom of the screen.
Context-sensitive Help	Use **Help** to find more information about the screen that is currently displayed.

Change Password

You can change the password of the account that is currently used to access the management console. From the management console banner, click the account name on the top-right hand corner and select **Change password.**

In the fields provided, type the old password and the new passwords twice; then, click **Save**.

Getting Started Tasks

Procedure

1. Activate the product license using a valid Activation Code. For details, see *License on page 6-103*.
2. Specify the Deep Discovery Analyzer host name and IP address. For details, see *Network Tab on page 6-50*.
3. Configure proxy settings if Deep Discovery Analyzer connects to the management network or Internet through a proxy server. For details, see *Proxy Tab on page 6-54*.
4. Configure date and time settings to ensure that Deep Discovery Analyzer features operate as intended. For details, see *Time Tab on page 6-57*.
5. Configure SMTP settings to enable sending of notifications through email. For details, see *SMTP Tab on page 6-55*.
6. Import sandbox instances to Virtual Analyzer. For details, see *Importing an Image on page 4-55*.

7. Configure Virtual Analyzer network settings to enable sandbox instances to connect to external destinations. For details, see *Enabling External Connections on page 4-66*.

8. (Optional) Configure sample submission policies based on your network environment and submission sources. By default, samples of all file types are submitted to all sandbox instances. For details, see *Configuring a Submission Policy on page 4-72*.

9. (Optional) Deploy and configure additional Deep Discovery Analyzer appliances for use in a high availability or load-balancing cluster. For details, see *Cluster Tab on page 6-62*.

10. Configure supported Trend Micro products for integration with Deep Discovery Analyzer. For details, see *Integration with Trend Micro Products on page 2-6*.

11. Adjust Virtual Analyzer resource allocation between all sources by assigning weight and timeout values to all sources that submit objects to Deep Discovery Analyzer for analysis. For details, see *Submitters on page 4-88*.

Integration with Trend Micro Products

Deep Discovery Analyzer integrates with the following Trend Micro products.

Sandbox Analysis

The following lists the Trend Micro products that can send samples to Deep Discovery Analyzer for sandbox analysis:

- Apex One as a Service
- Apex One 2019
- Deep Discovery Email Inspector 2.5 or later
- Deep Discovery Inspector 3.7 or later
- Deep Discovery Web Inspector 2.5 or later

- Deep Security 10.0 or later
- InterScan Messaging Security Virtual Appliance (IMSVA) 8.2 SP2 or later
- InterScan Messaging Security Suite (IMSS) for Linux 9.1
- InterScan Messaging Security Suite (IMSS) for Windows 7.5 or later
- InterScan Web Security Virtual Appliance (IWSVA) 6.0 or later
- InterScan Web Security Suite (IWSS) 6.5
- ScanMail for IBM Domino 5.6 SP1 Patch 1 HF4666 or later
- ScanMail for Microsoft Exchange 11.0 or later
- Trend Micro TippingPoint Security Management System 5.0 or later
- Trend Micro Web Security 3.1 or later
- Trend Vision One

Note

- You can view all samples on the **Virtual Analyzer** > **Submissions** screen. Deep Discovery Analyzer administrators and investigators can also manually submit samples on this screen.
- Deep Discovery Analyzer can analyze samples from other third-party products through one of the following:
  - ICAP
  - Email messages
  - Network share scanning

On the management console of the integrating product, go to the appropriate screen (see the product documentation for details on which screen to access) and specify the following information:

- API key. This is available on the Deep Discovery Analyzer management console, in **Help** > **About**.

- Deep Discovery Analyzer IP address. If unsure of the IP address, check the URL used to access the Deep Discovery Analyzer management console. The IP address is part of the URL.
- Deep Discovery Analyzer IPv4 or IPv6 virtual address. When using Deep Discovery Analyzer in a high availability configuration, the virtual IP address is used to provide integrating products with a fixed IP address for configuration. This is available on the Deep Discovery Analyzer management console, in **Administration** > **System Settings** > **High Availability**.
- Deep Discovery Analyzer SSL port 443. This is not configurable.

Important

If the Deep Discovery Analyzer API key changes after registering with the integrated product, remove Deep Discovery Analyzer from the integrated product and add it again.

Note

Some integrating products require additional configuration to integrate with Deep Discovery Analyzer properly. See the product documentation for details.

(Optional) On the Deep Discovery Analyzer management console, review and modify the weight values of integrated products to adjust Virtual Analyzer resource allocation. For details, see *Submitters on page 4-88*.

Suspicious Objects List

Products that retrieve the suspicious objects list from Deep Discovery Analyzer:

- Deep Discovery Email Inspector 2.5 or later
- Deep Discovery Inspector 3.7 or later
- Deep Discovery Web Inspector 2.5 or later
- InterScan Web Security Virtual Appliance (IWSVA) 6.0 or later

- InterScan Web Security Suite (IWSS) 6.5
- Standalone Smart Protection Server 2.6 with the latest patch or later
- Trend Micro Apex Central 2019 with the latest hotfix
- Trend Micro Web Security 3.1 or later
- Trend Vision One

On the management console of the integrating product, go to the appropriate screen (see the product documentation for information on which screen to access) and specify the following information:

- API key. This is available on the Deep Discovery Analyzer management console, in **Help** > **About**.
- Deep Discovery Analyzer IPv4 or IPv6 address. If unsure of the IP address, check the URL used to access the Deep Discovery Analyzer management console. The IP address is part of the URL.
- Deep Discovery Analyzer IPv4 or IPv6 virtual address. When using Deep Discovery Analyzer in a high availability configuration, the virtual IP address is used to provide integrated products with a fixed IP address for configuration. This is available on the Deep Discovery Analyzer management console, in **Administration** > **System Settings** > **High Availability**.
- Deep Discovery Analyzer SSL port 443. This is not configurable.
- Deep Discovery Analyzer user logon credentials. For details, see *Accounts Tab on page 6-84*.

Important

If the Deep Discovery Analyzer API key changes after registering with the integrated product, remove Deep Discovery Analyzer from the integrated product and add it again.

Note

Some integrating products require additional configuration to integrate with Deep Discovery Analyzer properly. See the product documentation for details.

Exceptions

Products that send exceptions to Deep Discovery Analyzer:

- Deep Discovery Director
- Trend Micro Apex Central 2019 with the latest hotfix
- Trend Vision One

On the management console of the integrating product, go to the appropriate screen (see the product documentation for information on which screen to access) and specify the following information:

- Deep Discovery Analyzer IPv4 or IPv6 address. If unsure of the IP address, check the URL used to access the Deep Discovery Analyzer management console. The IP address is part of the URL.
- Deep Discovery Analyzer IPv4 or IPv6 virtual address. When using Deep Discovery Analyzer in a high availability configuration, the virtual IP address is used to provide integrated products with a fixed IP address for configuration. This is available on the Deep Discovery Analyzer management console, in **Administration** > **System Settings** > **High Availability**.
- Deep Discovery Analyzer SSL port 443. This is not configurable.
- Deep Discovery Analyzer user logon credentials. For details, see *Accounts Tab on page 6-84*.

Important

If the Deep Discovery Analyzer API key changes after registering with the integrated product, then Deep Discovery Analyzer will need to be deleted from the integrated product and added again.

Note

Some integrating products require additional configuration to integrate with Deep Discovery Analyzer properly. See the product documentation for details.

Chapter 3

Dashboard

This chapter describes the Deep Discovery Analyzer dashboard.

Dashboard Overview

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

The dashboard consists of the following user interface elements.

Element	Description
Tabs	Tabs provide a container for widgets. For details, see *Tabs on page 3-2*.
Widgets	Widgets represent the core dashboard components. For details, see *Widgets on page 3-3*.

Note

Click the gear icon ( ) to display the following options:

- **Add Widget**: Click to add a new widget
- **Play Tab Slide Show**: Click to show a dashboard slide show

Tabs

Tabs provide a container for widgets. Each tab on the dashboard can hold up to 20 widgets. The dashboard supports up to 30 tabs.

Tab Tasks

The following table lists all the tab-related tasks:

Task	Steps
Add a tab	Click the **plus** icon ( ) on top of the dashboard. The system adds a new tab with the default tab name.

Task	Steps
Edit a tab	Click the down-arrow icon ( ) next to the tab title and select an option. • **Rename**: Select this option to change the tab name • **Change Layout**: Select this option and select a layout option • **Delete**: Select this option to remove a tab
Move a tab	Use drag-and-drop to change a tab's position.

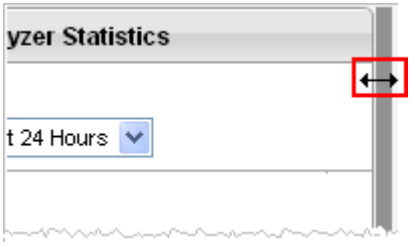
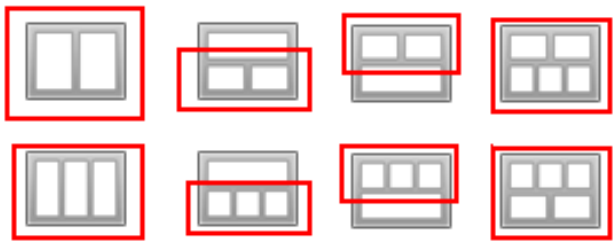
Widgets

Widgets are the core components of the dashboard. Widgets contain charts and graphs that allow you to monitor the system status and track threats.

Widget Tasks

All widgets follow a widget framework and offer similar task options.

Task	Steps
Add a widget	At the top right corner of a tab screen, click the gear icon ( ) and then click **Add Widgets**. The **Add Widgets** screen displays. For details, see *Adding Widgets to the Dashboard on page 3-4*.
Refresh widget data	Click the refresh icon ( ) to refresh widget data. Click the refresh settings icon ( ) to set the frequency that the widget refreshes or to automatically refresh widget data.
Delete a widget	Click the delete icon ( ) to close the widget. This action removes the widget from the tab that contains it, but not from any other tabs that contain it or from the widget list in the **Add Widgets** screen.
Change period	If available, click the **Period** drop-down menu to select the time period.
Change the node	If available, click the **Node** drop-down box on top of the widget to change the node.

Task	Steps
Move a widget within the same tab	Use drag-and-drop to move the widget to a different location within the tab.
Resize a widget	Point the cursor to the widget's right edge to resize a widget. When you see a thick vertical line and an arrow (as shown in the following image), hold and then move the cursor to the left or right.  You can resize any widget within a multi-column tab (red squares). These tabs have any of the following layouts. 

Adding Widgets to the Dashboard

The **Add Widgets** screen appears when you add widgets from a tab on the Dashboard.

Do any of the following:

Procedure

- To reduce the widgets that appear, click a category from the left side.
- To search for a widget, specify the widget name in the search text box at the top.
- To change the widget count per page, select a number from the **Records** drop-down menu.
- To switch between the Detailed and Summary views, click the display icons () at the top right.
- To select the widget to add to the dashboard, select the check box next to the widget's title.
- To add the selected widgets, click **Add**.

Summary Tab

View the **Summary** tab widgets to understand threats detected by Deep Discovery Analyzer based on type and amount, the volume of suspicious objects discovered during analysis, submissions over time, and the Virtual Analyzer summary.

Threat Types

This widget shows the type, amount, and risk level of threats detected in all submissions during the specified time period.

The default period is **Last 24 hours**. Change the period according to your preference.

Click a number under **High Risk**, **Medium Risk**, **Low Risk**, or **Total** to go to the **Submissions** screen and view detailed information.

Suspicious Objects

This widget plots the number of objects (IP addresses, domains, URLs, and files) added to the Suspicious Objects list during the specified time period.

The default period is **Last 24 hours**. Change the period according to your preference.

Click **View suspicious objects** to go to the **Suspicious Objects** screen and view detailed information.

For details, see *Generated Suspicious Objects List on page 4-41*.

Submissions Over Time

This widget plots the number of samples submitted to Virtual Analyzer over a period of time.

The default period is **Last 24 hours**. Change the period according to your preference.

Click **View submissions** to go to the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

Virtual Analyzer Summary

This widget shows the total number of samples submitted to Virtual Analyzer and the number of these samples with risk.

The default period is **Last 24 hours**. Change the period according to your preference.

Click the total number of submissions or the number of submissions with **High risk**, **Medium risk**, or **Low risk** to go to the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

System Status Tab

View the widgets in the **System Status** tab to understand the overall performance of Deep Discovery Analyzer based on Virtual Analyzer status, queued samples, and the hardware status.

Virtual Analyzer Status

This widget displays the status of Virtual Analyzer on one or all nodes, and the number of instances for each image.

Depending on the node type, the widget content includes one of the following:

- Single node or all nodes in a cluster: The number of queued and processing samples
- Primary or secondary node in a cluster: The number of URLs in pre-Virtual Analyzer processing queue and the number of samples the Virtual Analyzer is processing

---

Note

- The **Node** drop-down list is not available when you deploy Deep Discovery Analyzer as a standalone appliance.
- If Deep Discovery Analyzer is the primary appliance in a cluster or ICAP integration is enabled, the number of Virtual Analyzer (VA) instances displayed might not be equal to the number of Virtual Analyzer instances configured.

  To view the number of Virtual Analyzer instances configured, see *Images Tab on page 4-54*.

Click **Manage Virtual Analyzer** to go to the **Sandbox Management** screen. For details, see *Sandbox Management on page 4-52*.

Normal status on all nodes indicates all nodes are operating without errors.

If the status shows an error on one or more nodes, go to **Administration** > **System Settings** and click the **Cluster** tab to view detailed information about the error.

Queued Samples

This widget displays the number of queued samples in Virtual Analyzer. The red line indicates the estimated number of samples Virtual Analyzer can analyze within 5 minutes.

Click **View queue** to go to the **Queued** tab in the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

Hardware Status

This widget displays the real-time utilization of key hardware components.

Average Virtual Analyzer Processing Time

This widget shows the average processing time used by Virtual Analyzer for the specified period.

This widget compares the following data:

- **VA analysis time**: average time spent by samples inside Virtual Analyzer, from start to completion of the Virtual Analyzer analysis process
- **Total processing time**: average total time spent by samples inside Deep Discovery Analyzer, from the time Deep Discovery Analyzer receives the sample to the time Deep Discovery Analyzer generates the final analysis result

The default period is **Last 4 hours**. Change the period according to your preference.

Click **Manage Virtual Analyzer** to go to the **Images Tab** screen.

For details, see *Images Tab on page 4-54*.

Chapter 4

Virtual Analyzer

This chapter describes the Virtual Analyzer.

Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

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

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

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

It works in conjunction with Threat Connect, the Trend Micro service that correlates suspicious objects detected in your environment and threat data from the Smart Protection Network.

Submissions

The **Submissions** screen, in **Virtual Analyzer** > **Submissions**, includes a list of samples processed by Virtual Analyzer. Samples are files and URLs submitted automatically by integrated products, through email messages

from permitted sender domains and SMTP servers, or manually by Deep Discovery Analyzer administrators or investigators.

The **Submissions** screen organizes samples into the following tabs:

- **Completed**: Samples that Virtual Analyzer has analyzed
- **Processing**: Samples that Virtual Analyzer is currently analyzing
- **Queued**: Samples that are pending analysis
- **Unsuccessful**: Samples that have gone through the analysis process but do not have analysis results due to errors

Note

Samples listed on the **Unsuccessful** tab are not included in the sample count displayed on a widget.

- **ICAP Pre-scan**: High-risk samples received from integrated ICAP clients.

Note

The **ICAP Pre-scan** tab displays when you enable ICAP integration on the **Administration** > **> Integrated Products/Services** > **ICAP** screen.

Each tab displays a table summarizing basic information about the submitted samples. To customize which columns appear in the table, click the gear icon (), select the columns to be displayed in the table, and click **Apply**.

To update the data displayed in the table, click **Refresh**.

The following table outlines all available columns. Column display varies depending on the tab you select.

TABLE 4-1. Submission columns

COLUMN	INFORMATION
Object Information	

COLUMN	INFORMATION
Submitted	Date and time when the sample was submitted This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.
File Name	This field displays one of the following information: • File name of the sample • File name of the child object with the highest risk level • File name of any child object if no risk is detected **Note** "NONAMEFL" if file size is 0 or too small for analysis
Sample Package	Archived copy of the file sample **Note** Downloads are only available for file submissions. Click to download the file sample as an archived file. The archive password is `virus`. This column is available on the **Unsuccessful** tab only.
Submitter	This field displays one of the following: • Name of the Trend Micro product that submitted the sample • "Email Submission" if the sample was submitted through an email message • "Manual Submission" if the sample was manually submitted • "ICAP Client" if the sample originated from an ICAP client This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.

Column	Information
Submitter Name	• Host name of the product that submitted the sample • Logon account name if a sample is submitted manually • IP address of the ICAP client or SMTP server that submitted the sample
SHA-1	SHA-1 value of the sample
SHA-256	SHA-256 value of the sample This column is available on the **Completed** and **ICAP Pre-scan**tabs only.
Object Type	File or URL This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.
Detected	Date and time when the sample was detected This column is available on the **ICAP Pre-scan** tab only.
ICAP Mode	Mode reported by the ICAP client when the sample was detected Possible values are: • REQMOD: ICAP Request modification method • RESPMOD: ICAP Response modification method This column is available on the **ICAP Pre-scan** tab only.
Analysis Information	

COLUMN	INFORMATION
Risk Level	Virtual Analyzer performs static analysis and behavior simulation to identify a sample's characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings. • **Red icon** (): High risk. The object exhibited highly suspicious characteristics that are commonly associated with malware. Examples: • Malware signatures; known exploit code • Disabling of security software agents • Connection to malicious network destinations • Self-replication; infection of other files • Dropping or downloading of executable files by documents • **Yellow icon** (): Low risk. The object exhibited mildly suspicious characteristics that are most likely benign. • **Green icon** (): No risk. The object did not exhibit suspicious characteristics. • **Gray icon** (): Not analyzed For possible reasons why Virtual Analyzer did not analyze a file, see *Possible Reasons for Analysis Failure on page 4-38*. **Note** If several instances processed a sample, the icon for the most severe risk level displays. For example, if the risk level on one instance is yellow and then red on another, the red icon displays. Mouseover the icon for details about the risk level. This column is available on the **Completed** tab only.
Completed	Date and time that sample analysis was completed This column is available on the **Completed** tab only.

Column	Information
File Type	• File type of the object • File type of the archive / File type of the highest risk child object • File type of the archive / File type of any child object if no risk **Note** "Empty" or "UNKNOWN" if file size is 0 or too small to identify file type for analysis This column is available on the **Completed** and **ICAP Pre-scan** tabs only.
Threat	Name of threat as detected by Trend Micro pattern files and other components This column is available on the **Completed** and **ICAP Pre-scan** tabs only. **Note** For the ICAP Pre-scan tab, if the threat name is not available (e.g. the Web Inspection Service doesn't provide a threat name for a URL), "Undefined threat" is displayed.
Threat Types	Type of threat as detected by Trend Micro pattern files and other components This column is available on the **Completed** tab only.
Elapsed Time	The amount of time that has passed since processing started This column is available on the **Processing** tab only.

COLUMN	INFORMATION
Processed By	IP address of the node that is processing the object, if Deep Discovery Analyzer is configured in a load-balancing cluster This column is available on the **Completed** and **Processing** tabs only. **Note** When Deep Discovery Analyzer is analysing a sample with interactive mode enabled, you can perform the following tasks on the **Processing** screen: • View the current status (Preparing for access, Accessible, Completing, or Completed) • Click this field to display detailed information (for example, analysis method and IP address and port information for VNC access in interactive mode) • Click **Stop Analysis** to terminate a sample analysis
Priority	Priority assigned to the sample This column is available on the **Queued** tab only.
Time in Queue	The amount of time that has passed since Virtual Analyzer added the sample to the queue This column is available on the **Queued** tab only.
Error	Reason for analysis failure This column is available on the **Unsuccessful** tab only.
Child Files	The number of child files detected in the sample You can click the number to view detailed child file detection information. For more information, see *Viewing Child File Detection Information for ICAP Pre-scan on page 4-34*. This column is available on the **ICAP Pre-scan** tab only.
Identified By	The name of the detection module that processed the object This column is available on the **ICAP Pre-scan** tab only.

Column	Information
YARA Rule File	Name of the YARA rule file that contains the matched YARA rule If a child file is detected, you can click the link to view detailed YARA detection information. This column is available on the **Completed** tab only. **Note** • If a match is found for a child file but not the parent file, this field displays the name of any YARA rule file that contains the matched YARA rule. • If a match is found for a parent file or a file without any child file, this field displays the name of the YARA rule file that contains the matched YARA rule.
YARA Rule Name	Name of the matched YARA rule. This column is available on the **Completed** and **ICAP Pre-scan** tabs.
Event Information	
Event Logged	• For samples submitted by other Trend Micro products, the date and time the product dispatched the sample • For manually submitted samples and for samples submitted by ICAP clients, the date and time Deep Discovery Analyzer received the sample
Source / Sender	Where the sample originated • IP address for network traffic • Email address for email submissions • No data (indicated by a dash) if manually submitted
Destination / Recipient	Where the sample is sent • IP address for network traffic or email address for email • No data (indicated by a dash) if the sample is submitted manually or through an email message

COLUMN	INFORMATION
Protocol	• Protocol used for sending the sample, such as SMTP for email or HTTP for network traffic • No data (indicated by a dash) if manually submitted This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.
URL	URL of the sample  **Note** Deep Discovery Analyzer may have normalized the URL when submitted using the management console.
Email Subject	Email subject of the sample This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.
Message ID	Message ID of the sample This column is available on the **Completed**, **Processing**, **Queued** and **Unsuccessful** tabs only.
Source IP	IP address where the sample originated, based on the X-Client-IP ICAP header sent by the ICAP client This column is available on the **ICAP Pre-scan** tab only.
Destination IP	IP address where the sample was sent, based on the X-Server-IP ICAP header sent by the ICAP client This column is available on the **ICAP Pre-scan** tab only.
Source User	User currently logged on when the sample was found, based on the X-Authenticated-User ICAP header sent by the ICAP client This column is available on the **ICAP Pre-scan** tab only.
Threat Connect	Displays a link to Threat Connect This column is available on the **ICAP Pre-scan** tab only.

ICAP Submissions

Deep Discovery Analyzer supports integration with Internet Content Adaptation Protocol (ICAP) clients.

ICAP Pre-scans

When ICAP clients send samples to Deep Discovery Analyzer for analysis, Deep Discovery Analyzer performs a pre-scan which compares samples received with known existing threats using the following resources:

- Advanced Threat Scan Engine (ATSE) for file scans
- YARA rules
- Suspicious objects and user-defined suspicious objects lists
- Predictive Machine Learning engine
- Web Reputation Services (WRS) for URL scans
- Deep Discovery Analyzer cache

Depending on the result of the pre-scan, Deep Discovery Analyzer performs the following actions.

Result	Action
If the sample is a known good file / URL	• Deep Discovery Analyzer sends the original request as a response back to the ICAP client.

Result	Action
If the pre-scan result for the sample is unknown	• Deep Discovery Analyzer sends the original request as a response back to the ICAP client. • Deep Discovery Analyzer treats the sample as a submission and sends it to the Submission queue. The sample is not shown on the **ICAP Pre-scan** tab. • Deep Discovery Analyzer adds the sample to the Deep Discovery Analyzer database to benefit later submissions. **Note** If Virtual Analyzer does not support the file type of a submitted sample, Deep Discovery Analyzer does not send the sample to the Submission queue or add to the Deep Discovery Analyzer database.
If the sample matches a known malicious threat	• Deep Discovery Analyzer reponds with a `403 Forbidden` message to the ICAP client. • Deep Discovery Analyzer logs the sample and displays sample details on the **ICAP Pre-scan** tab.

Note

To view the **ICAP Pre-scan** tab on the **Submissions** screen, enable the setting in **Administration** > **Integrated Products/Services** > **ICAP**. This tab is hidden by default.

For details, see *ICAP Tab on page 6-28*.

ICAP Header Responses

For each sample submitted by ICAP clients, Deep Discovery Analyzer returns ICAP headers.

The following shows an example.

```
ICAP/1.0 200 OK
Server: Deep Discovery Analyzer 7.2 Build 1165
```

```
ISTag: "12.300.1011"
X-Virus-ID: TROJ_FRS.0NA103DD20,TROJ_FRS.0NA104DD20
X-Infection-Found: Type=0; Resolution=2; Threat=TROJ_FRS.0NA103
DD20,TROJ_FRS.0NA104DD20;
X-Response-Desc: URL: No risk rating from WRS; FILE: Detected b
y ATSE
Encapsulated: res-hdr=0, res-body=86
Date: Thu, 16 Apr 2020 07:38:01 GMT
```

The following table describes the ICAP headers.

ICAP Headers	Values	Examples

ICAP/1.0	ICAP status code.
	For example:
	• 204: If an ICAP client accepts the 204 status code with cached content
	• 200:
	  • If an ICAP client does not accept the 204 status code
	  • Content is too big for an ICAP client to store in the cache. Deep Discovery Analyzer will return `200 OK` with the HTTP content.
	  • A threat is detected. Deep Discovery Analyzer will return `200 OK` with the ICAP header and HTTP 403 Forbidden
	For more information on the status codes, see the RFC 3507 documentation.
		ICAP 1.0 200 OK
		ICAP 1.0 204 No Content

Server	Deep Discovery Analyzer version and build number	Server: Deep Discovery Analyzer 7.2 Build 1165

ICAP Headers	Values	Examples
ISTag	Version of the Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit) component This is used to validate that previous Deep Discovery Analyzer responses can still be considered fresh by an ICAP client that may still be caching them.	ISTag: "12.300.1011"
Encapsulated	The offset of each encapsulated section's start relative to the start of the encapsulating message's body	Encapsulated: req-hdr=0, req-body=86
Date	The date time value provided by the Deep Discovery Analyzer clock, specified as an RFC 1123 compliant date/time string	Date: Thu, 16 Apr 2020 07:38:01 GMT

For more details about ICAP headers, refer to the following site:

http://www.icap-forum.org/

The following table describes the additional headers that Deep Discovery Analyzer returns.

Note

If enabled, Deep Discovery Analyzer always returns the X-Response-Desc header, and only returns the X-Virus-ID and X-Infection-Found headers when a known threat is detected during the pre-scanning of samples received from ICAP clients.

ICAP Headers	Values	Examples
X-Virus-ID	One line of US-ASCII text with the name of the virus or risk encountered	X-Virus-ID: TSPY_ONLINEG.MCS
X-Infection-Found	Numeric code for the type of infection, the resolution, and the risk description	X-Infection-Found: Type=0; Resolution=2; Threat=TSPY_ONLINEG.MCS;

ICAP Headers	Values	Examples
X-Response-Desc	Reason Deep Discovery Analyzer considers a URL or file sample as malicious or safe	X-Response-Desc: URL: No risk rating from WRS; FILE: Detected by ATSE

Note

To enable these headers and configure other ICAP settings, go to **Administration** > **Integrated Products/Services** > **ICAP**.

For details, see *Configuring ICAP Settings on page 6-30*.

The X-Response-Desc header varies based on the pre-scan result. The following tables describes the X-Response-Desc headers.

Table 4-2. X-Response-Desc headers: URL

X-Response-Desc Header	Description
No risk rating from WRS	The URL is detected by Web Reputation Services (WRS) and is considered as safe.
Match found in URL exception list	The URL matches an entry in the exception list and is displayed on the Exceptions screen.
No risk rating from VA	The URL is detected by Virtual Analyzer is considered as safe.
Bypass URL scanning in RESPMOD mode	If you select **Bypass URL scanning in RESPMOD mode** on the ICAP screen, Deep Discovery Analyzer does not scan URLs in RESPMOD mode.
Invalid URL	The URL is detected with an invalid format.
Unable to analyze URL in VA	The URL is not supported in Virtual Analyzer.
Detected by WRS	The URL is detected by WRS and is considered as malicious.
Detected by suspicious objects list	The URL matches an entry in the suspicious objects list.
Detected by user-defined suspicious objects list	The URL matches an entry in the user-defined suspicious objects list.

X-Response-Desc Header	Description
Detected by VA cache	The URL is already analyzed by Virtual Analyzer and is considered as malicious.
URL submitted to VA	No pre-scan result is available for the URL. Submit the URL sample to Virtual Analyzer for analysis.

Table 4-3. X-Response-Desc headers: File

X-Response-Desc Header	Description
Match found in file exception list	The file matches an entry in the exception list and is displayed on the Exceptions screen.
No risk rating from VA	The file is detected by Virtual Analyzer is considered as safe.
Unsupported file type in VA	The file is not analyzed by Virtual Analyzer due to one of the following: • The file type is not supported in Virtual Analyzer For more information on supported file types, see *Supported File Types in Virtual Analyzer on page 4-74*. • The file is password protected and cannot be extracted by Virtual Analyzer for analysis • Other reasons that Virtual Analyzer is unable to perform the file analysis
Bypass MIME content-type scanning	If you select **Enable MIME content-type exclusion** and the content-type is in the exclusion list, Deep Discovery Analyzer does not scan the file.
Maximum file size exceeded	The file size has exceeded the maximum (60MB).
Bypass true file type scanning	If you select **Enable MIME content-type validation** and the file type is in the exclusion list, Deep Discovery Analyzer does not scan the file.
Detected by ATSE	The file is detected by Advanced Threat Scan Engine (ATSE) for Deep Discovery.
Detected by YARA rule	The file matches a YARA rule.

X-Response-Desc Header	Description
Detected by suspicious objects list	The file matches an entry in the suspicious objects list.
Detected by user-defined suspicious objects list	The file matches an entry in the user-defined suspicious objects list.
Detected by Predictive Machine Learning engine	The file is detected by the Predictive Machine Learning engine.
Detected by VA cache	The file is already analyzed by Virtual Analyzer and is considered as malicious.
File submitted to VA	No pre-scan result is available for the file. Submit the file sample to Virtual Analyzer for analysis.
Detected as password-protected file. Block sample without scanning	If you select **Classify samples as password-protected files without scanning** on the **ICAP** screen and the file is password protected, Deep Discovery Analyzer blocks the file without scanning.
Detected as password-protected file. Block non-malicious sample that cannot be extracted	If you select **Classify samples with no known risks as password-protected files only if the files cannot be extracted** on the **ICAP** screen, Deep Discovery Analyzer returns this result in the header when a password-protected file cannot be extracted but is scanned by all ICAP pre-scan modules with no risk.

The following header example indicates that the file and URL are considered safe.

```
ICAP/1.0 204 No Content
Server: Deep Discovery Analyzer 7.2 Build 1165
ISTag: "12.300.1011"
X-Response-Desc: URL: No risk rating from WRS; FILE: No risk ra
ting from VA
Date: Thu, 16 Apr 2020 07:32:30 GMT
```

The following header example indicates that Deep Discovery Analyzer returns the `HTTP/1.1 403 Forbidden` status code because the file is detected by ATSE. The URL is not scanned.

Note

If you configure the redirect page in the management console, Deep Discovery Analyzer sends the redirect page content after the HTTP 403 Forbidden header.

```
ICAP/1.0 200 OK
Server: Deep Discovery Analyzer 7.2 Build 1165
ISTag: "12.300.1011"
X-Virus-ID: TROJ_FRS.0NA103DD20,TROJ_FRS.0NA104DD20
X-Infection-Found: Type=0; Resolution=2; Threat=TROJ_FRS.0NA103
DD20,TROJ_FRS.0NA104DD20;
X-Response-Desc: URL: Bypass URL scanning in RESPMOD mode; FILE
: Detected by ATSE
Encapsulated: res-hdr=0, res-body=86
Date: Thu, 16 Apr 2020 07:38:01 GMT

HTTP/1.1 403 Forbidden
```

The following header example indicates that the URL is considered as safe and there is no detection information for the file. The file sample is automatically submitted to Deep Discovery Analyzer for analysis.

```
ICAP/1.0 204 No Content
Server: Deep Discovery Analyzer 7.2 Build 1165
ISTag: "12.300.1011"
X-Response-Desc: URL: No risk rating from WRS; FILE: File submi
tted to VA
Date: Thu, 16 Apr 2020 07:22:41 GMT
```

Submissions Tasks

The following table lists all the **Submissions** tasks.

TABLE 4-4. Submissions Tasks

TASK	STEPS
Submit Objects	Click **Submit** when you are done and then check the status on the **Processing** or **Queued** tab. When the sample has been analyzed, it appears in the **Completed** tab. For details, see *Submitting Objects on page 4-24*. To manually submit multiple files at once, use the Manual Submission Tool. See *Manually Submitting Objects on page 4-27*.
Reanalyze	Select one or more samples and click **Reanalyze** to: • Remove the existing analysis result • Resubmit the sample to the queue • Reanalyze the sample again, ignoring any cached data This option is available on the **Completed** and **Unsuccessful** tabs only. For more information, see *Reanalyzing Samples on page 4-22*.
Export All	Export all displayed submissions to a CSV file. This option is available on the **Completed**, **Unsuccessful** and **ICAP Pre-scan** tabs only.
Delete	On the **Completed**, **Queued**, or **Unsuccessful** tab, select one or more entries (up to 50) and click **Delete** to delete the selected samples and all related analysis data. On the **Processing** tab, select one or more entries (up to 50) and click **Delete** to move the selected samples to the **Unsuccessful** tab.
Detailed Information Screen	On the **Completed** tab, click anywhere on a row to view detailed information about the submitted sample. A new section below the row shows the details. For details, see *Detailed Information Screen on page 4-32*.
Prioritize Objects	On the **Queued** tab, select one or more entries (up to 50) and click **Prioritize** to move the entries to the top of the queue.

Task	Steps
Data Filters	If there are too many entries in the table, use data filters to limit the entries. Each tab uses a different set of data filters. Available data filters on the **Completed** tab only: • **Risk level**: Filters by the **Risk Level** column. • **Event logged**: Filters by the **Event Logged** column. All time periods indicate the time used by Deep Discovery Analyzer. If no time period is selected, the default configuration of **Last 24 hours** is used. Available data filter on the **Processing** tab only: • **Type**: Allows you to display all entries or samples processed with interactive mode enabled Available data filters on the **Unsuccessful** tab only: • **Error**: Filters by the **Error** column. • **Submitted**: Filters by the **Submitted** column. All time periods indicate the time used by Deep Discovery Analyzer. If no time period is selected, the default configuration of **Last 24 hours** is used. Available data filter on the **ICAP Pre-scan** tab only: • **Detected**: Filters by the **Detected** column. All time periods indicate the time used by Deep Discovery Analyzer. If no time period is selected, the default configuration of **Last 24 hours** is used. The following options are available on all tabs: • All tabs contain a search box. Type some characters in the search text box, and then press ENTER. Deep Discovery Analyzer searches only the file names and URLs in the current tab for matches. Performing a search on the **Completed** tab also searches for child file names as well. • The **Advanced** link can limit the entries according to information specified in one or more columns. For details, see *Applying Advanced Filters on page 4-21*.

Task	Steps
Customize columns	To customize which columns appear in the table, click the gear icon ( ), select the columns to be displayed in the table, and click **Apply**. Deep Discovery Analyzer saves the column settings for your user account and displays the selected table columns the next time you access the **Submissions** screen.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of samples. If all samples cannot display at the same time, use the pagination controls to view the samples that are hidden from view.

Applying Advanced Filters

Procedure

1. Click **Advanced**.

   The filter bar appears.

2. In the **Filter** drop-down box, select an attribute.

3. Depending on the attribute selected, specify any additional details required by the attribute.

4. To add another attribute, click +.

   To remove an attribute, click ×. You cannot delete the last filter.

5. Click **Apply** to immediately apply the filter to the current table.

   Once applied, the following options are available:

   - **Edit**: Modify the current filter
   - **Clear**: Removes the applied filter
   - **Save**: Saves any changes made to the filter, or saves the filter under a new name

Note

- Filters are saved in the tab where they were created. However, Deep Discovery Analyzer does not allow duplicate filter names, even if they were saved in a different tab.
- Click ▼ on the search text box to view all filters saved for the current tab. Selecting a saved filter immediately applies that filter to the current table.
- Click ✖ to delete a saved filter.

6. Click **Cancel** to discard the current filter.

Reanalyzing Samples

You can reanalyze selected samples to:

- Remove the existing analysis result
- Resubmit the sample to the queue
- Reanalyze the sample again, ignoring any cached data

Note

You can also reanalysis samples with interactive mode enabled.

Procedure

1. Go to **Virtual Analyzer** > **Submissions**.
2. Select one or more samples and click **Reanalyze**.
3. (Optional) Select **Delete associated suspicious objects** to remove suspicious objects detected from the last sample analysis.
4. (Optional) To allow VNC access to Virtual Analyzer for the sample analysis, select **Enable interactive mode for this sample analysis** and configure the following settings:

a. Select a Windows image.

b. Select a timeout period.

Note

- Deep Discovery Analyzer starts the countdown timer for the timeout when a sample is submitted successfully. When the timeout period is reached, Deep Discovery Analyzer terminates VNC access, even when an analysis is still in progress. For example, when you configure a timeout period of 30 minutes for a sample submission and start a VNC session after 5 minutes, the remaining time for the session is 25 minutes.
- The actual timeout period for an archive file may be longer than the setting you specify because Deep Discovery Analyzer starts the timeout countdown separately for each file in the archive.

c. Select the **Automatic** analysis method to have Virtual Analyzer start the analysis automatically when you access the image using a VNC client; otherwise, select **Manual** to manually start the analysis after you have started the VNC session.

Note

- Interactive mode is not available for URL list submissions or when more than one sample is selected for reanalysis.
- Deep Discovery Analyzer administrators can configure advanced interactive mode settings (such as port range and security password for VNC access).

  For more information, see *Interactive Mode Tab on page 4-68*.

5. Click **Continue**.

Submitting Objects

Procedure

1. Go to **Virtual Analyzer** > **Submissions**.
2. Click **Submit Objects**.

   The **Submit objects** window appears.
3. To submit a single file, select **File**.
   a. Browse and select a sample to upload.
   b. (Optional) For Portable Executable samples, specify command line parameters if required.
   c. (Optional) Select **Prioritize** to put submitted objects at the top of the queue.
   d. (Optional) To allow VNC access to Virtual Analyzer for the sample analysis, select **Enable interactive mode for this sample analysis** and configure the following settings:
      1. Select an image.
      2. Select a timeout period.

      Note

      Deep Discovery Analyzer starts the countdown timer for the timeout when a sample is submitted successfully. When the timeout period is reached, Deep Discovery Analyzer terminates VNC access, even when an analysis is still in progress. For example, when you configure a timeout period of 30 minutes for a sample submission and start a VNC session after 5 minutes, the remaining time for the session is 25 minutes.

      3. Select the **Automatic** analysis method to have Virtual Analyzer start the analysis automatically when you access the image

using a VNC client; otherwise, select **Manual** to manually start the analysis after you have started the VNC session.

Note

- Interactive mode is not available for URL list submissions or when more than one sample is selected for submission.
- Deep Discovery Analyzer administrators can configure advanced interactive mode settings (such as port range and security password for VNC access).

  For more information, see *Interactive Mode Tab on page 4-68*.

e. Click **Submit**.

Note

- After submitting a sample, you can view the VNC access information and analysis status on the **Processing** tab. Use the VNC access information to start a VNC session to a running Virtual Analyzer image.
- For archives, Virtual Analyzer merges analysis results for files inside archives into one report.

4. To submit a single URL, select **URL**.

a. Specify a single URL.

b. (Optional) Select **Send to URL pre-filter** to send submitted URLs to the URL pre-filter. URLs found safe by the URL pre-filter are not sent to Virtual Analyzer for scanning and analysis.

c. (Optional) Select **Prioritize** to put submitted objects at the top of the queue.

d. Click **Submit**.

Note

Before submission, Deep Discovery Analyzer normalizes all occurrences of the following:

- Punycode for URL domains
- URL encoding for URL paths and query strings

5. To submit multiple URLs, select **URL list**.
   a. Browse and select a URL list file.

Note

A URL list is a CSV or TXT file containing a maximum of 1,000 URLs. For CSV files, specify URLs in the first column. The URL list file must specify each URL in own line, and use UTF-8 encoding.

Before submission, Deep Discovery Analyzer normalizes all occurrences of the following:

- Punycode for URL domains
- URL encoding for URL paths and query strings

Analysis of 1,000 URLs may take several hours.

   b. (Optional) Select **Send to URL pre-filter** to send submitted URLs to the URL pre-filter. URLs found safe by the URL pre-filter are not sent to Virtual Analyzer for scanning and analysis.
   c. (Optional) Select **Prioritize** to put submitted objects at the top of the queue.
   d. Click **Submit**.
6. To upload applications which require certain files to be located in specific paths, select **Bundle file**.
   a. Browse and select an archive file.

Note

For archives, Virtual Analyzer merges analysis results for files inside archives into one report.

b. Specify which file inside the archive to run.

c. (Optional) For Portable Executable samples, specify command line parameters if required.

d. (Optional) Select **Prioritize** to put submitted objects at the top of the queue.

e. Specify where the files should be extracted.

- To extract all files in the archive to a single folder, specify the complete path in the **Extraction Path** text box.
- To extract specific files in the archive to another path, specify the **File name** and the complete **Path** for each file in the section below.
  - Click + to specify a new file.
  - Click × to remove an entry.

f. Specify the character encoding used in file names.

g. Click **Submit**.

Note

To manually submit multiple files at once, use the Manual Submission Tool. For details, see *Manually Submitting Objects on page 4-27*.

Manually Submitting Objects

Use the Manual Submission Tool to remotely submit samples from locations on users' computers to Deep Discovery Analyzer. This feature allows users to submit multiple samples at once, which are added to the **Submissions** queue.

In addition to Microsoft Windows operating systems, the Manual Submission Tool supports the following Linux distributions:

- CentOS/RedHat 5.x (32-bit and 64-bit)
- CentOS/RedHat 6.x (32-bit and 64-bit)
- CentOS/RedHat 7.x (32-bit and 64-bit)
- CentOS/RedHat 8.x (64-bit)
- CentOS/RedHat 9.x (64-bit)
- CentOS Stream 9 (64-bit)
- Ubuntu 12.04 (32-bit)
- Rocky Linux 9.0 (64-bit)

Important

`glibc.i686` and `zlib.i686` must be installed on 64-bit Linux distributions.

Manually Submitting Objects in Windows

Procedure

1. If it is not already installed, install the Manual Submission Tool. For details, see *Manual Submission Tool on page 6-101*.
2. Go to the Manual Submission Tool package folder, open the `work` folder, and then place all of the sample files or an URL list file into the `indir` folder.
3. Run `cmd.exe`, and change the directory (`cd`) to the tool package folder.
4. Depending on the type of object you want to upload, do one of the following:

Tip

Execute `dtascli.exe` for help.

- **File**: Execute `dtascli.exe -u` to upload all of the files in the `work/indir` folder to Virtual Analyzer.

  After executing `dtascli.exe -u`, `cmd.exe` shows the following, along with all of the files that were uploaded from the `work/indir` folder.

- **URL list**: Execute `dtascli.exe -u --url` to upload the file `url.txt` in the `work/indir` folder to Virtual Analyzer.

  After executing `dtascli.exe -u --url`, `cmd.exe` shows the following, along with all of the URLs that were uploaded in the `url.txt` file.

Note

The URL list must use the name `URL.txt`.

Before submission, Deep Discovery Analyzer normalizes all occurrences of the following:

- Punycode for URL domains
- URL encoding for URL paths and query strings

5. After uploading the files or URLs to Virtual Analyzer, confirm that they are being analyzed in the management console. Click **Virtual Analyzer** > **Submissions** to locate the files.

   Shortly after submitting the files or URLs, before they have been analyzed, they appear in the **Processing** or **Queued** tab. When the samples have been analyzed, they appear in the **Completed** tab. If the samples encountered errors during analysis, they appear in the **Unsuccessful** tab.

Manually Submitting Objects in Linux

Procedure

1. If it is not already installed, install the Manual Submission Tool. For details, see *Manual Submission Tool on page 6-101*.
2. Go to the Manual Submission Tool package folder, open the `work` folder, and then place all of the sample files or an URL list file into the `indir` folder.
3. Open the terminal, and change the directory (`cd`) to the tool package folder.
4. Execute `chmod +x dtascli`.
5. Depending on the type of object you want to upload, do one of the following:

Tip

Execute `./dtascli` for help.

- **File**: Execute `./dtascli -u` to upload all of the files in the `work/indir` folder to Virtual Analyzer.

  After executing `./dtascli -u`, `terminal` shows all of the files that were uploaded from the `work/indir` folder.

- **URL list**: Execute `./dtascli -u --url` to upload the file `url.txt` in the `work/indir` folder to Virtual Analyzer.

  After executing `./dtascli -u --url`, `terminal` shows all of the URLs that were uploaded in the `url.txt` file.

  Note

  The URL list must use the name `URL.txt`.

  Before submission, Deep Discovery Analyzer normalizes all occurrences of the following:

  - Punycode for URL domains
  - URL encoding for URL paths and query strings

6. After uploading the files or URLs to Virtual Analyzer, confirm that they are being analyzed in the management console. Click **Virtual Analyzer** > **Submissions** to locate the files.

   Shortly after submitting the files or URLs, before they have been analyzed, they appear in the **Processing** or **Queued** tab. When the samples have been analyzed, they appear in the **Completed** tab. If the samples encountered errors during analysis, they appear in the **Unsuccessful** tab.

Detailed Information Screen

On the **Completed** tab, click anywhere on a row to view detailed information about the submitted sample. A new section below the row shows the details.

The following fields are displayed on this screen:

<table>
<tr><th rowspan="2">Field Name</th><th colspan="2">Information</th></tr>
<tr><th>File/Email Message Sample</th><th>URL Sample</th></tr>
<tr><td>Submission details</td><td>Basic data fields (such as Logged, File name, and Type) extracted from the raw logs</td><td>Basic data fields (such as Logged, URL, Source IP and port, and Destination IP and port) extracted from the raw logs

  Note
Deep Discovery Analyzer may have normalized the URL.</td></tr>
<tr><td></td><td colspan="2">• Sample ID (SHA-1)
• Child files, if available, contained in or generated from the submitted sample
• The IP address of the node that processed the sample
• The Raw Logs link shows all the data fields in the raw logs
• Scan actions for scans performed on network shares</td></tr>
</table>

Field Name	Information	
	File/Email Message Sample	URL Sample
Notable characteristics	The categories of notable characteristics that the sample exhibits, which can be any or all of the following: • Anti-security, self-preservation • Autostart or other system reconfiguration • Deception, social engineering • File drop, download, sharing, or replication • Hijack, redirection, or data theft • Malformed, defective, or with known malware traits • Process, service, or memory object change • Rootkit, cloaking • Suspicious network or messaging activity	
Other submission logs	A table that shows the following information about other log submissions: • Logged • Protocol • Direction • Source IP • Source Host Name • Destination IP • Destination Host Name	
MITRE ATT&CK ™ Framework	A list of MITRE ATT&CK ™ tactics, techniques, and sub-techniques detected. Click a link to view more information on the MITRE website.	

Field Name	Information	
	File/Email Message Sample	URL Sample
Report	The PDF icon ( ) links to a downloadable PDF report and the HTML icon ( ) links to an interactive HTML report. **Note** An unclickable link means there were errors during simulation. Mouseover the link to view details about the error.	
Investigation package	**Download** links to a password-protected investigation package that you can download to perform additional investigations. For details, see *Investigation Package on page 4-35*.	
Global intelligence	**View in Threat Connect** is a link that opens Trend Micro Threat Connect The page contains detailed information about the sample.	
VirusTotal	Click **View in VirusTotal** to open VirusTotal in a new browser tab with a query for the sample. **Tip** If the object contains multiple objects, you can view the VirusTotal information for selected detected child objects in a window that appears.	

Viewing Child File Detection Information for ICAP Pre-scan

You can view the detailed detection information of child files in a submitted sample for ICAP Pre-scan.

Procedure

1. Go to **Virtual Analyzer** > **Submissions**.
2. Click the **ICAP Pre-scan** tab.
3. Click the number in the **Child Files** column.

The **Child File Detections** screen appears.

The following table describes the information on the screen.

Field	Description
File Name	Name of the child file
File Type	File type of the child file
Threat	Name of threat as detected by Trend Micro pattern files and other components
SHA-1	SHA-1 value of the child file
SHA-256	SHA-256 value of the child file
YARA Rule Name	Name of the YARA rule that was matched
YARA Rule File	Name of the YARA rule file that contains the matched YARA rule
VirusTotal	Click to open VirusTotal in a new browser tab with a query for the child file.

Investigation Package

The investigation package helps administrators and investigators inspect and interpret threat data generated from samples analyzed by Virtual Analyzer. It includes files in OpenIOC format that describe Indicators of Compromise (IOC) identified on the affected host or network.

The table below describes some of the files within the investigation package that will aid in an investigation.

Table 4-5. Investigation Package Contents

Path within the Investigation Package	Description
\%SHA1%	Each folder at the root level, with an SHA-1 hash value as its name, is associated with one object. More than one folder of this type will only exist if the first object is an archive file or an email message.

Path within the Investigation Package	Description
\%SHA1%\%imageID%	Associated with a sandbox image that analyzed the object.
\%SHA1%\%imageID%\drop\droplist	Contains a list of the files that were generated or modified during analysis.
\%SHA1%\%imageID%\memory\image.bin	Contains the raw memory dump after the process was launched into memory.
\%SHA1%\%imageID%\pcap\%SHA1%.pcap	Contains captured network data that can be used to extract payloads. The file does not exist If no network data was generated.
\%SHA1%\%imageID%\report\report.xml	Contains the final analysis report for a single object for a specific image.
\%SHA1%\%imageID%\report\so.xml	Contains a list of all suspicious objects detected during analysis. This file is empty if no suspicious objects were detected during analysis.
\%SHA1%\%imageID%\report\SHA1.ioc	Contains technical characteristics that identify attacker's tactics, techniques and procedures or other evidence of compromise.
\%SHA1%\%imageID%\screenshot\ %SHA1%-%N%.png	A screenshot of a UI event that occurred during analysis. The file does not exist if no UI events occurred during analysis.
\common	Contains files that are common amongst all of the samples.
\common\drop\%%	Generated or modified during analysis.
\common\sample\%SHA1%	The submitted sample.
\common\sample\extracted\%SHA1%	Extracted from the sample during analysis.
\%SHA1%.report.xml	The final analysis report for all objects.
\%SHA1%\%imageID%\extrainfo	Contains files related to the sandbox image that analyzed the object.

Path within the Investigation Package	Description
\%SHA1%\%imageID%\extrainfo\extra_info.xml	Contains additional details about the sandbox image that analyzed the object.
\%SHA1%\%imageID%\strings	Contains files related to the sandbox image that analyzed the object.
\%SHA1%\%imageID%\strings\%SHA1%.string	Contains string dump retrieved from the object during the analysis in the sandbox image.
\%SHA1%.ioc	The IOC file.
\%SHA1%_ioc.stix	The STIX IOC file.
\%SHA1%_so.stix	The STIX SO file.
\%SHA1%_so_stix2.json	The STIX2 SO file.
\%SHA1%_ioc_stix2.json	The STIX2 IOC file.
\working	Contains logs and reports generated by Virtual Analyzer. Analysis results for samples are generated based on the aggregated data from other modules and the consolidated log and report data.

Investigation Package Data Retention

Deep Discovery Analyzer can retain the investigation package data for up to 100 days, but the time can be reduced due to storage limitations.

Note

To ensure the availability of the investigation package data, Trend Micro recommends backing up the data to an external server. For details, see *Data Backup on page 6-94*.

The following examples illustrate how storage limitations can affect the amount of time that the investigation package data is retained in Deep Discovery Analyzer.

Based on testing done by Trend Micro, the average size of the investigation package data is 8 MB. If Deep Discovery Analyzer analyzes 8000 samples per day, then the resulting investigation package data is 64000 MB.

If Deep Discovery Analyzer is in cluster mode, the disk space occupied per day is multiplied by the number of appliances in the cluster.

Possible Reasons for Analysis Failure

If the Risk Level column shows a gray icon ( ), Virtual Analyzer has not analyzed the sample. The following table lists possible reasons for analysis failure and identifies actions you can take.

TABLE 4-6. Possible Reasons for Analysis Failure

REASON	ACTION
Virtual Analyzer does not support the file format, or the file is empty.	Check the supported file type list in the **Virtual Analyzer** > **Sandbox Management** > **Submission Policies** tab.
The available sandbox images do not support the file format.	Check the sandbox image information in the **Virtual Analyzer** > **Sandbox Management** > **Images** tab.
The URL exceeds the limit of 2083 characters.	Verify that the URL does not exceed 2,083 characters.
Virtual Analyzer does not support the encryption or compression format.	Check the password list in the **Virtual Analyzer** > **Sandbox Management** > **File Passwords** tab.
Virtual Analyzer does not support the file format.	Unsupported file type in current sandbox image. Check the sandbox image information in the **Virtual Analyzer** > **Sandbox Management** > **Images** tab.

Reason	Action
Virtual Analyzer is unable to access the Internet.	Verify the connection of the sandbox management network to the Internet.
An unexpected error has occurred on the Sandbox for macOS.	Please contact your support provider.
The Sandbox for macOS did not return an analysis result before the timeout period expired.	Resubmit the object for analysis. If the issue persists, contact your support provider.
Unable to establish a connection to the Sandbox for macOS.	Verify the connection of the management network to the Internet.
The URL is invalid.	Verify that the specified URL is in a valid format.
Extracted file sizes exceeds total limitation	Verify that the total file size of the extracted samples do not exceed the specified limitation.
Archive extracted for analysis. Child file scanning is unsuccessful.	See the scan results for the extracted files.
Virtual Analyzer is unable to analyze the object. The available disk space is insufficient.	Verify that the disk space is sufficient to perform the analysis.
Virtual Analyzer is unable to analyze the object within the timeout period.	Resubmit the object for analysis. If the issue persists, contact your support provider.

Reason	Action
Virtual Analyzer is unable to analyze the object. Dependencies that the object requires cannot be found.	Missing required files to execute the application. Use the **Bundle files** option to upload the required files to analyze the object.
Virtual Analyzer is unable to analyze the object. The object crashes while being analyzed.	Resubmit the object for analysis. If the issue persists, contact your support provider.
Virtual Analyzer is unable to analyze the object. The object must be run with the correct command line arguments.	Resubmit the object with the required command line parameters.
Virtual Analyzer is unable to analyze the object. The Office license has expired.	Re-import an image with a valid license for Microsoft Office.
An unexpected error has occurred.	Resubmit the object for analysis. If the issue persists, contact your support provider.
The license for the Sandbox for macOS has expired.	Please contact your support provider.
Analysis has been canceled by the user	A user has stopped the sample analysis in Interactive Mode. Resubmit the object for analysis.
Virtual Analyzer is unable to analyze the object within the timeout period	In Interactive Mode, a sample is not analyzed before the timeout period and Virtual Analyzer returns a rating of -45. Resubmit the object for analysis, set a longer timeout value, and start the sample analysis before the timeout period in Interactive Mode.

Suspicious Objects

Suspicious objects are objects with the potential to expose systems to danger or loss. Deep Discovery Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.

Note

- You can configure Deep Discovery Analyzer to synchronize suspicious objects from Trend Vision One or Deep Discovery Director.

  For more information, see *Trend Vision One Tab on page 6-10* or *Registering to Deep Discovery Director on page 6-18*.

- If you integrate Deep Discovery Analyzer with Deep Discovery Director and Trend Micro Apex Central, Deep Discovery Analyzer uploads the Suspicious Objects list only to Deep Discovery Director.

  You can check the synchronization status on the Deep Discovery Director management console. For more information, see the **Deep Discovery Director Administrator's Guide**.

- If you integrate Deep Discovery Analyzer with Trend Vision One, Deep Discovery Director, and Trend Micro Apex Central, Deep Discovery Analyzer uploads the Suspicious Objects list only to Trend Vision One.

Generated Suspicious Objects List

The following table describes the suspicious objects that Deep Discovery Analyzer detects and adds to the Generated Suspicious Objects list.

Field	Description
Last Detected	Date and time Virtual Analyzer last found the object in a submitted sample
Expiration	Date and time Virtual Analyzer will remove the object from the **Suspicious Objects** tab

Field	Description
Risk Level	If the suspicious object is: • **IP address** or **domain**: The risk level that typically shows is either **High** or **Medium** (see risk level descriptions below). This means that high- and medium-risk IP addresses/domains are treated as suspicious objects. • **URL**: The risk level that shows is **High** or **Medium** • **File SHA-1**: The risk level that shows is always **High** Risk level descriptions: • **High**: Known malicious or involved in high-risk connections • **Medium**: IP address/domain/URL is unknown to reputation service
Type	**IP address**, **Domain**, **URL**, or **File SHA-1**
Object	The IP address, domain, URL, or SHA-1 hash value of the file
Latest Related Sample	SHA-1 hash value of the sample where the object was last found.
Related Submissions	The total number of samples where the object was found. Clicking the number opens the **Submissions** screen with the SHA-1 hash value as the search criteria.

The following table describes the tasks you can perform on the **Generated Suspicious Objects** tab.

Table 4-7. Suspicious Objects Tasks

Task	Steps
Export/Export All	Select one or several objects and then click **Export** to save the objects to a CSV file. Click **Export All** to save all the objects to a CSV file.
Add to Exceptions	Select one or several objects that you consider harmless and then click **Add to Exceptions**. The objects move to the **Exceptions** tab.

Task	Steps
Never Expire	Select one or several objects that you always want flagged as suspicious and then click **Never Expire**.
Expire Now	Select one or several objects that you want to remove from the **Suspicious Objects** and then click **Expire Now**. When the same object is detected in the future, it will be added back to the **Suspicious Objects**.
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type in the **Show** drop-down box. • Select a column name in the **Search column** drop-down box and then type some characters in the **Search keyword** text box next to it. As you type, the entries that match the characters you typed are displayed. Deep Discovery Analyzer searches only the selected column in the table for matches.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

Synchronized Suspicious Objects List

The following table describes the suspicious objects that Deep Discovery Analyzer synchronizes from Deep Discovery Director or Trend Vision One.

Field	Description
Object	The IP address, domain, URL, or SHA-1 hash value of the file
Type	**IP address**, **Domain**, **URL**, or **File SHA-1**
Source	The source (Deep Discovery Director or Trend Vision One) that added the suspicious object

Field	Description
Risk level	If the suspicious object is: • **IP address** or **domain**: The risk level that typically shows is either **High** or **Medium** (see risk level descriptions below). This means that high- and medium-risk IP addresses/domains are treated as suspicious objects. • **URL**: The risk level that shows is **High** or **Medium** • **File SHA-1**: The risk level that shows is always **High** Risk level descriptions: • **High**: Known malicious or involved in high-risk connections • **Medium**: IP address/domain/URL is unknown to reputation service
Expiration	Date and time Virtual Analyzer will remove the object from the **Suspicious Objects** tab
Last synchronized	Date and time the object was last synchronized from Deep Discovery Director or Trend Vision One

The following table describes the tasks you can perform on the **Synchronized Suspicious Objects** tab.

Task	Steps
Export All	Click **Export All** to save all the objects to a CSV file.
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type from the **Type** drop-down list. • Type a keyword in the **Search keyword** text box.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

User-defined Suspicious Objects List

On the **User-defined Suspicious Objects** tab, you can manually add suspicious objects to Deep Discovery Analyzer using the Structured Threat Information eXpression (STIX) format.

The following columns show information about objects on the **User-defined Suspicious Objects** tab.

TABLE 4-8. User-defined Suspicious Objects columns

COLUMN NAME	INFORMATION
Added	Date and time when the suspicious object was added
Type	IP address, Domain, URL, file SHA-1, or file SHA-256
Object	The IP address, domain, URL, or SHA-1 or SHA-256 hash value of the file Click **Edit** to modify the displayed value.
Source	The source (Deep Discovery Director, local, or Trend Vision One) that added the suspicious object

Deep Discovery Analyzer can import STIX files formatted using the 1.2, 1.1.1 and 1.0.1 version specifications. The 1.0.1 specification can only be used for Virtual Analyzer output.

The STIX file can include multiple objects. However, Deep Discovery Analyzer only imports the following supported STIX indicators:

- Indicator - File Hash Watchlist (SHA-1 and SHA-256)
- Indicator - URL Watchlist
- Indicator - Domain Watchlist
- Indicator - IP Watchlist

STIX indicators can use the following Properties attributes:

- `@condition` must be `Equals`
- `@apply_condition` must be `ANY`

Managing the User-defined Suspicious Objects List

Important

To have Deep Discovery Analyzer block a domain (for example, test.com) on the User-defined Suspicious Objects list, create two entries to add the domain as a Domain object type and a URL object type to the list.

Procedure

1. Go to **Virtual Analyzer** > **Suspicious Objects**, and click the **User-defined Suspicious Objects** tab.
2. To specify a single object:
   a. Click **Add**.

      The **Add Object** window appears.

   b. Select an object type:

      - **IP address**: Type the IP address or a hyphenated range
      - **Domain**: Type a domain name

        Note

        Wildcards are only allowed in a prefix, and must be connected with a ". " symbol. Use only one wildcard per domain. For example, *.com will match abc.com or test.com.

      - **URL**: Type the URL

Note

Deep Discovery Analyzer supports both HTTP and HTTPS.

Wildcards are only allowed in a prefix. Wildcards used in the domain part of an URL must be connected with a ". " symbol. Use only one wildcard per URL. For example, http://*.com will match abc.com or test.com.

A wildcard can match any part of the URL's URI part. For example, http://abc.com/*abc will match http://abcd.com/test.abc.

- **File SHA-1**: Type the SHA-1 hash value of the file
- **File SHA-256**: Type the SHA-256 hash value of the file

c. Click **Add**.

Note

The **User-defined Suspicious Objects** list supports a maximum of 25,000 objects.

3. To add multiple objects using a STIX file:

a. Click **Import List from STIX**.

b. Specify a valid STIX file.

c. Click **Import**.

Note

Deep Discovery Analyzer can import STIX files formatted using the 1.2, 1.1.1 and 1.0.1 version specifications. The 1.0.1 specification can only be used for Virtual Analyzer output.

The STIX file can include multiple objects. However, Deep Discovery Analyzer only imports the following supported STIX indicators:

- Indicator - File Hash Watchlist (SHA-1 and SHA-256)
- Indicator - URL Watchlist
- Indicator - Domain Watchlist
- Indicator - IP Watchlist

STIX indicators can use the following Properties attributes:

- `@condition` must be `Equals`
- `@apply_condition` must be `ANY`

4. To remove objects in the list:
   - Select one or more objects, and click **Delete** to remove the selected objects.
   - Click **Delete All** to remove all objects in the list.

Exceptions

Objects in the exceptions list are automatically considered safe and are not added to the suspicious objects list. Manually add trustworthy objects or go to the **Virtual Analyzer** > **Suspicious Objects** screen and select suspicious objects that you consider harmless.

The following columns show information about objects in the exception list.

TABLE 4-9. Exceptions Columns

COLUMN NAME	INFORMATION
Added	Date and time Virtual Analyzer added the object to the **Exceptions** tab
Type	The object type (**IP address**, **Domain**, **URL**, **File SHA-1**, or **File SHA-256**).
Object	The IP address, domain, URL, or SHA-1 or SHA-256 hash value of the file
Source	The source (Trend Vision One, Apex Central, Deep Discovery Director, or local) that added the exception
Notes	Notes for the object. Click the link to edit the notes.

Exceptions Tasks

The following table lists all the **Exceptions** tab tasks:

TABLE 4-10. Exceptions Tasks

TASK	STEPS
Add	1. Click **Add** to add an object. The **Add Exceptions** window appears. 2. Specify the **IP address**, **Domain**, **URL**, **File SHA-1**, or **File SHA-256** exception criteria. • For IP addresses, select **IP address** for the type and then type the IP address or a hyphenated range. • For domains, select **Domain** for the type and then type the domain.

Task	Steps
	Note Wildcards are only allowed in a prefix. When a wildcard is used in a prefix, it must be connected with ". ". Only one wildcard may be used in a domain. For example, *.com will match abc.com or test.com. • For URLs, select **URL** for the type and then type the URL. **Note** • Wildcards are only allowed in a prefix. When a wildcard is used in the domain part of an URL, it must be connected with ". ". Only one wildcard may be used in a URL. For example, http://*.com will match abc.com or test.com. • When an unassigned wildcard is used in the URI part of an URL, it can match all parts. For example, http://abc.com/*abc will match http://abcd.com/test.abc. • Deep Discovery Analyzer accepts both HTTP and HTTPS URLS. • For files, select **File SHA-1** or **File SHA-256** for the type and type the hash value. • **Notes**: Type some notes for the object. • **Add More**: Click this button to add more objects. Select an object type, type the object in next field, type some notes, and then click **Add to List**. 3. (Optional) Type some notes for the object. 4. Click **Add More** to add more objects. a. Specify the **IP address**, **Domain**, **URL**, **File SHA-1**, or **File SHA-256** exception criteria.

Task	Steps
	b. Click **Add to List**. 5. Click **Add** when you have defined all the objects that you wish to add. **Note** Deep Discovery Analyzer supports the addition of up to 25,000 exceptions.
Import	Click **Import** to add objects from a properly-formatted CSV file. In the new window that opens: • If you are importing exceptions for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), browse and then select the CSV file. • If you have imported exceptions previously, save another copy of the CSV file, populate it with new objects, browse and then select the CSV file. **Important** • Importing overwrites the current exception list. However, objects retrieved from integrated products are not modified. To keep a copy of the current exception list, export the list before starting the import process. • A CSV file can import a maximum of 25,000 exceptions.
Delete/Delete All	Select one or several objects to remove and then click **Delete**. Click **Delete All** to delete all the objects.
Export/Export All	Select one or several objects and then click **Export** to save the objects to a CSV file. Click **Export All** to save all the objects to a CSV file.
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type in the **Show** drop-down box.

Task	Steps
	• Select a column name in the **Search column** drop-down box and then type some characters in the **Search keyword** text box next to it. As you type, the entries that match the characters you typed are displayed. Deep Discovery Analyzer searches only the selected column in the table for matches.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of objects. If all the objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

Sandbox Management

The **Sandbox Management** screen includes the following:

- *Status Tab on page 4-52*
- *Images Tab on page 4-54*
- *YARA Rules Tab on page 4-58*
- *File Passwords Tab on page 4-62*
- *Network Connection Tab on page 4-66*
- *Scan Settings Tab on page 4-68*
- *Smart Feedback Tab on page 4-69*
- *Sandbox for macOS Tab on page 4-70*
- *Submission Policies Tab on page 4-71*

Note

If Virtual Analyzer does not contain images, clicking **Sandbox Management** displays the **Images** tab.

Status Tab

The **Status** tab displays the following information:

- Overall status of Virtual Analyzer, including the number of samples queued and currently processing

  Virtual Analyzer displays the following:

TABLE 4-11. Virtual Analyzer Statuses

STATUS	DESCRIPTION
Not initialized	Virtual Analyzer has not been initialized.
No images	No images have been imported into Virtual Analyzer.
Disabled	Virtual Analyzer is temporarily unavailable.
Modifying instances…	Virtual Analyzer is increasing or decreasing the number of instances for one or more images.
Importing images…	Virtual Analyzer is importing one or more images.
Removing images…	Virtual Analyzer is removing one or more images.
Configuring...	Virtual Analyzer is configuring sandbox settings.
Starting...	Virtual Analyzer is starting all sandbox instances.
Running	Virtual Analyzer is analyzing or ready to analyze samples.
Stopping...	Virtual Analyzer is stopping all sandbox instances.
Unrecoverable error	Virtual Analyzer is unable to recover from an error. Contact your support provider for troubleshooting assistance.
Deploying images from Deep Discovery Director...	Virtual Analyzer is deploying images from Deep Discovery Director.

- Status of imported images

TABLE 4-12. Image Information

STATUS	DESCRIPTION
Image	Permanent image name
Instances	Number of deployed sandbox instances

Status	Description
Current Status	Distribution of idle and busy sandbox instances
Utilization	Overall utilization (expressed as a percentage) based on the number of sandbox instances currently processing samples

Images Tab

Virtual Analyzer does not contain any images by default. To analyze samples, you must prepare and import at least one image in the Open Virtual Appliance (OVA) format.

You can use existing VirtualBox or VMware images, or create new images using VirtualBox. For details, see Chapters 2 and 3 of the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Before importing, validate and configure images using the Virtual Analyzer Image Preparation Tool. For details, see Chapter 4 of the *Virtual Analyzer Image Preparation User's Guide*.

The hardware specifications of your product determine the number of images that you can import and the number of instances that you can deploy per image.

You can view the following information on the **Images** screen:

- The number of configured instances for an image
- The number of instances in use

The following table describes the tasks that you can perform on the **Images** screen.

Task	Description
Import an image	Click **Import** to upload a new Virtual Analyzer image. For more information, see *Importing an Image on page 4-55*. **Note** For Linux images, Deep Discovery Analyzer supports CentOS 7.8, RedHat 7.9, and RedHat 8.3 only.
Export an image	Select an image and click **Export**.
Change the image name or the number of sandbox instances	Select an image and click **Modify**. For more information, see *Modifying Sandbox Instances on page 4-57*.
Display entries by platform	Select an option from the **Platform** drop-down list.

Importing an Image

You can import up to four images (one Linux and three Windows images). The hardware specifications of your product determine the number of images that you can import and the number of instances that you can deploy per image.

Virtual Analyzer supports OVA files up to 30GB in size.

Important

Virtual Analyzer stops analysis and keeps all samples in the queue whenever an image is added or deleted, or when instances are modified.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Images** tab.

   The **Images** screen appears.

2. Click **Import**.

   The **Import Image** screen appears.

3. Select a **Platform** option.

4. Select an image source and configure the applicable settings.

   a. Type a permanent image name with a maximum of 50 characters.

   b. Choose the number of instances to allocate for the image.

   c. Type the URL or network share path of the OVA file.

   d. (Optional) Select **Connect through a proxy sever**.

   e. (Optional) Type the logon credentials if authentication is required.

5. Click **Import**.

   Virtual Analyzer validates the OVA files before starting the import process.

Note

- If you selected **HTTP/HTTPS or FTP server**, Deep Discovery Analyzer downloads the images first before importing into Virtual Analyzer. The process can only be canceled before the download completes.
- Deep Discovery Analyzer supports connection to a source HTTP / HTTPS server that complies with HTTP/1.0 or later.

Importing an Image Using the Virtual Analyzer Image Import Tool

Virtual Analyzer supports OVA files that are between 1 GB and 30 GB in size.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Images** tab.

2. Click **Import**.
3. Select a **Platform** option.
4. For **Source**, select **Image import tool**.
5. Click **Download** to download the image import tool.
6. Open the file `VirtualAnalyzerImageImportTool.exe`.
7. Type the IP address for Deep Discovery Analyzer.

   Deep Discovery Analyzer deploys instances immediately after an image uploads. Wait for the instance deployment to complete.

The image import process may stop or be considered unsuccessful because of the following reasons:

- No connection is established. The product may be busy.
- The connection to the appliance was interrupted.
- The connection timed out.
- Memory allocation was unsuccessful.
- Windows socket initialization was unsuccessful.
- The image file is corrupt.
- The image upload did not complete.
- The image upload was cancelled.

Modifying Sandbox Instances

You can import up to four images (one Linux and three Windows images). The hardware specifications of your product determine the number of images that you can import and the number of instances that you can deploy per image.

Important

Virtual Analyzer stops all analysis and keeps all samples in the queue whenever an image is added or deleted, or when instances are modified. All instances are also automatically redistributed whenever you add images.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Images** tab.

   The **Images** screen appears.

2. Click **Modify**.

   The **Modify Sandbox Instances** screen appears.

3. (Optional) Modify the name of an image.

4. Modify the instances allocated to any image.

5. Click **Configure**.

   Virtual Analyzer displays a confirmation message.

6. Click **OK**.

   Virtual Analyzer configures the sandbox instances. Please wait for the process to finish before navigating away from the screen.

   Note

   If configuration is unsuccessful, Virtual Analyzer reverts to the previous settings and displays an error message.

YARA Rules Tab

Virtual Analyzer uses YARA rules to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment. Deep Discovery Analyzer supports a maximum of 5,000 YARA rules regardless of the number of YARA rule files.

The following columns show information about YARA rule files.

TABLE 4-13. YARA Rules columns

COLUMN NAME	INFORMATION
File name	Name of the YARA rule file
Rules	Number of YARA rules contained in the YARA rule file
Files to analyze	File types to analyze using the YARA rules in the YARA rule file
Added	Date and time the YARA rule file was added

The following table lists all the YARA Rules tab tasks:

TABLE 4-14. YARA Rules Tasks

TASK	STEPS
Add	Browse and select a YARA rule file and the file types to analyze. For details, see *Managing YARA Rule Files on page 4-61*.
Delete	Select one or several YARA rule files to remove and then click **Delete**.
Export	Select one YARA rule file, and click **Export** to download a copy of the YARA rule file.
Edit	Click the **File name** of the YARA rule file to be edited. For details, see *Managing YARA Rule Files on page 4-61*.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of YARA rule files. If all samples cannot display at the same time, use the pagination controls to view the samples that are hidden from view.

Creating a YARA Rule File

Deep Discovery Analyzer supports YARA rules that follow version 4.1.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

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

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

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

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

The following example shows a simple YARA rule:

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

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

TABLE 4-15. YARA Rule Parts and Usage

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

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

Managing YARA Rule Files

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management**, and then go to the **YARA Rule** tab.
2. Do one of the following:
   - To add a new YARA rule, click **Add**.

     Virtual Analyzer validates the YARA rule file before adding it. For details about creating valid YARA rule files, see *Creating a YARA Rule File on page 4-59*.

- To edit an existing YARA rule, click the **File name** of the YARA rule file to be edited.

3. Click **Choose File** to browse and select a YARA rule file to add.
4. For **Files to analyze**, do one of the following:
   - Select **Specify file types** and add selected file types that Virtual Analyzer associates with this YARA rule file.
   - Select **All file types** to have Virtual Analyzer associate all file types with this YARA rule file.

Note

Analyzing all file types may cause unintended detections and affect system performance. Trend Micro recommends analyzing specific file types that are targeted by the YARA rule file.

5. Click **Save**.

   After adding a YARA rule file, you can:
   - Click **Export** to download a copy of the selected YARA rule file.
   - Click **Delete** to delete one or more selected YARA rule files.

File Passwords Tab

Always handle suspicious files with caution. Trend Micro recommends adding such files to a password-protected archive file or password-protecting document files from being opened before transporting the files across the network. Deep Discovery Analyzer can also heuristically discover passwords in email messages to extract files.

Deep Discovery Analyzer uses user-specified passwords to extract files or open password-protected documents. For better performance, list commonly used passwords first.

Deep Discovery Analyzer supports the following password-protected archive file types:

- 7z
- alz
- egg
- rar
- zip

Deep Discovery Analyzer supports the following password-protected document file types:

- doc
- docx
- odp
- odt
- ods
- pdf
- ppt
- pptx
- xls
- xlsx

If Virtual Analyzer is unable to extract files using any of the listed passwords, Deep Discovery Analyzer displays the error Unsupported file type.

Note

- File passwords are stored as unencrypted text.
- After you register Deep Discovery Analyzer to Deep Discovery Director, you can only export file passwords on the **File Passwords** screen. Deep Discovery Analyzer automatically synchronizes file password settings from Deep Discovery Director and overwrites existing file password settings that you have configured.

The following table describes the tasks that you can perform on the **File Passwords** screen.

Task	Description
Add a password	Click **Add Password** to add a password to the list. For more information, see *Adding File Passwords on page 4-64*.
Import passwords	Click **Import Passwords** to import passwords from a selected file.
Export all passwords	Click **Export All** to export all file passwords and save the file on your computer.

Adding File Passwords

Deep Discovery Analyzer supports a maximum of 100 passwords.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **File Passwords** tab.
2. Click **Add Password**.
3. Type a password.

Note

Passwords are case-sensitive.

4. Optional: Click **Add Password** and type another password.
5. Optional: Drag and drop the password to move it up or down the list.
6. Optional: Delete a password by clicking the x icon beside the corresponding text box.
7. Click **Save**.

Importing File Passwords

You can add up to 100 passwords in Deep Discovery Analyzer.

Note

Importing passwords from a file replaces the existing passwords in Deep Discovery Analyzer. Before you import passwords, it is recommended you use the export feature to back up the existing passwords.

Procedure

1. Go to **Sandbox Management** > **File Passwords**.

   The **File Passwords** screen appears.
2. Click **Import Passwords**.

   The **Import Passwords** window appears.
3. Browse and select the file to import.

   Note

   Click **Download sample file** to view a sample of a properly formatted file.

   Deep Discovery Analyzer checks the entries in the selected file to identify any invalid or duplicate passwords.
4. Click **Import**.

Network Connection Tab

Use the **Network Connection** tab to specify how sandbox instances connect to external destinations.

External connections are disabled by default. Trend Micro recommends enabling external connections using an environment isolated from the management network. The environment can be a test network with Internet connection but without proxy settings, proxy authentication, and connection restrictions.

When external connections are enabled, any malicious activity involving the Internet and remote hosts actually occurs during sample processing.

Enabling External Connections

Sample analysis is paused and settings are disabled whenever Virtual Analyzer is being configured.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Network Connection** tab.

   The **Network Connection** screen appears.

2. Select **Enable external connections**.

   The settings panel appears.

3. Select the type of connection to be used by sandbox instances.

   - Custom: Any user-defined network

     Important

     Trend Micro recommends using an environment isolated from the management network.

   - Management network: Default organization Intranet

WARNING!

Enabling connections to the management network may result in malware propagation and other malicious activity in the network.

4. If you selected **Custom**, specify the following:
   - Network adapter: Select an adapter with a linked state.
   - IP address: Type an IPv4 address.
   - Subnet mask
   - Gateway
   - DNS
5. If the sandbox requires a proxy server for network connection, select **Use a dedicated proxy server**, and specify the following.
   - Server address
   - Port
   - User name: This option is only available if **Proxy server requires authentication** is enabled.
   - Password: This option is only available if **Proxy server requires authentication** is enabled.
6. Click **Save**.

Testing Internet Connectivity

Verify Internet connectivity after enabling the external connection and configuring the settings.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Network Connection** tab.
2. Click **Test Internet Connectivity**.

Note

Test Internet Connectivity will be disabled if external connections are not enabled or the settings are not saved.

Scan Settings Tab

You can use the **Scan Settings** tab in **Virtual Analyzer** > **Sandbox Management** to enable Virtual Analyzer to analyze samples using suspicious objects that are synchronized from Trend Vision One or Deep Discovery Director.

Note

To enable this scan setting, you must also configure Deep Discovery Analyzer to synchronize suspicious objects from Trend Vision One or Deep Discovery Director.

For more information, see *Trend Vision One Tab on page 6-10* or *Registering to Deep Discovery Director on page 6-18*.

Interactive Mode Tab

You can configure advanced settings for VNC access.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Interactive Mode** tab.
2. Type a password that contains at least 8 characters and includes uppercase letters, lowercase letters, numbers, and special characters.

   Leave this field empty if you do not want to set the password.

   Note

   If you forget the password you specify, you must reset it.

3. Specify the port range.

Note

The starting port number must be between 5900 and 6100.

4. Click **Save**.

Smart Feedback Tab

Deep Discovery Analyzer integrates the new Trend Micro Feedback Engine. This engine sends threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence.

Information collected by Smart Feedback:

- Product ID and version
- URLs suspected to be fraudulent or possible sources of threats
- Metadata of detected files (file type, file size, SHA-1 hash value, and SHA-1 hash value of parent file)
- Detection logs (from Advanced Threat Scan Engine, Predictive Machine Learning engine, and Virtual Analyzer)
- Sample of the following detected file types: bat, class, cmd, dll, exe, htm, html, jar, js, lnk, macho, mov, ps1, svg, swf, url, vbe, vbs, wsf
- Macros in Microsoft Office files

Enabling Smart Feedback

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Smart Feedback** tab.
2. Configure Smart Feedback settings.

a. Select **Enable Smart Feedback (recommended)** to send protected threat information to Trend Micro from your network.

b. Select **Submit suspicious files to Trend Micro** to send high-risk files to Trend Micro for further investigation.

Sandbox for macOS Tab

Enable **Sandbox for macOS** to allow Deep Discovery Analyzer to send possible Mac OS threats to the Trend Micro **Sandbox for macOS** service for analysis.

Enabling Sandbox for macOS

Before enabling the **Trend Micro Sandbox for macOS**, verify that Deep Discovery Analyzer has an Internet connection.

Note

In a cluster environment, the **Trend Micro Sandbox for macOS** setting does not propagate from the primary appliance. Enable the **Trend Micro Sandbox for macOS** setting on the management console of each secondary appliance.

Important

The **Trend Micro Sandbox for macOS** setting is automatically disabled if the Deep Discovery Analyzer license expires.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Sandbox for macOS** tab.
2. Select **Send possible threats for macOS to Sandbox as a Service for analysis**.
3. Click **Save**.

Submission Policies Tab

You can configure sample submission policies that set Deep Discovery Analyzer to analyze samples using a specified Virtual Analyzer image based on the following:

- File type or extension
- Submitters

Note

For information on how Deep Discovery Analyzer matches and applies submission policies, see *Submission Policy Matching on page 4-84*.

The following table describes the information on the **Submission Policies** screen.

Field	Description
Policy Name	Name of the submission policy
Description	Additional information about the submission policy
Submitters	One or more submitters that are associated with the submission policy
Image	Name of the image that is associated with the submission policy
Created	Time and date the submission policy was created
Status	Toggle to enable or disable the submission policy

The following table lists all the tasks you can perform on the **Submission Policies** screen.

TASK	DESCRIPTION
Add a submission policy	Click **Add** to add a submission policy. For more information, see *Configuring a Submission Policy on page 4-72*. **Important** Before you can create a submission policy, import one or more images. For more information, see *Importing an Image on page 4-55*.
Edit a submission policy	Click a policy name to edit the settings. For more information, see *Configuring a Submission Policy on page 4-72*.
Delete a submission policy	Select one or more entries and click **Delete** and click **OK** to confirm.
Create a copy of a submission policy	Select the submission policy you want to copy and click **Duplicate**.
Enable or disable a submission policy	Click the toggle switch in the **Status** field to enable or disable a submission policy
Search for a submission policy	Type a keyword in the text field and press [Enter] to search. **Note** You can also filter the entries by submitter and image type.

Configuring a Submission Policy

Important

Before you can create a submission policy, import one or more images. For more information, see *Importing an Image on page 4-55*.

Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Submission Policies** tab.
2. Do one of the following:
   - Click **Add** to create a new submission policy.
   - Click a policy name to edit the settings.

   Note

   Some settings in the default policy are not configurable.
3. Click the **Status** toggle to enable or disable the submission policy.
4. Type a policy name.
5. Type a description for the policy.
6. Specify the submitters for the policy. Select one or more entries from the **Submitters** drop-down list.
7. Under **Submission Rules**, configure the submission settings.
   a. Do one of the following:
      - Click **Add** to create a new entry.
      - Click an image name to edit the settings.

   b. Select an image.

   c. For **Submission Settings**, select one of the following options and configure the required settings:
      - **Specify**: Select this option to specify the file types to analyze.

      Tip

      Click **>>** or **<<** to move the selected entries between the lists.

- **Use the submission settings of another image**: Select this option to use the same submission settings from the image you select.

  Note

  - You can only share submission settings between images with the same platform. For example, a Windows 7 image can use the submission settings from a Windows 10 image but not from a Red Hat 7.x image.
  - In the drop-down list that appears, the system displays only images with the same platform type in the list.

a. Click **Save**.

b. (Optional) Repeat the steps to create more submission rules for the policy.

8. Click **Save**.

Tip

For information on how Deep Discovery Analyzer matches and applies submission policies, see *Submission Policy Matching on page 4-84*.

Supported File Types in Virtual Analyzer

This section provides the list of file types that Virtual Analyzer supports. Trend Micro identifies files by true file type and not by extension. Sample file extensions are provided for reference.

Note

Updates to the Virtual Analyzer Configuration Pattern may also include added support for new file types. After the update, Virtual Analyzer places new file types in the **Analyzed** list.

TABLE 4-16. Virtual Analyzer File Types: Windows

DISPLAYED FILE TYPE	FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
bat	Microsoft™ Windows™ batch file	.bat
cmd	Microsoft™ Windows™ command script file	.cmd
cell	Hancom™ Hancell spreadsheet	.cell
chm	Compiled HTML (CHM) help file	.chm
csv	Comma-separated values (CSV) file	.csv
class	Java™ Class file	.class .cla
com	Microsoft™ Windows™ executable file	.com
dll	AMD™ 64-bit DLL file Microsoft™ Windows™ 16-bit DLL file Microsoft™ Windows™ 32-bit DLL file	.dll .ocx .drv
doc	Microsoft™ Word™ 1.0 document Microsoft™ Word™ 2.0 document	.doc .dot
docx	Microsoft™ Office Word™ (2007 or later) document Microsoft™ Office Word™ (2007 or later) macro-enabled document	.docx .dotx .docm .dotm

Displayed File Type	Full File Type	Example File Extensions

exe	AMD™ 64-bit EXE file
	ARJ compressed EXE file
	ASPACK 1.x compressed 32-bit EXE file
	ASPACK 2.x compressed 32-bit EXE file
	DIET DOS EXE file
	GNU UPX compressed EXE file
	IBM™ OS/2 EXE file
	LZEXE DOS EXE file
	LZH compressed EXE file
	LZH compressed EXE file for ZipMail
	MEW 0.5 compressed 32-bit EXE file
	MEW 1.0 compressed 32-bit EXE file
	MEW 1.1 compressed 32-bit EXE file
	Microsoft™ Windows™ 16-bit EXE file
	Microsoft™ Windows™ 32-bit EXE file
	MIPS EXE file
	MSIL Portable executable file
	PEPACK compressed executable
	PKWARE™ PKLITE™ compressed DOS EXE file
	PETITE compressed 32-bit executable file
	PKZIP compressed EXE file
	WWPACK compressed executable file
		`.cpl`
		`.exe`
		`.sys`
		`.crt`
		`.scr`

gul	JungUm™ Global document	`.gul`
hta	HTML Application file	`.hta`

Displayed File Type	Full File Type	Example File Extensions
html	Hypertext Markup Language (HTML) file	.htm .html
hwp	Hancom™ Hangul Word Processor (HWP) document	.hwp
hwpx	Hancom™ Hangul Word Processor (2014 or later) (HWPX) document	.hwpx
iqy	Microsoft Excel Web Query File	.iqy
jar	Java™ Applet Java™ Application **Note** Virtual Analyzer does not support the java library.	.jar
js	JavaScript™ file	.js
jse	JavaScript™ encoded script file	.jse
jtd	JustSystems™ Ichitaro™ document	.jtd
lnk	Microsoft™ Windows™ Shell Binary Link shortcut Microsoft™ Windows™ 95/NT shortcut	.lnk
mht mhtml	Web page archive file	.mht .mhtml
mov	Apple QuickTime media	.mov
msi	Microsoft™ installer package	.msi
odt	OpenDocument Text	.odt
odp	OpenDocument Presentation	.odp
ods	OpenDocument Spreadsheet	.ods

Displayed File Type	Full File Type	Example File Extensions
pdf	Adobe™ Portable Document Format (PDF)	.pdf
ppt	Microsoft™ Powerpoint™ presentation	.ppt .pps
pptx	Microsoft™ Office PowerPoint™ (2007 or later) presentation Microsoft™ Office PowerPoint™ (2007 or later) macro-enabled presentation	.pptx .ppsx
ps1	Microsoft™ Windows™ PowerShell script file	.ps1
pub	Microsoft™ Office Publisher™ (2016) file	.pub
rtf	Microsoft™ Rich Text Format (RTF) document	.rtf
shtml	Server-parsed HyperText Markup Language	.shtml
slk	Microsoft™ symbolic link format	.slk
svg	Scalable Vector Graphics file	.svg
swf	Adobe™ Shockwave™ Flash file	.swf
vbe	Visual Basic™ encoded script file	.vbe
vbs	Visual Basic™ script file	.vbs
wsf	Microsoft™ Windows™ Script File	.wsf
xls	Microsoft™ Excel™ spreadsheet	.xls .xla .xlt .xlm

Displayed File Type	Full File Type	Example File Extensions
xlsx	Microsoft™ Office Excel™ (2007 or later) spreadsheet Microsoft™ Office Excel™ (2007 or later) macro-enabled spreadsheet	.xlsx .xlsb .xltx .xlsm .xlam .xltm
xml	Microsoft™ Office 2003 XML file Microsoft™ Word™ 2003 XML document Microsoft™ Excel™ 2003 XML spreadsheet Microsoft™ PowerPoint™ 2003 XML presentation	.xml
xht xhtml	Extensible Hypertext Markup Language	.xht .xhtml
url	Internet shortcut file	.url

Note

For the following script types, Virtual Analyzer does not perform an analysis if the file extension and file type do not match:

- bat
- cmd
- csv
- hta
- htm
- html
- iqy
- js
- jse
- mht
- mhtml
- ps1
- shtml
- slk
- svg
- url
- vbe
- vbs
- wsf
- xht
- xhtml
- xls

TABLE 4-17. Virtual Analyzer File Types: Linux

DISPLAYED FILE TYPE	FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
elf	ELF Executable	N/A
sh	Shell script	.sh

Virtual Analyzer can scan files that match the supported file types in an archive file that is not password protected. The following table lists the supported archive file types.

Note

For the list of password-protected archive files that Virtual Analyzer can analyze, see *File Passwords Tab on page 4-62*.

TABLE 4-18. Archive file types

TRUE FILE TYPE	FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
7ZIP	7-zip archive	.7z
ACE	WinAce archive	.ace
ALZ	ALZip archive	.alz
AMG	Fujitsu AMG archive	.amg
APK	Google™ Android™ Application Package (APK)	.apk
ARJ	ARJ archive	.arj
BINHEX	BinHex file	.hqx
BZIP2	BZIP2 archive	.bz2 .bzip2
CAB	Microsoft™ Cabinet file	.cab
CRX	Chrome Extension Format (CRX)	.crx

True File Type	Full File Type	Example File Extensions
EGG	ALZip archive	.egg
GZIP	GNU ZIP archive	.gzip .gz
ISO	ISO image	.iso
LHA	LHARC compressed archive	.lha .lharc
LZW	Lempel-Ziv-Welch (LZW) Compressed Amiga archive	.lzh
MACBIN	Apple™ MacBinary file	.bin.macbin
MIME	Multipurpose Internet Mail Extensions (MIME) Base64 file	.eml .email
MSG	Microsoft™ Outlook™ Item	.msg
MSI	Microsoft™ installer package	.msi
MSCOMP	Microsoft™ compressed files	.arc
RAR	Roshal Archive (RAR) archive	.rar
SIS	Symbian™ Installation file	.sis
SIT	Smith Micro™ StuffIt archive	.sit .sitx
TAR	TAR archive	.tar .tgz
TNEF	Microsoft™ Outlook™ Transport Neutral Encapsulation Format (TNEF) file	.tnef .winmail.dat .win.dat
UUCODE	Uuencode file	.uue

True File Type	Full File Type	Example File Extensions
WIM	Microsoft™ Windows Image (WIM)	`.wim`
XZ	XZ archive	`.xz`
ZIP	PKWARE PKZIP archive (ZIP)	`.zip`

The following table lists the Mac file types that Deep Discovery Analyzer automatically submits to Sandbox for MacOS for analysis, regardless of the submission settings.

Note

Deep Discovery Analyzer submits JAR and CLASS files to both Sandbox for MacOS and the internal Virtual Analyzer for analysis.

Table 4-19. Virtual Analyzer File Types: Mac

True File Type	Full File Type	Example File Extensions
DMG	Apple disk image file	`.dmg`
JAR	Java™ Applet Java™ Application **Note** Virtual Analyzer does not support the java library.	`.jar`
CLASS	Java™ Class file	`.class` `.cla`
PKG	Mac OS X installation file	`.pkg`
Mach-O	Mach object file	`.o`

Submission Policy Matching

The following describes the submission policy matching guidelines in Deep Discovery Analyzer:

- File samples:
  - For single file samples, Deep Discovery Analyzer analyzes the samples using the Virtual Analyzer image specified in the matched policy. If no match is found, the default policy applies.
  - For archive samples:
    - If extracted files match a submission policy and the default policy, Deep Discovery Analyzer uses the Virtual Analyzer image specified in the matched policy and the default policy to analyze files.
    - If some extracted files match a policy and no policy match is found for other files in the same archive sample, Deep Discovery Analyzer applies the matched policy.
    - If some extracted files match the default policy and no policy match is found for other files in the same archive sample, Deep Discovery Analyzer applies the default policy.
    - If no policy match is found for all extracted files in an archive sample, Deep Discovery Analyzer applies the default policy with the unsupported analysis result (displayed as a gray icon ( ) in the **Risk Level** field on the **Submissions** screen).
- URL samples:
  - With prefilter scanning:
    - If the prefilter scan result is non-malicious, Deep Discovery Analyzer does not apply any policies nor analyze the sample using a specific Virtual Analyzer image.
    - If the prefilter scan result is potentially malicious, Deep Discovery Analyzer analyzes the samples using the Virtual Analyzer image specified in the matched policy by submitter

(not by file type). If no match is found, the default policy applies.

- If URL samples link to downloadable files, Deep Discovery Analyzer analyzes the downloaded file samples using the Virtual Analyzer image specified in the matched policy. If no match is found, the default policy applies.

- Without prefilter scanning:

  Deep Discovery Analyzer analyzes the samples using the Virtual Analyzer image specified in the matched policy by submitter (not by file type). If no match is found, the default policy applies.

Note

If the Trend Micro Sandbox for macOS service is enabled for supported Mac file type, Deep Discovery Analyzer sends samples to Sandbox for macOS for analysis and includes the result in the analysis report.

For example, Deep Discovery Analyzer contains three submission policies listed in the following table.

TABLE 4-20. Submission policy examples

POLICY NAME	SUBMITTER	FILE TYPE	IMAGE
Policy A	Deep Discover Inspector	EXE	Windows 7
		CSV	Windows XP
Policy B	Apex One	PPT	Windows 10
Default	Any	• SH • ELF	CentOS 7

Policy Name	Submitter	File Type	Image
		• EXE • CSV • PPT • DOC • PDF	• Windows 8 • Windows 10

Note

- Deep Discovery Analyzer automatically adds the EXE, CSV, and PPT file types to the default policy based on the user-defined policies (Policy A and Policy B).
- If the default policy is the only policy matched, Deep Discovery Analyzer analyzes the SH and ELF files using the CentOS 7 image. Any supported Windows file types are analyzed using the Windows images.

The following table shows the matched policies and the Virtual Analyzer image used for samples submitted to Deep Discovery Analyzer.

Table 4-21. Policy matching result examples

Sample	File Type	Submitter	Matched Policy	Image Used
File	EXE	Deep Discovery Inspector	Policy A	Windows 7
	CSV	Deep Discovery Inspector	Policy A	Windows XP
	EXE	Apex One	Default	• Windows 8 • Windows 10
	PPT	Apex One	Policy B	Windows 10
	SH	Apex One	Default	CentOS 7

Sample	File Type	Submitter	Matched Policy	Image Used
Archive	ZIP (EXE)	Deep Discovery Inspector	Policy A	Windows 7
	ZIP (EXE and CSV)	Deep Discovery Inspector	Policy A	• Windows 7 • Windows XP
	ZIP (EXE, CSV, DOC, and PDF)	Deep Discovery Inspector	Policy A	• Windows 7 • Windows XP
			Default	• Windows 8 • Windows 10
	ZIP (EXE, DOC, and PDF)	Deep Discovery Inspector	Policy A	Windows 7
			Default	• Windows 8 • Windows 10
	HTML	Deep Discovery Inspector	Default	• Windows 8 • Windows 10 Result: Unsupported
	ZIP (EXE and HTML)	Deep Discovery Inspector	Policy A	Windows 7
	ZIP (EXE, CSV, DOC, and PDF)	Apex One	Default	• Windows 8 • Windows 10
URL (from prefilter with no policy matching)	Not applicable	Any	Not applicable	All images
URL (without file samples)	Not applicable	Deep Discovery Inspector	Policy A	• Windows 7 • Windows XP

Sample	File Type	Submitter	Matched Policy	Image Used
	Not applicable	ScanMail for Microsoft Exchange	Default	• Windows 8 • Windows 10
URL (with file samples)	EXE	Deep Discovery Inspector	Policy A	Windows 7
	ZIP (EXE, DOC, and PDF)	Deep Discovery Inspector	Policy A	Windows 7
			Default	• Windows 8 • Windows 10

Submitters

Use the **Submitters** screen, in **Virtual Analyzer** > **Submitters**, to adjust Virtual Analyzer resource allocation between all sources that submit objects to Deep Discovery Analyzer for analysis. Virtual Analyzer utilizes more resources to process submissions by submitters with higher weight settings.

The following columns show information about submitters, average processing time, total submissions, and total resources allocated to submitters. Columns for the adjustment of weight and removal of submitters are provided as well.

Table 4-22. Submitters Columns

Column Name	Information / Action
Submitter	Name of the Trend Micro product that submits the objects
Host Name	• Host name of the integrated security product that submitted the objects • No data (indicated by a dash) for email or manual submissions • IP address of the ICAP clients • Name of the network share
Last Submission	Date and time Virtual Analyzer last received a submission

Column Name	Information / Action
Average Processing Time	Average time it takes Virtual Analyzer to process a submitted object
Submissions (% of Total)	Number of objects submitted by the Trend Micro product
Weight	Weight setting of the Trend Micro product Specify a value between 1 and 100 to recalculate resource allocation.
% of Total Resources	Percentage of total Virtual Analyzer resources allocated to the Trend Micro product.
Timeout	Timeout period allotted for the Trend Micro product Specify a timeout period from 0 to 10000 minutes. A value of 0 means timeout is disabled. The number of samples affected by the timeout period for the past 24 hours is summarized in the **Count** column.
Action	Deletes the Trend Micro product from Deep Discovery Analyzer Deleted products cannot submit new objects for scanning and analysis or query analysis results, but queued objects will be processed and analysis results will be stored. **Note** To reintegrate the product, see *Integration with Trend Micro Products and Services on page 2-6*.

Network Shares

With network share scanning, Deep Discovery Analyzer scans files on network shares to detect and prevent potential malicious files from propagating in your network environment.

The following table describes the information on the **Network Shares** screen.

Field	Description
Share name	Name of the network share
Description	Additional information about the network share
Storage service	Storage service for the network share
Server address	Server IP address or FQDN for the network share
Path	Location of the network share
Scheduled scan	Scheduled scan settings for the network share
Scan results	Scan results of the most recent network share scan. Click a number to view detailed scan results. **Note** If a scan is in progress, the system automatically updates the scan results every 10 seconds.
Scan status	Status of the last network share scan If a scan is still in progress, you can click **Stop** to terminate the scan task.
Manual scan	Click **Scan** to start a manual scan
Network status	Connection status (**Accessible** or **Inaccessible**) for the network share
Status	Toggle to enable or disable the scan settings for the network share **Note** If you disable the scan settings for a network share, the system disables the manual scan function and the scheduled scan settings do not take effect.

The following table describes the tasks you can perform on the **Network Shares** screen.

TABLE 4-23. Network Shares: Tasks

TASK	DESCRIPTION
Add a network share	Click **Add** to add a network share. For more information, see *Configuring a Network Share on page 4-92*.  **Tip** After you add a network share, you can access the **Submitters** screen to view the associated sample submissions and adjust the weight value (the default is 4) for Virtual Analyzer resource allocation.
Test the connection to a network share	Click a network share name and click **Test Connection**. Check the test result in the **Network status** field on the **Network Shares** screen.
Edit a network share	Click a network share name to edit the settings. For more information, see *Configuring a Network Share on page 4-92*.  **Note** You cannot edit the settings of a network share If a scan for the network share is in progress.
Delete a network share	Select one or more entries and click **Delete** and click **OK** to confirm.
Stop a scan	When a scan is in progress, click **Stop** in the **Scan status** field.
Start a manual scan	Click **Scan** in the **Manual scan** field to start a scan.
Enable or disable network share configuration	Click the toggle switch in the **Status** field to enable or disable network share configuration

Task	Description
Viewing scan results	In the **Scan results** field: • **Scanned**: Click the number to view information on successful scans on the **Submissions** screen. • **Unsuccessful**: Click the number to view information on the **Unsuccessful Scans** screen. For more information, see *Viewing Unsuccessful Scans on page 4-99*.

Configuring a Network Share

Procedure

1. Go to **Virtual Analyzer** > **Network Shares**.
2. Do one of the following:
   - Click **Add** to configure a new network share.
   - Click a network share name to change the settings.
3. Click the **Status** toggle to enable or disable the network share configuration.
4. Type a descriptive name for the network share.
5. Type additional information for the network share.
6. Select a storage service and configure the required settings.
   - **NFS** or **CIFS** storage service

Field	Description
Server address	Type the IP address or fully qualified domain name (FQDN) of the network share server. **Note** Make sure the network share server uses UTF-8 encoding to allow Deep Discovery Analyzer to perform sample analysis and display the server address properly.
Path	Type the network share path (for example, `/Users/Shares/Website`).
User name	Type the user name to access the network share. For domain users, type the user name in the format `domain_name\user_name`.
Password	Type the password to access the network share.

- **AWS S3** storage service

Note

- Enabling network share scanning for AWS S3 may incur additional data transfer cost.
- Configure the required permissions for Deep Discovery Analyzer to access the AWS S3 storage service for network share scanning.

Field	Description
Server address	This field displays the server address for the storage service.

Field	Description
Path	Type the bucket name or bucket folder path (for example, `my_bucket` or `my_bucket/my_folder/../`). **Note** You must specify at least the bucket name in the path.
Access key ID	Type the access key ID that Deep Discovery Analyzer uses to access AWS S3.
Secret access key	Type the secret access key that Deep Discovery Analyzer uses to access AWS S3.
Proxy setting	If a proxy server is required for Deep Discovery Analyzer to connect to AWS S3, select **Connect using system proxy server** or **Connect using custom proxy setting** and configure the required settings.

- **Azure Blob** storage service

Note

- Enabling network share scanning for Azure Blob may incur additional data transfer cost.
- Configure the required permissions for Deep Discovery Analyzer to access the Azure Blob storage service for network share scanning.

Field	Description
Server address	This field displays the server address for the storage service.

Field	Description
Path	Type the container name or the container folder path (for example, `my_container` or `my_container/my_folder/../`). **Note** You must specify at least the container name in the path.
Account name	Type the account name that Deep Discovery Analyzer uses to access Azure Storage.
Access key	Type the access key that Deep Discovery Analyzer uses to access Azure Storage.
Proxy setting	If a proxy server is required for Deep Discovery Analyzer to connect to Azure Blob, select **Connect using system proxy server** or **Connect using custom proxy setting** and configure the required settings.

7. For file matching, configure file name patterns that Deep Discovery Analyzer uses to filter files for scanning. Do the following:

   a. Select to match files based on the inclusion or exclusion list.

   Note
   If you select to use both lists for file name matching, the exclusion list has a higher priority.

   b. Type one or more file name pattern for the selected list.

Note

- File name patterns are not case sensitive.
- Deep Discovery Analyzer supports the following wildcards in file name patterns:
  - `*`: Matches all
  - `?`: Matches any single character
  - `[seq]`: Matches any character in `seq`
  - `[!seq]`: Matches any character not in `seq`
- You can configure up to 10 file name patterns in a list.
- The same file name pattern cannot exist in both inclusion and exclusion lists.
- Deep Discovery Analyzer scans files that match the selected file name pattern list.

8. Specify the scan action.

Action	Description
Do not move files after scanning	Select this option to keep the files in the original folder after scanning. This is the default setting. **Note** To have Deep Discovery Analyzer automatically create the `output_ddan` output folder, select the **Copy analysis report to output folder** option.

Action	Description
Move files	Select this option to move files to the specified output location after scanning. Select one of the following options: • **Destination path**: Select this option to move a detected file to a sub-folder in the destination path you specify. The system automatically creates the sub-folder for each risk level in the destination path. • **Destination path by risk level**: Select this option and specify the destination path for each risk level to move detected files. To access the output path using the same access credentials as the network share, select **Inherit credentials from network share**; otherwise, specify the access credentials for the output path. **Note** • The output path and the network share path cannot be the same. • Make sure read-write permissions are set on the output location. • Files in the output path are excluded from scanning.
Delete files with the selected risk level(s) after scanning	Select this option to delete files with the selected risk levels after scanning. **Note** To have Deep Discovery Analyzer automatically create the `output_ddan` output folder, select the **Copy analysis report to output folder** option.

Deep Discovery Analyzer stores the following generated files in the output folder (which is excluded from scanning):

- Report files (with the file naming convention `id_filename_report.zip`)

- Report metadata files (with the file naming convention `id_filename.meta`) that contain the original file path information for scanned files.

9. Select a scan method.

Note

This setting is not applicable if you select the option to move files after scanning.

- **Quick scan**: Select this option to only scan files that are modified since the last scan. This is the default setting.
- **Full scan**: Select this option scan all files.

Note

- For the first quick scan, Deep Discovery Analyzer performs a full scan and scans only modified files in subsequent quick scans.
- If you switch from **Full scan** to **Quick scan**, Deep Discovery Analyzer scans only modified files after the previous full scan is completed.

10. Specify other scan settings.

- **Rename detected files**: Select this option to rename detected files to prevent accidental execution of malicious files.

  Deep Discovery Analyzer renames detected files in the format `id_<original filename>.vir`.

  For example, if the original file name is `test`, the renamed file becomes `56_test.vir`.

- **Copy analysis report to output folder**: Select this option to create a copy of the analysis report to the output folder.

Note

If you enable a scan setting, make sure read-write permissions are set on the output location.

11. Configure scheduled scan settings. Do the following:
    a. Click the toggle button to enable or disable scheduled scan.
    b. Select a schedule option and configure the required settings.

Note

If you select **Full scan**, you can only configure a weekly or monthly schedule.

12. (Optional) Click **Test Connection** to test the connection to the network share.
13. Click **Save**.

Tip

After you add a network share, you can access the **Submitters** screen to view the associated sample submissions and adjust the weight value (the default is 4) for Virtual Analyzer resource allocation.

Viewing Unsuccessful Scans

You can view the list of files that Deep Discovery Analyzer cannot scan on the **Unsuccessful Scans** screen.

Note

Deep Discovery Analyzer will attempt to scan the files again in the next scheduled or on-demand scan.

To display the **Unsuccessful Scans** screen, go to **Virtual Analyzer** > **Network Shares** and click the number next to **Unsuccessful** in the **Scan results** field.

You can use the search function or filter entries (by file name, path, network share name, error type, or event logged time).

The following table describes the information on the **Unsuccessful Scans** screen.

Field	Description
File name	View the name of the file that Deep Discovery Analyzer cannot scan successfully
Share name	View the name of the network share
Path	View the location of the file on the network share
Error type	View the scan error type
Event logged	View the time the event was detected

Chapter 5

Alerts and Reports

This chapter describes the features of **Alerts** and **Reports**.

Alerts

The **Alerts** screen includes the following:

- Triggered Alerts Tab
- Rules Tab

Triggered Alerts Tab

The **Triggered Alerts** tab, in **Alerts / Reports** > **Alerts**, shows all alert notifications generated by Deep Discovery Analyzer. Alert notifications provide immediate intelligence about the state of Deep Discovery Analyzer.

The following columns show information about alert notifications created by Deep Discovery Analyzer:

TABLE 5-1. Triggered Alerts Columns

COLUMN NAME	INFORMATION
Triggered	Date and Time Deep Discovery Analyzer triggered the alert notification.
Level	Level of the triggered alert notification. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **Informational**: The event requires limited observation
Rule	Rule that triggered the alert notification.
Affected Appliance	Host name, IPv4 and IPv6 addresses of the appliance affected by the alert notification content, if applicable.
Details	Click the icon to view the full alert notification details, including the list of notification recipients, subject, and message of the alert notification.

Rules Tab

The **Rules** tab, in **Alerts / Reports** > **Alerts**, shows all alert notification rules used by Deep Discovery Analyzer.

The following columns show information about the alert notification rules used by Deep Discovery Analyzer:

TABLE 5-2. Rules Columns

COLUMN NAME	INFORMATION
Alert Level	Level of the alert notification rule. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **Informational**: The event requires limited observation
Rule	Rule that triggers the alert notification.
Criteria	Description of the alert rule.
Alert Frequency	Frequency at which the alert notification is sent if threshold is reached or exceeded.
Status	Click the toggle to enable or disable the rule.

The threshold to trigger each alert is configurable. For details, see *Modifying Rules on page 5-6*

Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention. Deep Discovery Analyzer considers malfunctioning sandboxes and appliances as critical problems.

TABLE 5-3. Critical Alerts

NAME	CRITERIA (DEFAULT)	ALERT FREQUENCY (DEFAULT)
Virtual Analyzer Stopped	Virtual Analyzer encountered an error and was unable to recover. Analysis has stopped.	Immediate
Passive Primary Appliance Activated	The active primary appliance encountered an error and was unable to recover. The passive primary appliance took over the active role.	Immediate

Name	Criteria (Default)	Alert Frequency (Default)
License Expiration	License is about to expire or has expired.	Immediate

Important Alerts

The following table explains the important alerts triggered by events that require observation. Deep Discovery Analyzer considers suspicious object detections, hardware capacity changes, certain sandbox queue activity, component update, account and clustering issues as important problems.

Table 5-4. Important Alerts

Name	Criteria (Default)	Alert Frequency (Default)
Account Locked	An account was locked because of multiple unsuccessful logon attempts.	Immediate
Long Virtual Analyzer Queue	The number of Virtual Analyzer submissions has exceeded the threshold of 100.	Once every 30 minutes
Component Update Unsuccessful	A component update was unsuccessful.	Once every 30 minutes
High CPU Usage	The average CPU usage in the last 5 minutes has exceeded the threshold of 90%.	Once every 30 minutes
High Memory Usage	The average memory usage in the last 5 minutes has exceeded the threshold of 90%.	Once every 30 minutes
High Disk Usage	Disk usage has exceeded the threshold of 85%.	Once every 30 minutes
Secondary Appliance Unresponsive	A secondary appliance in the cluster encountered an error and was unable to recover.	Immediate

Name	Criteria (Default)	Alert Frequency (Default)
High Availability Suspended	The passive primary appliance encountered an error and was unable to recover. High availability was suspended.	Once every 30 minutes
New High-Risk Objects Identified	The number of new high-risk objects identified during the last 30 minutes has reached the threshold of 10.	Immediate
Connection Issue	Unable to establish connection to a required resource.	Once every 30 minutes
Long Virtual Analyzer Processing Time	The Virtual Analyzer processing time has exceeded the threshold of 30 minutes.	Once every 30 minutes
Network Share Inaccessible	A network share is inaccessible.	Once every 30 minutes

Note

Consider decreasing the number of sandbox instances if the system frequently experiences high CPU or memory usage for long periods of time.

For details, see *Modifying Sandbox Instances on page 4-57*.

Informational Alerts

The following table explains the alerts triggered by events that require limited observation. Deep Discovery Analyzer considers restoration of high availability, and inaccessibility of syslog and backup servers as informational events.

TABLE 5-5. Informational Alerts

NAME	CRITERIA (DEFAULT)	ALERT FREQUENCY (DEFAULT)
Syslog Server Inaccessible	The syslog server was inaccessible. Logs were not sent to the server.	Once every 30 minutes
Backup Server Inaccessible	The backup server was inaccessible. Logs and objects were not backed up.	Once every 30 minutes
High Availability Restored	The passive primary appliance recovered from an error and high availability was restored.	Immediate

Modifying Rules

Before you begin

Configure the SMTP server to send notifications. For details, see *SMTP Tab on page 6-55*.

All triggered alert rules can notify recipients with a custom email message. Some rules have additional parameters, including object count, submission count, or time period. Trend Micro recommends adding at least one notification recipient for all critical and important alerts.

Procedure

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

   The **Rules** screen appears.

2. Click the name of an alert rule under the **Rule** column.

   The alert rule configuration screen appears.

3. Modify the rule settings.

   Note

   For details, see *Alert Notification Parameters on page 5-7*.

4. Click **Save**.

Alert Notification Parameters

All triggered alert rules can notify recipients with a custom email message. Some rules have additional parameters, including object count, submission count, or time period.

Critical Alert Parameters

Note

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-24*.

TABLE 5-6. Virtual Analyzer Stopped

PARAMETER	DESCRIPTION
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%ConsoleURL%`

Parameter	Description
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-7. Passive Primary Appliance Activated

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PasssiveApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-8. License Expiration

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.

Parameter	Description
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %LicenseType% • %LicenseStatus% • %ExpirationDate% • %DaysBeforeExpiration% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Important Alert Parameters

Note

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-24*.

TABLE 5-9. Account Locked

PARAMETER	DESCRIPTION
Status	Select to enable or disable this alert. **Tip** If you are accessing the management console from Apex Central using single sign-on, verify the password setting in Apex Central before you attempt to log on again.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %LockedAccount% • %SourceIPAddress% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

TABLE 5-10. Long Virtual Analyzer Queue

PARAMETER	DESCRIPTION
Status	Select to enable or disable this alert.

Parameter	Description
Alert level	Shows the level of this alert. Cannot be modified.
Submissions	Specify the submissions threshold that will trigger the alert. **Tip** Refer to the red line of the **Queued Samples** widget to see the estimated number of samples Virtual Analyzer can analyze within 5 minutes. For details, see *Queued Samples on page 3-8*.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%SandboxQueueThreshold%` • `%SandboxQueue%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%ConsoleURL%`
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-11. Component Update Unsuccessful

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.

Parameter	Description
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ComponentList% • %UpdateError% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-12. High CPU Usage

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Average CPU usage	Specify the average CPU usage threshold that will trigger the alert.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Check interval	Specify the amount of time to wait between each check.
Check duration	Specify the duration of each check.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %CPUThreshold% • %CPUUsage% • %CheckingInterval% • %CheckingDuration% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-13. High Memory Usage

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Average memory usage	Specify the average memory usage threshold that will trigger the alert.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Check interval	Specify the amount of time to wait between each check.
Check duration	Specify the duration of each check.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %MemThreshold% • %MemUsage% • %CheckingInterval% • %CheckingDuration% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-14. High Disk Usage

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Disk usage	Specify the disk usage threshold that will trigger the alert.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Check interval	Specify the amount of time to wait between each check.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %DiskThreshold% • %DiskUsage% • %FreeDiskSpace% • %CheckingInterval% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-15. Secondary Appliance Unresponsive

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ApplianceError% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-16. High Availability Suspended

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PassiveApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-17. New High-Risk Objects Identified

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Objects	Specify the objects threshold that will trigger the alert.  **Note** Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.

Parameter	Description
Time period	Specify the time period threshold that will trigger the alert. **Note** Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections.
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %HighRiskThreshold% • %TimeRange% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-18. Connection Issue

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Monitored services	Select services to be monitored by this alert.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ServiceList% • %DiagnosisTip% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-19. Long Virtual Analyzer Processing Time

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Process time	Specify the process time threshold that will trigger the alert.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %SandboxProcessTimeThreshold% • %SampleList% • %TotalSampleNumber% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-20. Network Share Inaccessible

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL% • %NetworkShare%
Recipients	Specify the recipients who will receive the triggered alert email message.

Informational Alert Parameters

Note

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-24*.

Table 5-21. Syslog Server Inaccessible

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %SyslogServer% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-22. Backup Server Inaccessible

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Select the frequency at which this alert is sent when rule criteria are met.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %BackupServer% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Table 5-23. High Availability Restored

Parameter	Description
Status	Select to enable or disable this alert.
Alert level	Shows the level of this alert. Cannot be modified.
Alert frequency	Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified.
Subject	Specify the subject of the triggered alert notification.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PassiveApplianceIP% • %DateTime% • %ConsoleURL%
Recipients	Specify the recipients who will receive the triggered alert email message.

Alert Notification Message Tokens

The following table explains the tokens available for alert notifications. Use the table to understand which alert rules accept the message token and the information that the token provides in an alert notification.

Note

Not every alert notification can accept every message token. Review the alert's parameter specifications before using a message token. For details, see *Alert Notification Parameters on page 5-7*.

TABLE 5-24. Message Tokens

TOKEN	DESCRIPTION	WHERE ALLOWED
%ActiveApplianceIP%	The IP address of the Deep Discovery Analyzer active primary appliance Example: • 123.123.123.123 | 2001:0:3238:DFE1:63::FEFB	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
%ActiveApplianceName%	The host name of the Deep Discovery Analyzer active primary appliance Examples: • DDAN-A • DDAN-123	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
%ApplianceError%	The error encountered by the appliance Examples: • Not connected • Invalid API key • Incompatible software version	Secondary Appliance Unresponsive
%ApplianceIP%	The IP address of the Deep Discovery Analyzer appliance Example: • 123.123.123.123 | 2001:0:3238:DFE1:63::FEFB	All except the following: • High Availability Restored • High Availability Suspended • Passive Primary Appliance Activated

Token	Description	Where Allowed
%ApplianceName%	The host name of the Deep Discovery Analyzer appliance Examples: • DDAN-A • DDAN-123	All except the following: • High Availability Restored • High Availability Suspended • Passive Primary Appliance Activated
%BackupServer%	The host name or IP address of the backup server Examples: • my.example.com • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	Backup Server Inaccessible
%ComponentList%	The list of components Examples: • Advanced Threat Scan Engine • Deep Discovery Malware Pattern • IntelliTrap Exception Pattern • IntelliTrap Pattern	Component Update Unsuccessful
%ConsoleURL%	The Deep Discovery Analyzer management console URL Example: • https://192.168.85.69/ | https://[2001:0:3238:DFE1:63::FEFB]/	All

Token	Description	Where Allowed
%CPUThreshold%	The average CPU usage as a percentage allowed in the last 5 minutes before Deep Discovery Analyzer sends an alert notification Example: • 80%	High CPU Usage
%CPUUsage%	The total CPU usage as a percentage in the last 5 minutes Example: • 80%	High CPU Usage
%DateTime%	The date and time the alert was initiated Example: • 2014-03-21 03:34:09	All
%DaysBeforeExpiration%	The number of days before the product license expires Example: • 4	License Expiration
%DiagnosisTip%	Information for the connction issue	Connection Issue
%DiskThreshold%	The disk usage as a percentage allowed before Deep Discovery Analyzer sends an alert notification Example: • 85%	High Disk Usage
%DiskUsage%	The total disk usage as a percentage Example: • 85%	High Disk Usage

Token	Description	Where Allowed
%ExpirationDate%	The date that the product license expires Example: • 2014-03-21 03:34:09	License Expiration
%FreeDiskSpace%	The amount of free disk space in GB Example: • 50GB	High Disk Usage
%HighRiskThreshold%	The maximum number of new high-risk objects identified during the specified time period before Deep Discovery Analyzer sends an alert notification Example: • 10	New High-Risk Objects Identified
%LicenseStatus%	The current status of the product license Example: • Activated	License Expiration
%LicenseType%	The type the product license	License Expiration
%LockedAccount%	The account that was locked Example: • guest	Account Locked
%MemThreshold%	The average memory usage as a percentage allowed in the last 5 minutes before Deep Discovery Analyzer sends an alert notification Example: • 90%	High Memory Usage

Token	Description	Where Allowed
%MemUsage%	The total memory usage as a percentage in the last 5 minutes Example: • 90%	High Memory Usage
%NetworkShare%	The network share folder information Example: Share name: test | Server address:123.123.123.123 | Protocol: CIFS	Network Share Inaccessible
%PassiveApplianceIP%	The IP address of the Deep Discovery Analyzer passive primary appliance Example: • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
%PassiveApplianceName%	The host name of the Deep Discovery Analyzer passive primary appliance Examples: • DDAN-A • DDAN-123	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
%ProductName%	The product name Example: • Deep Discovery Analyzer	All
%ProductShortName%	The abbreviated product name Example: • DDAN	All

Token	Description	Where Allowed
%SandboxQueue%	The submission count in the sandbox queue waiting to be analyzed by Virtual Analyzer Example: • 100	Long Virtual Analyzer Queue
%ServiceList%	The list of affected services	Connection Issue
%SandboxQueueThreshold%	The maximum number of submissions in the sandbox queue before Deep Discovery Analyzer sends an alert notification Example: • 30	Long Virtual Analyzer Queue
%SyslogServer%	The host name or IP address of the syslog server Examples: • my.example.com • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	Syslog Server Inaccessible
%TimeRange%	The time period observed for new high-risk objects before Deep Discovery Analyzer sends an alert notification Examples: • 5 minutes • 30 minutes • 1 hour • 12 hours • 24 hours	New High-Risk Objects Identified

Token	Description	Where Allowed
%UpdateError%	The list of update errors Examples: • Unable to download: Advanced Threat Scan Engine • Unable to update: Deep Discovery Malware Pattern • Unable to update: IntelliTrap Exception Pattern. The appliance is configuring Virtual Analyzer instances or shutting down.	Component Update Unsuccessful
%ServiceList%	The services affected by the issue Example: • Internal Virtual Analyzer network (eth1, No proxy)	Connection Issue
%SandboxProcessTimeThreshold%	The maximum amount of time spent processing a sample before Deep Discovery Analyzer sends an alert notification	Long Virtual Analyzer Processing Time alert
%SampleList%	The samples affected by the issue	Long Virtual Analyzer Processing Time alert
%TotalSampleNumber%	The total number of samples affected by the issue	Long Virtual Analyzer Processing Time alert
%CheckingDuration%	The amount of time it takes to perform each check	High CPU Usage High Memory Usage
%CheckingInterval%	The amount of time between each check	High CPU Usage High Memory Usage High Disk Usage
%DiagnosisTip%	Recommendations on how to resolve the issue	Connection Issue

Reports

All reports generated by Deep Discovery Analyzer are based on an operational report template.

Generated Reports Tab

The **Generated Reports** tab, in **Alerts / Reports** > **Reports** , shows all reports generated by Deep Discovery Analyzer.

In addition to being displayed as links on the management console, generated reports are also available as attachments to an email. Before generating a report, you are given the option to send it to one or several email recipients.

Report Tasks

The following table describe tasks you can perform on the **Generated Reports** screen.

Task	Steps
Generate a report	See *Generating Reports on page 5-33*.
Download a report	To download a report, go to the last column in the table and click the icon. Generated reports are available as PDF files.
Send a report	Select a report and then click **Send Report**. You can send only one report at a time.
Delete selected reports	Select one or more reports and then click **Delete**.
Sort the report table	Click a column title to sort the data below it.
Adjust the pagination controls to view reports	The panel at the bottom of the screen shows the total number of reports. If all reports cannot display at the same time, use the pagination controls to view the reports that are hidden from view.

Generating Reports

Procedure

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

   The **Generated Reports** screen appears.

2. Click **Generate New**.

   The **Generate Report** window appears.

3. Configure report settings.

Option	Description
Template	Select an operational report template.
Description	Type a description that does not exceed 500 characters.
Range	Specify the covered date(s) based on the selected report template. • **Daily operational report**: Select any day prior to the current day. The report coverage is from 00:00:00 to 23:59:59 of each day. • **Weekly operational report**: Select the day of the week on which the report coverage ends. For example, if you choose Wednesday, the report coverage is from Wednesday of a particular week at 23:59:59 until Thursday of the preceding week at 00:00:00. • **Monthly operational report**: Select the day of the month on which the report coverage ends. For example, if you choose the 10th day of a month, the report coverage is from the 10th day of a particular month at 23:59:59 until the 11th day of the preceding month at 00:00:00.
Format	The file format of the report is PDF only.
Send to all contacts	Select the checkbox to send the generated report to all contacts.
Recipients	Select a contact from the drop-down list, or type an email address and press ENTER.

Option	Description
	You can type a maximum of 100 email addresses, typing them one at a time. **Note** You must press ENTER after each email address. Do not type multiple email addresses separated by commas. Before specifying recipients, configure the SMTP settings in **Administration** > **System Settings** > **SMTP** . **Note** Deep Discovery Analyzer generates reports approximately five minutes after **Send** is clicked.

4. Click **Generate**.

Schedules Tab

The **Schedules** tab, in **Alerts / Reports** > **Reports** , shows all the report schedules created from report templates. Each schedule contains settings for reports, including the template that will be used and the actual schedule.

Note

This screen does not contain any generated reports. To view the reports, navigate to **Alerts / Reports** > **Reports** > **Generated Reports**.

This tab includes the following options:

TABLE 5-25. Schedules Tasks

Task	Steps
Add Schedule	Click **Add Schedule** to add a new report schedule. This opens the **Add Report Schedule** window, where you specify settings for the report schedule. For details, see *Add Report Schedule Window on page 5-35*.

Task	Steps
Edit	Select a report schedule and then click **Edit** to edit its settings. This opens the **Edit Report Schedule** window, which contains the same settings in the **Add Report Schedule** window. For details, see *Add Report Schedule Window on page 5-35*. Only one report schedule is edited at a time.
Delete	Select one or several report schedules to delete and then click **Delete**.
Sort Column Data	Click a column title to sort the data below it.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of report schedules. If all report schedules cannot be displayed at the same time, use the pagination controls to view the schedules that are hidden from view.

Add Report Schedule Window

The **Add Report Schedule** window appears when you add a report schedule. A report schedule contains settings that Deep Discovery Analyzer will use when generating scheduled reports.

This window includes the following options:

Table 5-26. Add Report Schedule Window Tasks

Field	Steps
Template	Choose a template.
Description	Type a description.

Field	Steps
Generate at	Configure the schedule according to the template you chose. If the template is for a daily report, configure the time the report generates. The report coverage is from 00:00:00 to 23:59:59 of each day and the report starts to generate at the time you specified. If the template is for a weekly report, select the start day of the week and configure the time the report generates. For example, if you choose Wednesday, the report coverage is from Wednesday of a particular week at 00:00:00 until Tuesday of the following week at 23:59:59. The report starts to generate on Wednesday of the following week at the time you specified. If the template is for a monthly report, select the start day of the month and configure the time the report generates. For example, if you choose the 10th day of a month, the report coverage is from the 10th day of a particular month at 00:00:00 until the 9th day of the following month at 23:59:59. The report starts to generate on the 10th day of the following month at the time you specified. **Note** If the report is set to generate on the 29th, 30th, or 31st day of a month and a month does not have this day, Deep Discovery Analyzer starts to generate the report on the first day of the next month at the time you specified.
Format	The file format of the report is PDF only.
Send to all contacts	Select the checkbox to send the generated report to all contacts.
Recipients	Select a contact from the drop-down list, or type a valid email address to which to send reports and then press ENTER. You can type up to 100 email addresses, typing them one at a time. It is not possible to type multiple email addresses separated by commas. Before specifying recipients, verify that you have specified SMTP settings in the **SMTP** tab located at **Administration** > **System Settings**.

Customization Tab

The **Customization** tab, in **Alerts / Reports** > **Reports**, allows you to customize items in the Deep Discovery Analyzer reports.

This screen includes the following options:

TABLE 5-27. Cover Page

OPTION	TASK	DISPLAY AREA
Title	Type a title that does not exceed 40 characters.	Report cover

TABLE 5-28. Email Message

OPTION	TASKS	DISPLAY AREA
Header logo	Browse to the location of the logo. The following are the image requirements. • Dimensions: 180 x 60 pixels • Maximum file size: 30 KB • File type: `BMP`, `GIF`, `JPG`, or `PNG`	Notification
Divider color	To change the default color, click in the box and use the color pick specify a new value.	Notification
Footer logo	Browse to the location of the logo. The following are the image requirements. • Dimensions: 100 x 40 pixels • Maximum file size: 30 KB • File type: `BMP`, `GIF`, `JPG`, or `PNG`	Notification
Footer text	Type a footer that does not exceed 60 characters.	Notification

Chapter 6

Administration

The features of **Administration** are discussed in this chapter.

Updates

Use the **Updates** screen, in **Administration** > **Updates**, to configure component and product update settings.

An Activation Code is required to use and update components. For details, see *License on page 6-103*.

Components Tab

The **Components** tab shows the security components currently in use.

TABLE 6-1. Components

COMPONENT	DESCRIPTION
Advanced Threat Correlation Pattern	The Advanced Threat Correlation Pattern contains a list of file features that are not relevant to any known threats.
Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)	The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection.
Contextual Intelligence Query Handler (Linux, 64-bit)	The Contextual Intelligence Query Handler processes the behaviors identified by the Contextual Intelligence Engine and sends the report to the Predictive Machine Learning engine.
Deep Discovery Malware Pattern	The Deep Discovery Malware Pattern contains information that helps Deep Discovery Analyzer identify the latest malware and mixed threat attacks. Trend Micro creates and releases new versions of the pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.
IntelliTrap Exception Pattern	The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning.
IntelliTrap Pattern	The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats.

Component	Description
Network Content Correlation Pattern	The Network Content Correlation Pattern implements detection rules defined by Trend Micro.
Network Content Inspection Engine (Linux, User mode, 64-bit)	The Network Content Inspection Engine is used to perform network scanning.
Network Content Inspection Pattern	The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning.
Script Analyzer Pattern (Deep Discovery)	The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.
Spyware/Grayware Pattern	The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware.
Trusted Certificate Authorities	Trusted Certificate Authorities provides the trusted certificate authorities to verify PE signatures.
Virtual Analyzer Configuration Pattern	The Virtual Analyzer Configuration Pattern contains configuration information for Virtual Analyzer, such as supported threat types and supported file types.
Virtual Analyzer Sensors Virtual Analyzer Sensors (Linux)	The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer (for Windows and Linux).

This screen includes the following options:

Option	Task
Update Now	Select one or more components, and click **Update Now** to manually update the selected components.
Rollback	Select one or more components, and click **Rollback** to revert the selected components to a previous version.

Option	Task
Sync Version Information	Click to retrieve the component version from the update source, and review if any of the components need updates. Update any component where the version displayed on the **Version on Update Source** column is greater than the current version. Additionally, Deep Discovery Analyzer displays the version numbers of components with available updates in a red font.

Component Update Settings Tab

The **Component Update Settings** tab allows you to configure automatic updates and the update source.

Setting	Description
Automatic updates	Select **Automatically check for updates** to set Deep Discovery Analyzer to check for updates every 15 minutes. You may also specify the update to run at a specific time.
Update source	Select one of the following options and configure the require settings: • Select **Trend Micro ActiveUpdate server** to download components directly from the Trend Micro. Verify that Deep Discovery Analyzer has Internet connection. To authenticate the ActiveUpdate server, select **Enable HTTPS authentication**. **Note** If you select **Enable HTTPS authentication** and enable HTTPS decryption on your network (for example, on a secure gateway), it is recommended that you include the ActiveUpdate server URL in the approved list. • Select **Other source** to specify a different update source location. The update source URL must begin with “http://” or “https//:”. You can select **Use system proxy** to use the system proxy settings you configure on the **Administration > System Settings > Proxy** screen to connect to the update source.

Setting	Description
	To verify the integrity of the update packages from other update sources, select **Enable component update package integrity check**. If you select this option, verify that the signature file is available on the update server for Deep Discovery Analyzer to verify the integrity of a component update package. If you need assistance setting up an update source, contact your support provider. **Note** • When the IPv6 address is part of a URL, enclose the address in square brackets ([]). • Verify that proxy settings are correct if Deep Discovery Analyzer requires a proxy server to connect to its update source. For details, see *Proxy Tab on page 6-54*. • You can also set Trend Vision One as the update source for Deep Discovery Analyzer. To do this, enable ActiveUpdate on Trend Vision One and configure the required settings that Deep Discovery Analyzer can obtain through the Service Gateway. For more information, see the Trend Vision One documentation.

Hotfixes / Patches Tab

Use the **Hotfixes / Patches** screen to apply hotfixes and patches to Deep Discovery Analyzer. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

TABLE 6-2. Hotfixes / Patches

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

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

http://downloadcenter.trendmicro.com/

Installing a Hotfix / Patch

Perform the following tasks when using Deep Discovery Analyzer in a high availability cluster configuration.

1. Detach the passive primary appliance.
2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again.

Procedure

1. Obtain the product update file from Trend Micro.
   - If the file is an official patch, download it from the download center.

     http://downloadcenter.trendmicro.com/
   - If the file is a hotfix, send a request to Trend Micro support.
2. On the logon page of the management console, select **Enable extended session timeout** and then log on using a valid user name and password.
3. Go to **Administration** > **Updates** > **Hotfixes / Patches**.
4. Click **Choose File** or **Browse**, and select the product update file.
5. Click **Install**.

   Important

   Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.

   Deep Discovery Analyzer will automatically restart after the update is complete.
6. Log on to the management console.
7. Go back to the **Administration** > **Updates** > **Hotfixes / Patches** screen.
8. Verify that the hotfix / patch displays in the **History** section as the latest update.

Rolling Back a Hotfix / Patch

Perform the following tasks when using Deep Discovery Analyzer in a high availability cluster configuration.

1. Detach the passive primary appliance.

2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again.

Deep Discovery Analyzer has a rollback function to undo an update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular hotfix / patch is applied.

Note

The rollback process automatically restarts Deep Discovery Analyzer, so make sure that all tasks on the management console have been completed before rollback.

Procedure

1. Go to **Administration** > **Updates** > **Hotfixes / Patches**.
2. In the **History** section, click **Roll Back**.

   Deep Discovery Analyzer will automatically restart after the rollback is complete.
3. Log on to the management console.
4. Go back to the **Administration** > **Updates** > **Hotfixes / Patches** screen.
5. Verify that the hotfix / patch no longer displays in the **History** section.

Firmware Tab

Use the **Firmware** tab to apply an upgrade to Deep Discovery Analyzer. Trend Micro prepares a readme file for each upgrade. Read the accompanying readme file before applying an upgrade for feature information and for special installation instructions.

Note

After applying the firmware update on hardware models 1200 and 1300, Deep Discovery Analyzer automatically migrates the settings of a Deep Discovery Analyzer 7.5 or 7.2 installation to 7.6.

Perform the following tasks when using Deep Discovery Analyzer in a high availability cluster configuration.

1. Detach the passive primary appliance.
2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again.

Perform the following steps to install the upgrade.

Procedure

1. On the logon page of the management console, select **Enable extended session timeout** and then log on using a valid user name and password.
2. Go to **Administration** > **Updates** and click the **Firmware** tab.
3. Click **Choose File** or **Browse**, and select the firmware upgrade file.
4. Click **Install**.

Important

Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.

Deep Discovery Analyzer will automatically restart after the upgrade is complete.

5. Clear the browser cache before you access the management console.

Integrated Products/Services

The Integrated Products/Services screen, in **Administration** > **Integrated Products/Services**, includes the following tabs:

Trend Vision One Tab

Trend Vision One extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With Trend Vision One, you can respond more effectively to threats, minimizing the severity and scope of a breach.

Deep Discovery Analyzer integrates with Trend Vision One through a Service Gateway to perform the following tasks for collaborative security analytics in a hybrid environment:

- Synchronize suspicious objects (synchronized and user-defined) and exceptions with Trend Vision One
- Upload new suspicious objects generated by the internal Virtual Analyzer to Trend Vision One

- Receive samples from Trend Vision One (through the Sandbox Analysis app) for analysis
- Upload analysis reports to Trend Vision One

You can configure Deep Discovery Analyzer to use the Service Gateway as an alternative source for ActiveUpdate or Smart Protection Services.

Note

- You can only integrate Deep Discovery Analyzer with Sandbox as a Service or Trend Vision One, but not both at the same time.
- Deep Discovery Analyzer does not upload existing suspicious objects generated by the internal Virtual Analyzer to Trend Vision One.
- If you register Deep Discovery Analyzer to Trend Vision One, Deep Discovery Director, and Trend Micro Apex Central, Deep Discovery Analyzer synchronizes data with the integrated products in the following priority:
  - Download exception list: Trend Vision One, Deep Discovery Director, Trend Micro Apex Central
  - Upload Virtual Analyzer-generated suspicious objects: Trend Vision One, Deep Discovery Director, Trend Micro Apex Central
  - Download Virtual Analyzer-generated and user-defined suspicious objects: Trend Vision One, Deep Discovery Director

Integrating Deep Discovery Analyzer with Trend Vision One

Note

You can only integrate Deep Discovery Analyzer with Sandbox as a Service or Trend Vision One, but not both at the same time.

If you integrate Deep Discovery Analyzer with Sandbox as a Service, this screen is not configurable.

You can integrate Deep Discovery Analyzer with Trend Vision One for threat intelligence sharing through a Service Gateway and receive samples for analysis through the Sandbox Analysis app.

Procedure

1. On the Trend Vision One console, go to **Workflow and Automation** > **Service Gateway Management**. If available, click the **Service Gateway Management 2.0** tab.
2. If you do not have an existing Service Gateway deployed, install a Service Gateway.
   a. Click **Download Virtual Appliance** to open the **Service Gateway Virtual Appliance** panel.
   b. Select either **VMware ESXi (OVA)** or **Microsoft Hyper-V (VHD)** as the image type you want to use.
   c. Select **I agree to the End User License Agreement** and click **Download Disk Image**.
   d. Record the **Registration Token** that you need to apply during deployment.
   e. Install the Service Gateway virtual appliance.

      For detailed deployment instructions, see Deploying a Service Gateway Virtual Appliance.
3. Click the Service Gateway name.
4. Click **Manage Services**.
5. Click the install icon to install and then enable the following services.

Service	Description
Forward proxy	Required for the Sandbox Analysis integration function that allows Deep Discovery Analyzer to perform the following: • Receive samples from Trend Vision One • Send analysis reports (for only samples received from Trend Vision One) to Trend Vision One
Suspicious Object list synchronization	Required for the Suspicious Objects synchronization function that allows Deep Discovery Analyzer to perform the following: • Synchronize the centralized Suspicious Object List and Exception List from Trend Vision One • Send analysis reports (for detected samples with a risk level) to Trend Vision One

6. Record the Service Gateway IP address and the API key that are needed for connection settings on the Deep Discovery Analyzer console.
   - IP address: Click the Service Gateway name and record the **IPv4 address** or **IPv6 address**.
   - API key: Click the **Manage API Key** button and record the API key.
7. On the Deep Discovery Analyzer web console, go to **Administration** > **Integrated Products/Services** and click **Trend Vision One**.
8. Select **Enable Service Gateway connection** and type the IPv4 or IPv6 address of the Service Gateway in the **Service Gateway IP address** field.
9. To connect to Trend Vision One through the Service Gateway for threat intelligence data sharing, do the following:
   a. Select **Enable Suspicious Object Synchronization**.
   b. Specify the API key you obtained from the Trend Vision One console.
   c. If a certificate is required for Deep Discovery Analyzer to communicate with the Service Gateway, select **Use certificate** and click **Select** to locate the certificate file.
   d. Click **Test Connection** to verify.

e. Click **Save**.

f. Wait until synchronization with the Service Gateway completes.

10. To have Deep Discovery Analyzer receive and analyze samples from Trend Vision One, do the following:

Note

Sandbox Analysis integration requires Service Gateway 2.0 or later.

a. On the Trend Vision One console, go to **Service Management** > **Product Instance**.

b. Click **Add Existing Product**.

c. For **Instance type**, select **Trend Micro Deep Discovery Analyzer** from the drop-down list.

d. Click the link to generate an enrollment token.

e. Copy the enrollment token for use on the Deep Discovery Analyzer web console.

f. Click **Save**.

g. On the Deep Discovery Analyzer web console, go to **Administration** > **Integrated Products/Services** and click **Trend Vision One**.

h. Select **Enable Sandbox Analysis integration**.

i. Paste the enrollment token you obtained from the Product Connector in Trend Vision One.

j. Click **Save**.

After Deep Discovery Analyzer is registered to Trend Vision One, the **Test Connection** button appears.

k. On the Trend Vision One console, go to **Threat Intelligence** > **Sandbox Analysis**.

l. Click **Submission Settings** and select **Use your Deep Discovery Analyzer instead of Sandbox Analysis sandbox**.

Unregistering Deep Discovery Analyzer from the Sandbox Analysis App

To stop receiving samples from Trend Vision One for analysis on Deep Discovery Analyzer, unregister Deep Discovery Analyzer from the Sandbox Analysis app.

Important

After unregistering the Sandbox Analysis service on Deep Discovery Analyzer, you must obtain a new enrollment token to register to Trend Vision One again.

Procedure

1. Go to **Administration** > **Integrated Products/Services**.

   The **Trend Vision One** tab appears.

2. In the Sandbox Analysis Integration section, click **Unregister**.

   A warning screen appears.

3. Click **Unregister** to confirm.

Deep Discovery Director Tab

Trend Micro Deep Discovery Director is a management solution that provides Indicators of Compromise (IOC) information and enables centralized deployment of product updates, product upgrades, configuration replication and Virtual Analyzer images to Deep Discovery Analyzer.

Deep Discovery Analyzer integrates with the following versions of Deep Discovery Director:

- 5.2 and above

Deploying updates or upgrades to Deep Discovery Analyzer appliances that are configured in a high availability cluster will temporarily:

- Detach the high availability appliances and suspend high availability
- Restrict access to the management console and display a static information screen

After the update or upgrade completes, the detached appliances will automatically reattach and restore high availability.

Important

- Before deploying updates or upgrades, ensure that the appliances are not executing any task.
- Avoid detaching appliances while an upgrade is in progress.
- If the appliances fail to upgrade or continue to show the **Upgrading Appliance** screen for more than two hours, check Deep Discovery Director for errors. To resolve errors, temporarily detach the appliances. Detached appliances continue to upgrade. After the upgrade, manually attach the appliances again to restore high availability.

Use the Deep Discovery Director management console to deploy or replicate a Virtual Analyzer image or configuration to a primary appliance. This is not required for secondary appliances since they are set to automatically sync Virtual Analyzer images or configuration from the primary appliance.

Deep Discovery Analyzer supports integration with Deep Discovery Director to enable the following:

- Upload of suspicious objects generated by the internal Virtual Analyzer to Deep Discovery Director
- Linux image deployment from Deep Discovery Director 5.3
- Download of the following from Deep Discovery Director:
  - Exceptions

- Suspicious objects (user-defined and synchronized)
- YARA rule files
- File passwords (Deep Discovery Director on-premises version 5.2 and above)

Note

- After you register Deep Discovery Analyzer to Deep Discovery Director, Deep Discovery Analyzer automatically synchronizes YARA rule settings from Deep Discovery Director and overwrites existing YARA rule settings that you have configured.
- After you register Deep Discovery Analyzer to Deep Discovery Director, Deep Discovery Analyzer automatically synchronizes file passwords from Deep Discovery Director and overwrites existing file passwords that you have configured. You can only change the file passwords on the Deep Discovery Director management console.
- If you register Deep Discovery Analyzer to Trend Vision One, Deep Discovery Director, and Trend Micro Apex Central, Deep Discovery Analyzer synchronizes data with the integrated products in the following priority:
  - Download exception list: Trend Vision One, Deep Discovery Director, Trend Micro Apex Central
  - Upload Virtual Analyzer-generated suspicious objects: Trend Vision One, Deep Discovery Director, Trend Micro Apex Central
  - Download Virtual Analyzer-generated and user-defined suspicious objects: Trend Vision One, Deep Discovery Director

The Deep Discovery Director screen displays the following information:

TABLE 6-3. Deep Discovery Director Fields

FIELD	INFORMATION
Status	The following appliance statuses can be displayed: • Not registered: The appliance is not registered to Deep Discovery Director. • Registered | Connected: The appliance is registered and connected to Deep Discovery Director. • Registered | Unable to connect: The appliance is registered to Deep Discovery Director, but unable to connect. Verify that the Deep Discovery Director network settings are valid. • Registered | Untrusted fingerprint: The appliance is registered to Deep Discovery Director, but the connection was interrupted. To restore the connection, trust the new fingerprint.
Last connected	The last time this appliance connected to Deep Discovery Director.
Host name	The host name of this appliance.
Server address	The Deep Discovery Director server address.
Port	The Deep Discovery Director port.
API key	The Deep Discovery Director API key.
Fingerprint (SHA-256)	The Deep Discovery Director fingerprint.
Use the system proxy settings	Select to use the system proxy settings to connect to Deep Discovery Director.
Synchronize suspicious objects from Deep Discovery Director	Select this option synchronize suspicious objects from Deep Discovery Director.

Registering to Deep Discovery Director

The following procedure is for registering to Deep Discovery Director. If you have already registered and want to change the connection settings, you must first unregister.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**.
2. Under **Connection Settings**, do the following:
   a. Type the **Server address** for Deep Discovery Director.
   b. Type the **Port** number for Deep Discovery Director. The default port number is 443.
   c. Type the **API key** for Deep Discovery Director.

   Note
   You can find this information on the **Help** screen on the management console of Deep Discovery Director.
3. (Optional) If you have configured proxy settings for Deep Discovery Analyzer and want to use these settings for Deep Discovery Director connections, select **Use system proxy**.

   Note
   This setting can be changed after registering to Deep Discovery Director.

   To update this setting without unregistering from Deep Discovery Director, click **Update Settings**.
4. (Optional) To synchronize suspicious objects from Deep Discovery Director, select **Synchronize suspicious objects from Deep Discovery Director**.

Note

- You can view the list of synchronized suspicious objects on the **Synchronized Suspicions Objects** screen.
- To use synchronized suspicious object lists for ICAP pre-scan and Virtual Analyzer analysis, configure the required scan settings on the **ICAP** and **Scan Settings** screens.

  For more information, see *Configuring ICAP Settings on page 6-30* and *Scan Settings Tab on page 4-68*.

5. Click **Register**.

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

Note

- If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust**.
- After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.
- If you are using Deep Discovery Analyzer in a load-balancing cluster, registering the primary appliance will automatically register all secondary appliances.

Unregistering from Deep Discovery Director

Follow this procedure to unregister from Deep Discovery Director or before registering to another Deep Discovery Director.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**
2. Click **Unregister**.

   The **Status** changes to **Not registered**.

   Note

   When you unregister Deep Discovery Analyzer from Deep Discovery Director, Deep Discovery Analyzer automatically removes all synchronized suspicious objects.

Sandbox as a Service Tab

With Sandbox as a Service integration, Deep Discovery Analyzer acts as a sandbox in the cloud to receive and analyze samples that are submitted to Sandbox as a Service.

Note

You can only integrate Deep Discovery Analyzer with Sandbox as a Service or Trend Vision One, but not both at the same time.

The following table describes the tasks you can perform on the **Sandbox as a Service** screen.

Task	Description
Register to a new server	Click **Register** to integrate Deep Discovery Analyzer with a new Sandbox as a Service server. For more information, see *Integrating Deep Discovery Analyzer with Sandbox as a Service on page 6-22*.
Unregister from a server	Select an entry and click **Unregister** to disconnect Deep Discovery Analyzer from the selected Sandbox as a Service server.

Task	Description
Test the connection to a server	Select an entry and click **Test Connection** to test the connection to the integrated Sandbox as a Service server.
Disable Sandbox as a Service integration	To stop Deep Discovery Analyzer from receiving and analyzing samples from Sandbox as a Service without unregistration, toggle to turn on the **Maintenance mode** switch. **Note** Disabling Sandbox as a Service integration does not affect samples that Deep Discovery Analyzer has already received and is currently analyzing.

Integrating Deep Discovery Analyzer with Sandbox as a Service

Note

You can only integrate Deep Discovery Analyzer with Sandbox as a Service or Trend Vision One, but not both at the same time.

If you integrate Deep Discovery Analyzer with Trend Vision One, this screen is not configurable.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Sandbox as a Service**.
2. Click **Register**.
3. Type the server name or IP address.
4. Type the group ID.
5. (Optional) If you have configured proxy settings for Deep Discovery Analyzer and want to use these settings for Sandbox as a Service connections, select **Use system proxy**.

6. Click **Register**.

   You can test the connection and check the activation status on the **Sandbox as a Service** screen.

Smart Protection Tab

Trend Micro Smart Protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By integrating Web Reputation Services, Deep Discovery Analyzer can obtain reputation data for websites that users attempt to access. Deep Discovery Analyzer logs URLs that Smart Protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.

Deep Discovery Analyzer connects to a Smart Protection source to obtain web reputation data.

Reputation services are delivered through the Trend Micro Smart Protection Network and Smart Protection Server. The following table provides a comparison.

TABLE 6-4. Smart Protection Sources

BASIS OF COMPARISON	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
Purpose	A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology	Localizes the File and Web Reputation Services to the corporate network to optimize efficiency. The Smart Protection Server also provides the following: • Certified Safe Software Service • Community File Reputation • Web Inspection Service • Web Reputation Service • Predictive Machine Learning engine • Community Domain/IP Reputation Service **Note** The Dynamic URL Scanning service is only available on the Smart Protection Network.
Administration	Hosted and maintained by Trend Micro	Installed and managed by Trend Micro product administrators
Connection protocol	HTTPS	HTTPS

Basis of Comparison	Trend Micro Smart Protection Network	Smart Protection Server
Usage	Use if you do not plan to install Smart Protection Server To configure Smart Protection Network as source, see *Configuring Smart Protection Settings on page 6-26*.	Use as primary source and the Smart Protection Network as an alternative source For guidelines on setting up Smart Protection Server and configuring it as source, see *Setting Up Smart Protection Server on page 6-25*.

About Smart Protection Server

Consideration	Description
Deployment	If you have previously installed a Smart Protection Server for use with another Trend Micro product, you can use the same server for Deep Discovery Analyzer. While several Trend Micro products can send queries simultaneously, the Smart Protection Server may become overloaded as the volume of queries increases. Make sure that the Smart Protection Server can handle queries coming from different products. Contact your support provider for sizing guidelines and recommendations.
IP Address	Smart Protection Server and the VMware ESX/ESXi server (which hosts the Smart Protection Server) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Deep Discovery Analyzer to make sure that these IP addresses are not assigned to the Smart Protection Server.
Installation	For installation instructions and requirements, refer to the *Installation and Upgrade Guide* for Trend Micro Smart Protection Server at https://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx.

Setting Up Smart Protection Server

Procedure

1. Install Smart Protection Server on a VMware ESX/ESXi server.
2. Configure Smart Protection Server settings from the Deep Discovery Analyzer management console.

For details, see *Configuring Smart Protection Settings on page 6-26*.

Note

- Smart Protection Server may not have reputation data for all URLs because it cannot replicate the entire Smart Protection Network database. When updated infrequently, Smart Protection Server may also return outdated reputation data.
- Enabling this option improves the accuracy and relevance of the reputation data.
- Disabling this option reduces the time and bandwidth to obtain the data.

Configuring Smart Protection Settings

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Smart Protection**.
2. Select **Enabled**.
3. Select a Smart Protection source:
   - Trend Micro Smart Protection Network™

     Trend Micro Smart Protection Network is a globally-scaled, cloud-based infrastructure providing reputation services to Trend Micro products that integrate Smart Protection technology. Deep Discovery Analyzer connects to the Smart Protection Network using HTTPS. Select this option if you do not plan to set up a Smart Protection Server.
   - Smart Protection Server

     Smart Protection Server does the following:

- Provides Web Reputation Services as offered by Smart Protection Network
- Relays these services to the global Trend Micro Smart Protection Network for network efficiency
- Acts as a reverse proxy for Deep Discovery Analyzer to connect to global services

As a Trend Micro product administrator, you must set up and maintain this server. Select this option if you have already set up a server.

4. If you select **Smart Protection Server**, configure the following settings:

   a. Specify the Smart Protection Server IP address or fully qualified domain name and port number.

      Obtain the IP address by going to **Smart Protection** > **Reputation Services** > **Web Reputation** on the Smart Protection Server console.

      The IP address forms part of the URL listed on the screen.

      Tip

      Trend Vision One that can also act as a local Smart Protection Server for Deep Discovery Analyzer. In this case, specify the Service Gateway address.

   b. (Optional) Select **Connect using a proxy server** if proxy settings for Deep Discovery Analyzer have been configured for use with Smart Protection Server connections.

      Note

      If proxy settings are disabled, Smart Protection Server will connect to Deep Discovery Analyzer directly.

   c. (Optional) If your organization uses a CA certificate, select **Use certificate** and click **Choose File** or **Browse** to locate the certificate file.

d. (Optional) If your organization uses a Certificate Revocation List, select **Use CRL** and click **Choose File** or **Browse** to locate the Certificate Revocation List file.

Important

Deep Discovery Analyzer supports connection to global services only if Smart Protection Server version 3.3 is used.

Note

When **Smart Protection Server** is selected as Smart Protection source, the following services and the ability to test their connectivity are enabled:

- Certified Safe Software Service (CSSS)
- Community File Reputation
- Community Domain/IP Reputation Service
- Predictive Machine Learning engine
- Web Inspection Service
- Web Reputation Service

5. Click **Save**.

ICAP Tab

Deep Discovery Analyzer supports integration with Internet Content Adaptation Protocol (ICAP) clients. An ICAP client can be a proxy server or network storage that submits samples to Deep Discovery Analyzer for analysis. The ICAP client performs an action (pass or block) on the sample based on the analysis result from Deep Discovery Analyzer .

After ICAP integration, Deep Discovery Analyzer can perform the following functions:

- Work as an ICAP server that analyzes samples submitted by ICAP clients
- Serve User Configuration Pages to the end user when the specified network behavior (URL access / file upload / file download) is blocked
- Control which ICAP clients can submit samples by configuring the ICAP Client list
- Bypass file scanning based on selected MIME content-types
- Bypass file scanning based on true file types
- Bypass URL scanning in RESPMOD mode
- Scan samples using different scanning modules
- Filter sample submissions based on the file types that Virtual Analyzer can process.

Deep Discovery Analyzer supports the following ICAP specifications.

Protocol	ICAP Mode	ICAP URL
ICAP	REQMOD	`icap://<DDAN_IP>:1344/request`
	RESPMOD	`icap:// <DDAN_IP>:1344/response`
ICAPS	REQMOD	`icaps://<DDAN_IP>:11344/request`
	RESPMOD	`icaps://<DDAN_IP>:11344/response`

The following describes the ICAP modes:

- REQMOD (Request Modification Mode): Checks the contents of the HTTP request body, including URLs and uploaded files
- RESPMOD (Response Modification Mode): Checks the contents of the HTTP response body, including URLs and downloaded files

For full compatibility with Deep Discovery Analyzer, set both Request Modification and Response Modification modes on ICAP clients.

Configuring ICAP Settings

Note

When ICAP integration is enabled, Deep Discovery Analyzer automatically reduces Virtual Analyzer throughput to conserve system resources.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **ICAP**.
2. Select **Enable ICAP**.
3. Type the **ICAP port number**.

   The default value is 1344.
4. To connect the ICAP client over a secure connection, select **Enable ICAP over SSL** and specify the following details:
   - **ICAPS port number**: Default value is 11344
   - **Certificate**: Certificates must use base64-encoding
   - **Private key**: Private keys must use base64-encoding

     Important

     Only encrypted private keys are supported.
   - **Passphrase**
   - **Confirm Passphrase**
5. (Optional) In the **Header Settings** section, specify how Deep Discovery Analyzer handles ICAP headers.
   a. Under **ICAP headers from Deep Discovery Analyzer**, select the ICAP headers Deep Discovery Analyzer sends to ICAP clients.

      For details, see *ICAP Header Responses on page 4-12*.

b. Under **ICAP headers from ICAP clients**, select the ICAP headers to save when Deep Discovery Analyzer receives the headers from ICAP clients.

6. (Optional) Under **Scan Settings**, select one or more of the following options:

- Bypass URL scanning in RESPMOD mode
- Scan samples using YARA rules
- Scan samples using the selected suspicious objects list

Note

- Suspicious objects in the generated suspicious objects list are added by the internal Virtual Analyzer in Deep Discovery Analyzer while suspicious objects in the synchronized suspicious objects list are obtained from Trend Vision One or Deep Discovery Director.
- If you select **Synchronized suspicious objects list**, you must also integrate Deep Discovery Analyzer with Trend Vision One or enable suspicious object synchronization from Deep Discovery Director.

  For more information, see *Integrating Deep Discovery Analyzer with Trend Vision One on page 6-11*.

- Scan samples using the user-defined suspicious objects list
- Scan samples using the Predictive Machine Learning engine
- Classify password-protected samples

7. (Optional) Under **Content Settings**, do the following:

a. Select **Enable MIME content-type exclusion** to exclude files from scanning based on the MIME content-types that you selected or specified.

b. To have Deep Discovery Analyzer check the true file type of submitted samples, select **Enable MIME content-type validation**.

Note

- The **Enable MIME content-type validation** setting only applies when you select **Enable MIME content-type exclusion**.
- When you select this option, Deep Discovery Analyzer will still perform an ICAP pre-scan on samples with one of the following:
  - HTTP compression
  - Some MIME content-types in ICAP Preview mode
  - Custom MIME content-types
  - Some pre-defined MIME content-types

  Samples with unsupported file types are not submitted to Virtual Analyzer for scanning after ICAP pre-scan.

8. (Optional) Under **User Notification Pages**, select **Use a user notification page whenever the ICAP client blocks network traffic for the following events** and specify a file that contains the page contents.

Note

This setting allows Deep Discovery Analyzer to display a custom page whenever an ICAP client blocks network traffic for specific events. The ICAP client may override this setting. If the setting is enabled and the custom page are not displayed, verify that there are no conflicts with the ICAP client configuration.

Deep Discovery Analyzer supports custom pages for the following events:

- URL access

- File upload
- File download

Note

Use any text editor to create the pages, and save as plain text. HTML tags may be used to apply formatting. Ensure that files are smaller than 5 MB.

9. (Optional) Under **ICAP Client List**, do the following:

   a. Specify the number of **Max connections** allowed.

      The default value is `1000`.

   b. Select **Accept scan request from the following ICAP clients only** to limit submissions to specific clients only.

      - To add a new IP address or IP address range, click **Add**.
      - To remove an existing entry, select an entry and click **Delete**.

      Note

      By default, all ICAP clients can submit samples to Deep Discovery Analyzer.

10. Click **Save**.

11. Verify that ICAP integration is working correctly in Deep Discovery Analyzer.

    For high-risk samples:

    - Deep Discovery Analyzer returns an “HTTP 403 Forbidden” message to the ICAP client.
    - If the **User Notification Page** setting is enabled, Deep Discovery Analyzer includes the uploaded page as part of the message.
    - If X-Virus-ID and X-Infection-Found ICAP headers are enabled, Deep Discovery Analyzer includes these headers within the message.

For no-risk samples:

- Deep Discovery Analyzer returns the original message it receives from the ICAP client.
- If the ICAP client supports ICAP “204 No Content”, it returns an ICAP “204 No Content” response without the original message.

Microsoft Active Directory Tab

Deep Discovery Analyzer supports integration with a Microsoft Active Directory server. After integration, Microsoft Active Directory accounts can be added as Deep Discovery Analyzer users.

Configuring Microsoft Active Directory

Note

Deep Discovery Analyzer supports integration with the Microsoft Active Directory 2012, 2016, and 2019 versions only.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Microsoft Active Directory**.
2. Select **Use Microsoft Active Directory server**.
3. Specify a server type.
4. For the primary Microsoft Active Directory server, specify the following details:
   - Server address
   - Access protocol
   - Port
5. (Optional) Select **Enable secondary server**.

The secondary server acts as a backup when the primary Microsoft Active Directory server is inaccessible.

6. For the primary Microsoft Active Directory server, specify the following details:
   - Base distinguished name
   - User name
   - Password
7. (Optional) If the primary server requires a certificate, select **Use CA certificate**, and then specify the required certificate.
8. (Optional) Click **Test Connection** to test the connection to the primary Microsoft Active Directory server.
9. Click **Save**.

SAML Authentication Tab

Security Assertion Markup Language (SAML) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports single sign-on (SSO), a technology that allows for a single user login to work across multiple applications and services. When you configure SAML settings in Deep Discovery Analyzer, users signing in to your organization's portal can seamlessly sign in to Deep Discovery Analyzer without an existing Deep Discovery Analyzer account.

In SAML single sign-on, a trust relationship is established between the identity provider (IdP) and the service provider (SP) by using SAML metadata files. The identity provider contains the user identity information stored on a directory server. The service provider (which in this case is Deep Discovery Analyzer) uses the user identity information from the identity provider for user authentication and authorization.

Deep Discovery Analyzer supports the following identity providers for single sign-on:

- Microsoft Active Directory Federation Services (AD FS) 4.0 or 5.0

- Okta

To connect Deep Discovery Analyzer to your organization environment for single-sign-on, complete the following:

1. Access the Deep Discovery Analyzer management console to obtain the service provider metadata file.

   You can also update the certificate in Deep Discovery Analyzer.

   For more information, see *Service Provider Metadata and Certificate on page 6-36*.

2. In your identity provider:

   a. Configure the required settings for single sign-on.

   b. Obtain the federation metadata file.

   For more information, see the documentation that comes with your identity provider.

3. In Deep Discovery Analyzer:

   a. Import the federation metadata file for your identity provider.

      For more information, see *Configuring Identity Provider Settings on page 6-37*.

   b. Create SAML user groups.

Service Provider Metadata and Certificate

Obtain the service provider metadata from Deep Discovery Analyzer to provide to your identity provider.

On the **SAML Authentication** screen, the Service Provider section displays the following service provider information:

- **Entity ID**: Identifies the service provider application
- **Single Sign On URL**: The endpoint URL responsible for receiving and parsing a SAML assertion (also referred to as "Assertion Consumer Service")

- **Single Sign Off URL**: The endpoint URL responsible for initiating the SAML logout process
- **Certificate**: The encryption certificate (verification certificate) in X.509 format

You can click the following in the Service Provide section:

- **Download Metadata**: Downloads the Deep Discovery Analyzer metadata file. You can import the metadata file on an Active Directory Federal Services (ADFS) identity provider.
- **Download Certificate**: Downloads the Deep Discovery Analyzer certificate file. You can import the certificate file on an OKTA identity provider.
- **Update Certificate**: Uploads a new certificate on Deep Discovery Analyzer.

  Deep Discovery Analyzer supports certificates in X.509 PEM format.

Configuring Identity Provider Settings

Note

- Before you add an identity provider, obtain the federation metadata file from your identity provider.
- You can add up to two identity providers in Deep Discovery Analyzer, one each for AD FS and Okta.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **SAML Authentication**.
2. In the Identity Provider section, do one of the following:
   - Click **Add** to add a new entry.
   - Click an identity provider name to change the settings.

3. Select a status option to enable or disable the identity provider settings.
4. Type a descriptive name for the identity provider.

Note

Deep Discovery Analyzer displays the name in the drop-down list on the **Log On** screen.

For more information, see *Logging On With Single Sign-On on page 2-3*.

5. Type a description.
6. Click **Select** or **Update** and choose the federation metadata file obtained from your identity provider.

   After importing the federation metadata file, the system displays the identity provider information.
7. Click **Save**.

Configuring Okta

Okta is a standards-compliant OAuth 2.0 authorization server that provides cloud identity solutions for your organization. Okta is a single sign-on provider that allows you to manage user access to Deep Discovery Analyzer.

This section describes how to configure Okta as a SAML (2.0) identity provider for Deep Discovery Analyzer to use.

Before you begin configuring Okta, make sure that:

- You have a valid subscription with Okta that handles the sign-in process and that eventually provides the authentication credentials to the Deep Discovery Analyzer management console.
- You are logged on to the management console as a Deep Discovery Analyzer administrator.

Procedure

1. Log in to your Okta organization as a user with administrative privileges.
2. Click **Admin** in the upper right, and then navigate to **Applications** > **Applications**.
3. Click **Add Application**, and then click **Create New App**.

   The **Create a New Application Integration** screen appears.
4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.
5. On the **General Settings** screen, type a name for Deep Discovery Analyzer in **App name**, for example, "Deep Discovery Analyzer", and click **Next**.
6. On the **Configure SAML** screen, specify the following:
   a. Type the Deep Discovery Analyzer address in the **Single sign on URL** field.
   b. Select **Use this for Recipient URL and Destination URL**.
   c. Specify the Audience URI in **Audience URI (SP Entity ID)** based on your serving site:
   d. For **Assertion Encryption**, select **Encrypted**.
   e. For **Encryption Certificate**, click **Browse files** to select the certificate file that you obtained from Deep Discovery Analyzer.

      For more information, see *Service Provider Metadata and Certificate on page 6-36*.
   f. In the **Group Attribute Statements (Optional)** section, specify the following:
      - **Name**: DDAN_groups
      - **Filter**: Matches regex ^(.*)*$
   g. Click **Next**.

7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, select **This is an internal app that we have created**, and then click **Finish**.

   The **Sign On** tab of your newly created Deep Discovery Analyzer application appears.

8. Click **Identity Provider Metadata** to download the metadata file from Okta.

   Note

   Import this metadata file to Deep Discovery Analyzer.

9. Assign the application to groups and add people to groups.

   a. Select **Directory** > **Groups**.

   b. Click the groups that you want to assign the application to, and then click **Manage Apps**.

      The **Assign Applications** screen appears.

   c. Locate Deep Discovery Analyzer you added and click **Assign**.

   d. Click **Manage People**.

      The **Add People to Groups** screen appears.

   e. Locate the user you want to allow access to Deep Discovery Analyzer and add the user to the Deep Discovery Analyzer group.

   f. Confirm that the application is assigned to the user and group.

      After assigning an application to a group, the system automatically assigns the application to all users in the group.

   g. Repeat the above steps to assign the application to more groups as necessary.

   You are now ready to configure Okta for single sign-on and create the required SAML groups in the Deep Discovery Analyzer management console.

Configuring Active Directory Federation Services

This section describes how to configure a federation server using Active Directory Federation Services (AD FS) to work with Deep Discovery Analyzer.

Note

Deep Discovery Analyzer supports connecting to the federation server using AD FS 4.0 and 5.0.

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

Before you begin configuring AD FS, make sure that:

- You have a Windows Server installed with AD FS 4.0 or AD FS 5.0 to serve as a federation server.
- You are logged on to the management console as a Deep Discovery Analyzer administrator.
- You have obtained the metadata file from Deep Discovery Analyzer.
- You have configured web browser settings on each endpoint to trust Deep Discovery Analyzer and the federation server.

  For more information, see *Configuring Endpoints for Single Sign-on through AD FS on page 6-44*.

Procedure

1. Go to **Start** > **All Programs** > **Administrative Tools** to open the AD FS management console.
2. Click **AD FS** in the left navigation, and under the **Action** area on the right, click **Add Relying Party Trust...**.
3. Complete settings on each tab of the **Add Relying Party Trust Wizard** screen.

a. On the **Welcome** tab, select **Claims aware** and click **Start**.

b. On the **Select Data Source** tab, select **Import data about the relying party from a file**, click **Browse** to select the metadata file you obtain from Deep Discovery Analyzer; then, click **Next**.

c. On the **Specify Display Name** tab, specify a display name for Deep Discovery Analyzer, for example, "Deep Discovery Analyzer", and click **Next**.

d. On the **Choose Access Control Policy** tab, select **Permit everyone** or **Permit specific group**. If you select **Permit specific group**, select one or more groups in **Policy**. Then, click **Next**.

e. On the **Ready to Add Trust** tab, click **Next**.

f. On the **Finish** tab, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** and click **Close**.

The **Edit Claim Rules** screen appears.

4. On the **Issuance Transform Rules** tab, click **Add Rule...**.

5. Complete settings on each tab of the **Add Transform Claim Rule Wizard** screen.

a. On the **Choose Rule Type** tab, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list, and click **Next**.

b. On the **Configure Claim Rule** tab, specify a claim rule name in the **Claim rule name** text box, and select **Active Directory** from the **Attribute store** drop-down list.

c. Select the **User-Principal-Name** LDAP attribute and specify **Name ID** as the outgoing claim type for the attribute.

d. Click **OK**.

TABLE 6-5. LDAP attribute

CLAIM RULE NAME	LDAP ATTRIBUTE	OUTGOING CLAIM TYPE
<user-defined rule name>	User-Principal-Name	Name ID

6. Configure settings for each AD group that you permitted in step 3d and to which you want to grant access to Deep Discovery Analyzer.

Note

- The following procedure shows you how to configure settings using the **Send Group Membership as a claim** rule for each AD group. If you want to grant access to users in a child group and its associated parent group, you must create a rule each for the child group and parent group.
- To customize settings based on your requirements, it is recommended that you use the **Send Claims using a Custom Rule** option.
- Make sure you set the outgoing claim type as **DDAN_groups**.

For more information, see https://success.trendmicro.com/solution/000258112.

a. Click **Add Rule...**.

   The **Add Transform Claim Rule Wizard** screen appears.

b. On the **Choose Rule Type** tab, select **Send Group Membership as a Claim** from the **Claim rule template** drop-down list, and click **Next**.

   The **Configure Claim Rule** tab appears.

c. For **Claim rule name**, type the name of the AD group.

d. For **User's group**, click **Browse** and then select the AD group.

e. For **Outgoing claim type**, type "`DDAN_groups`".

f. For **Outgoing claim value**, type the name of the AD group.

g. Click **Apply** and then click **OK**.

TABLE 6-6. Group membership rule

CLAIM RULE NAME	USER GROUP	OUTGOING CLAIM TYPE	OUTGOING CLAIM VALUE
<user-defined rule name>	<user group name in AD FS>	DDAN_groups	<user group name in AD FS>

7. Click **Apply** and then **OK**.

Configuring Endpoints for Single Sign-on through AD FS

Before endpoints can access Deep Discovery Analyzer using single sign-on through Active Directory Federation Services (AD FS), configure the web browser settings on each endpoint to trust both Deep Discovery Analyzer and the federation server.

You can configure the web browser settings on endpoints manually or through group policies.

The following provides the procedure for endpoints running Windows 10. Steps may vary depending on the Windows version.

Procedure

1. On an endpoint, open the **Control Panel** from the Start menu.
2. Click **Network and Internet** > **Internet Options**.

   The Internet Properties screen appears.
3. Click the **Security** tab.
4. Select **Local intranet** and click **Sites**.
5. Click **Advanced**.
6. In the **Add this website to the zone** field, type FQDN or IP address of the account federation server and click **Add**.
7. Repeat Step 6 to add the FQDN or IP address of Deep Discovery Analyzer to the Websites list.

8. Click **Close**.
9. Click **OK**.
10. Click **OK**.

Email Submission Tab

In addition to submitting objects using the management console and the Manual Submission Tool, you can enable the email submission feature to allow users to send suspicious email messages and attachments to Deep Discovery Analyzer for analysis.

The following provides an overview of the email submission process:

1. A user sends an email message with a suspicious attachment to Deep Discovery Analyzer.
2. Deep Discovery Analyzer receives the email message and scans the email content with the attachment.
3. After the analysis is complete, Deep Discovery Analyzer sends an email notification with the following to the user:
   - Analysis result summary
   - Detailed analysis report

Configuring Email Submission Settings

Procedure

1. Go to **Administration** > **Integrated Products/Services** and click the **Email Submission** tab.
2. Select **Enable Email Submission**.

Note

If you disable the email submissions feature, Deep Discovery Analyzer stops sending email notifications with analysis results for samples that Virtual Analyzer is currently processing.

3. In the General section, specify the email address that Deep Discovery Analyzer uses to receive email messages and send analysis result notifications. The default setting is `911@ddan.com`.

4. In the Email Senders section, specify the permitted user domains and SMTP servers that are allowed to send email messages to Deep Discovery Analyzer for analysis.

   - **Permitted domains**: Type a domain and press [Enter]. You can add up to five domains.
   - **Permitted SMTP servers**: Type an SMTP server address and press [Enter]. You can specify up to five server addresses.

     Configure the following settings for the SMTP server in Deep Discovery Analyzer:

     - **Port**: Type the server port number. The default is 25. This setting is required.
     - **SSL/TLS**: Select **Enable SSL/TLS** to establish a secure connection to the servers. Then, select the required certificate and private key files and the passphrase.

5. In the Email Notifications section, configure the SMTP server that Deep Discovery Analyzer uses to send email notifications with analysis results.

   a. Type the SMTP server host name, IPv4 address, or IPv6 address.

   b. Type the port number used by the SMTP server.

   c. Select the type of security used for the connection.

   d. If the server requires authentication, select **SMTP server requires authentication** and specify a user name and password.

   e. (Optional) Click **Test Connection** to test the connection to the SMTP server.

6. Specify the email subject and message content for the email notification template.

Tip

You can use the "%RiskLevel%" and "%Subject%" tokens in the notification email.

7. Click **Save**.

Syslog Tab

Deep Discovery Analyzer maintains system logs that provide summaries of the following:

- Virtual Analyzer analysis logs
- Integrated product detection logs
- ICAP pre-scan logs
- System events
- Alert events

Use the **Syslog** tab, in **Administration** > **Integrated Products/Services** > **Syslog**, to configure Deep Discovery Analyzer to send logs to multiple syslog servers.

Configuring Syslog Settings

Deep Discovery Analyzer can forward logs to multiple syslog servers after saving the logs to its database.

Note

- Deep Discovery Analyzer can be configured to forward logs to a maximum of 3 syslog servers.
- Only logs saved after enabling this setting are forwarded. Previous logs are excluded.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Syslog**.

   The **Syslog Settings** screen appears.

2. Perform one of the following:

   - To add a new syslog server, click **Add**.
   - To update the details of an existing syslog server, click the name of the syslog server to be updated.

3. On the screen that appears, specify the **Status** for the profile.

4. Type the **Profile name** and **Server address** of the syslog server.

5. Type the port number.

   Note

   Trend Micro recommends using the following default syslog ports:

   - **UDP**: 514
   - **TCP**: 601
   - **SSL**: 443

6. Select the protocol to transport log content to the syslog server.

   - UDP
   - TCP
   - SSL/TLS

7. Select the format in which event logs are sent to the syslog server.

   - **CEF**: Common Event Format (CEF) is an open log management standard developed by HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs.
   - **LEEF**: Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar. LEEF comprises an LEEF header, event attributes, and an optional syslog header.

- **Trend Micro Event Format (TMEF)**: Trend Micro Event Format (TMEF) is a customized event format developed by Trend Micro and is used by Trend Micro products for reporting event information.

8. Select the scope of logs to send to the syslog server:
   - Virtual Analyzer analysis logs
   - Integrated product detection logs
   - ICAP pre-scan logs
   - System event logs
   - Alert event logs
9. (Optional) Select the logs to exclude from sending to the syslog server.
10. Click **Save**.

System Settings

The **System Settings** screen, in **Administration** > **System Settings**, includes the following tabs:

- *HTTPS Certificate Tab on page 6-79*

Network Tab

Use this screen to configure the host name, the IPv4 and IPv6 addresses of the Deep Discovery Analyzer appliance, and other network settings (including the enforcement of TLS 1.2 or above).

An IPv4 address is required and the default is `192.168.252.2`. Modify the IPv4 address immediately after completing all deployment tasks.

Deep Discovery Analyzer uses the specified IP addresses to connect to the Internet when accessing Trend Micro hosted services, including the Smart Protection Network, the ActiveUpdate server, and Threat Connect. The IP addresses also determine the URLs used to access the management console.

You can select **Always use TLS 1.2 or above** to enhance data security for inbound and outbound connections on Deep Discovery Analyzer.

Note

- To be compliant with the Payment Card Industry Data Security Standard (PCI-DSS) v3.2, the appliance should use only TLS 1.2 or above for all inbound and outbound connections.
- Before you can configure this option, verify that the Deep Discovery Analyzer appliance is not in a high availability cluster. Detach passive primary appliances from the cluster at **Administration** > **System Settings** > **Cluster**.
- Ensure that the integrated products and services are using the latest version that supports TLS 1.2 or above. For details, see *TLS Support for Integrated Products/Services on page C-1*.
- Verify that the following products/services are configured to use TLS 1.2 or above.
  - The ActiveUpdate server source at **Administration** > **Updates** > **Component Update Settings** must use HTTPS.
  - The ICAP settings at **Administration** > **Integrated Products/Services** > **ICAP** must use ICAP over SSL.
  - The syslog servers at **Administration** > **Integrated Products/Services** > **Syslog** must use SSL.
  - The SMTP server at **Administration** > **System Settings** > **SMTP** must use SSL/TLS or STARTTLS.
  - The Email Submission settings at **Administration** > **Integrated Products/Services** > **Email Submission** must use SSL/TLS or STARTTLS.

The following table lists configuration limitations.

TABLE 6-7. Configuration Limitations

FIELD	LIMITATION
Host name	Cannot be modified when using high availability
IPv4 address	• Must differ from IPv4 virtual address • Must be in the same network segment as IPv4 virtual address
IPv6 address	• Must differ from IPv6 virtual address • Must be in the same network segment as IPv6 virtual address • Cannot be deleted if IPv6 virtual address has been configured • Cannot be added or deleted when using high availability

Network Interface Tab

You can use the **Network Interface** screen to perform the following:

- View network interface status
- Configure port settings

  For more information, see *Configuring Port Settings on page 6-52*.
- Configure NIC teaming

  For more information, see *Configuring NIC Teaming on page 6-53*.

Configuring Port Settings

Procedure

1. Go to **Administration** > **System Settings** > **Network Interface**.
2. Configure the settings under the Port List section.
   - To set the **Management Port** on the selected interface, select an option from the drop-down list. By default, Deep Discovery Analyzer uses the eth0 interface as the management port.
   - To configure the port settings for the interface used for sandbox analysis, click **Edit**.

- To view detailed information for the high availability port, click **View Details**.

3. Click **Save**.
4. When prompted to restart the network service, click **Yes**.

   The system restarts the network service. This may take some time. Wait for the process to complete before you can access the management console again.

Configuring NIC Teaming

A network interface card (NIC) team is a software-based virtual network interface that provides fault tolerance in the event of a network interface card failure.

Deep Discovery Analyzer supports up to two NIC teams. You must group two network interface cards in a NIC team.

Procedure

1. Go to **Administration** > **System Settings** > **Network Interface**.
2. Under the NIC Teaming section, do the following:
   a. Toggle the status button to enable a NIC team.
   b. Select a connection mode (**Active/Backup** or **LACP**).

Note

If you select **LACP**, you must also configure the required settings on the target switch to enable communication using LACP (Link Aggregation Control Protocol).

For example, if a NIC team contains the management port and functions as the management port using LACP, Deep Discovery Analyzer will not be able to establish communication with the target switch until the required settings are configured on the switch.

c. Select two network interface cards to add to the NIC team.

Note

- A network interface card can only belong to one NIC team.
- If a NIC team contains the management port (`eth0`) and a network port (`eth1`), the NIC team functions as the management port. If you disable this NIC team, either `eth0` or `eth1` will become the management port.

3. Click **Save**.
4. When prompted to restart the network service, click **Yes**.

   The system restarts the network service. This may take some time. Wait for the process to complete before you can access the management console again.

Proxy Tab

Specify proxy settings if Deep Discovery Analyzer connects to the Internet or management network through a proxy server.

Configure the following settings.

TABLE 6-8. Proxy Tab Tasks

TASK	STEPS
Use an HTTP proxy server	Select this option to enable proxy settings.
Server name or IP address	Type the proxy server host name or IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Port	Type the port number that Deep Discovery Analyzer uses to connect to the proxy server.

Task	Steps
Proxy server requires authentication	Select this option if the connection to the proxy server requires authentication. Deep Discovery Analyzer supports the following authentication methods: • No authentication • Basic authentication • Digest authentication • NTLMv1 authentication
User name	Type the user name used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.
Password	Type the password used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.

SMTP Tab

Deep Discovery Analyzer uses SMTP settings when sending notifications through email.

Procedure

1. Go to **Administration** > **System Settings** and click the **SMTP** tab.
2. Specify the following details:

TABLE 6-9. SMTP Tab Tasks

FIELD	STEPS
Server address	Type the SMTP server host name, IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Port	Type the port number used by the SMTP server.
Connection security	Specify the type of security used for the connection. Available values are: None, STARTTLS, SSL/TLS.
Sender email address	Type the email address of the sender.
SMTP server requires authentication	If the server requires authentication, select **SMTP server requires authentication** and specify a user name and password. **WARNING!** Ensure that the user name and password to be specified is valid for the SMTP server. Connections made using an incorrect user name and password may cause some SMTP servers to reject all network request originating from the Deep Discovery Analyzer server.

3. (Optional) To test the connection to the external SMTP server, do the following:

   a. Click **Test Connection**.

   b. Type the recipient email address.

   c. Click **OK**.

Note

Deep Discovery Analyzer does not send a test email message to the recipient.

4. Click **Save**.

Time Tab

Configure date and time settings immediately after installation.

Procedure

1. Go to **Administration** > **System Settings** and click the **Time** tab.

   The **Time** screen appears.

2. Click **Set date and time**.

   The settings panel appears.

3. Select one of the following methods and configure the applicable settings.

   - Select **Connect to an NTP server** and type the host name, IPv4 address, or IPv6 address of the NTP server.
   - Select **Set manually** and configure the time.

4. Click **Save**.

5. Click **Set time zone**.

   The settings panel appears.

6. Select the applicable time zone.

   Note

   Daylight Saving Time (DST) is used when applicable.

7. Click **Save**.

8. Click **Set format**.

   The settings panel appears.

9. Select the preferred date and time format.

10. Click **Save**.

SNMP Tab

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

On Deep Discovery Analyzer, use the **Administration** > **System Settings** > **SNMP** tab to perform the following tasks:

- Configure the appliance to send trap messages

  For details, see *Configuring Trap Messages on page 6-58*.

- Configure the appliance to listen for manager requests

  For details, see *Configuring Manager Requests on page 6-60*.

Configuring Trap Messages

A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Under **Trap Messages**, select **Send SNMP trap messages**.
3. Specify the trap message settings.

Option	Description
Manager server address	Specify the manager server address.

Option	Description
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: `""` (default context) • Context Engine ID: `<Auto>` • (Optional) MD5 Authentication protocol: `HMAC-MD5` • (Optional) AES Privacy protocol: `AES128`
Community name	Specify a community name.
Security model	Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	Specify the user name.
Password	Specify the password.
Privacy passphrase	Specify the privacy passphrase.

Note

Before configuring the appliance, set up the SNMP server first using the same SNMP version, community name, security model, user name, password, and privacy passphrase.

4. Click **Save**.
5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

- Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.
- For a list of Deep Discovery Analyzer supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request Deep Discovery Analyzer system information.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Under **Manager Requests**, select **Listen for requests from SNMP managers**.
3. Specify the manager request settings.

Option	Description
Device location	Specify the location of this appliance.
Administrator contact	Specify the administrator contact of this appliance.
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: `""` (default context) • Context Engine ID: `<Auto>` • (Optional) MD5 Authentication protocol: `HMAC-MD5` • (Optional) AES Privacy protocol: `AES128`

Option	Description
Allowed community names	Specify a maximum of 5 community names.
Security model	Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	Specify the user name.
Password	Specify the password.
Privacy passphrase	Specify the privacy passphrase.
Trusted manager server addresses	Specify a maximum of 5 trusted manager server addresses.

Note

Before configuring the appliance, set up the SNMP server first using the same SNMP version, community name, security model, user name, password, and privacy passphrase.

4. Click **Save**.
5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.
   - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.
   - For a list of Deep Discovery Analyzer supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

Password Policy Tab

Trend Micro recommends requiring strong passwords. Strong passwords usually contain a combination of both uppercase and lowercase letters, numbers, and symbols, and are at least eight characters in length.

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

Strict password policies sometimes increase costs to an organization when they force users to select passwords too difficult to remember. Users call the help desk when they forget their passwords, or record passwords and increase their vulnerability to threats. When establishing a password policy balance your need for strong security against the need to make the policy easy for users to follow.

Session Timeout Tab

At the logon screen of the management console, a user can choose default or extended session timeout.

The default session timeout is 10 minutes and the extended session timeout is one day. You can change these values according to your preference. New values take effect on the next logon.

Cluster Tab

Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.

Depending on your requirements and the number of Deep Discovery Analyzer appliances available, you may deploy the following cluster configurations:

TABLE 6-10. Cluster Configurations

CLUSTER CONFIGURATION	DESCRIPTION
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement. **Note** For all Deep Discovery Analyzer functions to operate properly in a load-balancing environment, make sure the primary and secondary appliances can communicate with each other.
High availability cluster with load balancing	In a high availability cluster with load balancing, one appliance acts as the active primary appliance, one acts as the passive primary appliance, and any additional appliances act as secondary appliances. The passive primary appliance takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.

For details, see the *Deep Discovery Analyzer Installation and Deployment Guide*.

The following table lists the available configuration modes and associated appliance behavior.

TABLE 6-11. Cluster Configuration Modes

CONFIGURATION MODE	DESCRIPTION
Primary (Active)	• Management console is fully accessible • Retains all configuration settings
Primary (Passive)	• Management console is unavailable • Automatically configured based on the settings of the active primary appliance • On standby • Takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover • Does not process submissions

Configuration Mode	Description

Secondary	• Automatically configured based on the settings of the active primary appliance
	• Identifies the active primary appliance using its IP address or virtual IP address
	• Processes submissions allocated by the active primary appliance for performance improvement
	• Management console only shows screens with configurable settings:
	  • **Virtual Analyzer** > **Sandbox Management** > **Network Connection**
	  • **Virtual Analyzer** > **Sandbox Management** > **Sandbox for macOS**
	  • **Administration** > **Updates** > **Hotfixes / Patches**
	  • **Administration** > **Updates** > **Firmware**
	  • **Administration** > **Integrated Products/Services** > **SAML Authentication**
	  • **Administration** > **System Settings** > **Network**
	  • **Administration** > **System Settings** > **Network Interface**
	  • **Administration** > **System Settings** > **HTTPS Certificate**
	  • **Administration** > **System Settings** > **Cluster**
	  • **Administration** > **Accounts / Contacts** > **Accounts**
	  • **Administration** > **System Logs**
	  • **Administration** > **System Maintenance** > **Network Services Diagnostics**
	  • **Administration** > **System Maintenance** > **Power Off / Restart**
	  • **Administration** > **System Maintenance** > **Debug**
	  • **Administration** > **License**

Note

In environments that use a load-balancing cluster or a High Availability cluster with load balancing, Deep Discovery Analyzer automatically slows down Virtual Analyzer throughput on the active primary appliance to prevent exhaustion of system resources

Nodes List

The **Nodes** list is displayed on the active primary appliance.

The Nodes list contains the following information:

TABLE 6-12. Nodes List Columns

COLUMN	DESCRIPTION
Status	Connection status of the appliance. Mouseover a status icon to view details.
Mode	Cluster mode of the appliance.
Management IP Address	Management IP address of the appliance.
Host Name	Host name of the appliance.
Last Connected	Date and time that the appliance last connected to the active primary appliance. **Note** No data (indicated by a dash) if the appliance is a passive primary appliance.
Details	Additional details about the operational status of the appliance. • For standalone appliance: • **Standalone appliance**: The appliance is a standalone appliance. • For passive primary appliance:

Column	Description
	• **Fully synced**: The passive primary appliance is fully synced to the active primary appliance. • **Syncing n%**: The passive primary appliance is syncing settings from the active primary appliance. • **Sync error**: The passive primary appliance is unable to connect to the active primary appliance. Verify that the appliances are directly connected using eth3, and that eth3 is not used for sandbox analysis. **Tip** This field also displays the connection latency and throughput information. • For secondary appliances: • **Inconsistent component version**: One or more components have different versions on the active primary appliance and secondary appliance. Use the same component versions on all appliances. • **Not connected**: The active primary appliance did not receive a heartbeat from the secondary appliance within the last 10 seconds. Verify that the secondary appliance is powered on and able to connect to the active primary appliance through the network. • **Invalid API key**: The secondary appliance is configured with an invalid API key. Verify the **Active primary API key** on the secondary appliance. • **Incompatible software version**: The firmware, hotfix, and patch versions on the active primary appliance and secondary appliance are different. Use the same firmware, hotfix, and patch version on all appliances. • **Unexpected error**: An unexpected error has occurred. If the issue persists, contact your support provider.
Action	Actions that can be executed depending on the appliance mode and status. • For active primary appliance:

Column	Description
	• **Swap**: Swap the roles of the primary appliances. Sets the current passive primary appliance to primary mode (active) and the current active primary appliance to primary mode (passive). Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Swapping the Active Primary Appliance and the Passive Primary Appliance on page 6-72* • For passive primary appliance: • **Detach**: Detach the passive primary appliance. Disables high availability and allows the passive primary appliance to be used as a standalone appliance. Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page 6-72* • **Remove**: Remove inaccessible passive primary appliance. Disables high availability. Appears when the active primary appliance is unable to reach the passive primary appliance through eth3. For details, see *Removing the Passive Primary Appliance from the Cluster on page 6-72* • For secondary appliances: • **Remove**: Remove inaccessible secondary appliance. Affects object processing capacity. Secondary appliances attempt to connect to the active primary appliance every 10 seconds. Appears when the active primary appliance does not receive a heartbeat from the secondary appliance within one minute. For details, see *Removing a Secondary Appliance from the Cluster on page 6-75*

Click **Refresh** to refresh the information in the **Nodes** list.

Adding a Passive Primary Appliance to the Cluster

The following table lists requirements that need to be fulfilled by both active primary appliance and passive primary appliance before the passive primary appliance can be added to the cluster.

TABLE 6-13. High Availability Clustering Requirements

REQUIREMENT	DESCRIPTION
Hardware model	Must be the same hardware model (1100 or 1200)

Physical connection	Recommended to connect to each other directly using eth3
	
	Important
	When using high availability, eth3 is used to connect the two identical appliances and cannot be used for other purposes (for example, as the management port, external network connection, or as a memeber port in a NIC team).
	
	Note
	• Deep Discovery Analyzer uses the IPv6 local-link IP address on the eth3 interface for high availability communication.
	• If the active primary appliance is not connected to the passive primary appliance directly (for example, if they are in different data centers), the following requirements must be met:
	  • The appliances must be Deep Discovery Analyzer 1100, 1200, or 1300.
	  • The connections between the appliances must meet the following conditions:
	  • Network latency is less than 15 ms
	  • Packet loss ratio is less than 0.000001%
	  • Network bandwidth is greater than 240Mbps

Firmware, hotfix, and patch version	Must be the same
Host name	Must be different

Requirement	Description
IP addresses	Must be symmetrical: • If only IPv4 address is configured on active primary appliance, passive primary appliance cannot configure both IPv4 address and IPv6 address. • If IPv4 address and IPv6 address are configured on active primary appliance, passive primary appliance cannot only configure IPv4 address.
Network segment	Must be in the same network segment
Virtual IP address	Must be configured on the active primary appliance
Management port	Must use the same network port
External connection port for Virtual Analyzer	Must use the same network port
NIC teaming	If configured, must use the same NIC teaming ports and connection type

In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.

Note

- If your network has Trend Micro Apex Central, only register the active primary appliance to Apex Central.
- When using high availability, use the virtual IP address to register.

Procedure

1. Perform the installation and deployment tasks as described in the *Deep Discovery Analyzer Installation and Deployment Guide*.

2. Configure the passive primary appliance.

   a. On the management console of the passive primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

   b. Select **Primary mode (passive)**.

   c. Type the IPv4 address or IPv6 address of the active primary appliance in **Active primary IP address**.

   d. Click **Test Connection**.

   e. Click **Save**.

      You will be redirected to the appliance standby screen.

- The passive primary appliance stops processing objects if it was previously doing so.
- The passive primary appliance will sync all settings from the active primary appliance. The total time to complete syncing depends on the appliance model.

  Important

  While the appliance is syncing, it cannot:

  - Take over as active primary appliance
  - Switch to another mode

- The management console of the passive primary appliance cannot be accessed. Manage the appliance and monitor the sync status from the management console of the active primary appliance.
- After you deploy Deep Discovery Analyzer in a high availibility cluster, you cannot change the settings for the following:
  - NIC teaming
  - Management port
  - External network connection

Swapping the Active Primary Appliance and the Passive Primary Appliance

Swapping the primary appliances sets the current passive primary appliance to primary mode (active) and the current active primary appliance to primary mode (passive).

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Click **Swap** to swap the primary appliances.

Detaching the Passive Primary Appliance from the Cluster

Detaching the passive primary appliance disables high availability and allows the appliance to be used as a standalone appliance. After a passive primary appliance is detached, it no longer appears in the nodes list.

Detach the passive primary appliance to update or upgrade the product.

Important

Detaching the passive primary appliance does not reset the appliance settings. Trend Micro recommends reinstalling the appliance if you want to use it as a standalone appliance.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Click **Detach** to detach the passive primary appliance from the cluster.

Removing the Passive Primary Appliance from the Cluster

Removing a disconnected or abnormal passive primary appliance from the cluster reduces the clutter in the nodes list.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Wait for **Remove** to appear next to the passive primary appliance in the nodes list.
3. Click **Remove** to remove the passive primary appliance from the cluster.

Note

The passive primary appliance automatically rejoins the cluster if it reconnects to the active primary appliance.

Adding a Secondary Appliance to the Cluster

Verify that the secondary appliance has the same firmware, hotfix, and patch version as the active primary appliance.

To view the appliance firmware, hotfix, and patch version, see *About Screen on page 6-105*.

Update or upgrade the appliance firmware, hotfix, and patch version as necessary. For details, see *Updates on page 6-2*.

Note

- If your network has Trend Micro Apex Central, only register the active primary appliance to Apex Central.
- When using high availability, use the virtual IP address to register.

Procedure

1. Perform the installation and deployment tasks as described in the *Deep Discovery Analyzer Installation and Deployment Guide*.
2. Configure the secondary appliance.

a. On the management console of the secondary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

b. Select **Secondary mode**.

c. Type the IPv4 address or IPv6 address of the active primary appliance in **Active primary IP address**.

Note

If you are using high availability, type the IPv4 virtual address or IPv6 virtual address.

d. Type the **Active primary API key**.

e. Click **Test Connection**.

Tip

Secondary appliances can test their connection to the active primary appliance at any time. Click **Test Connection** to get detailed information about any connectivity problems.

f. Click **Save**.

3. (Optional) Configure additional settings on the secondary appliance.

a. Configure the sandbox network connection setting.

For details, see *Enabling External Connections on page 4-66*.

Note

Trend Micro recommends using the external network connection setting of the active primary appliance.

b. Configure the **Sandbox for macOS** setting.

For details, see *Sandbox for macOS Tab on page 4-70*.

c. Configure the appliance network settings.

For details, see *Network Tab on page 6-50*.

d. Add accounts.

For details, see *Accounts Tab on page 6-84*.

Note

Secondary appliances automatically deploy sandbox instances based on the sandbox allocation ratio of the active primary appliance. The following table lists a configuration example:

TABLE 6-14. Example Configuration Using Two Images

APPLIANCE TYPE	DEEP DISCOVERY ANALYZER HARDWARE MODEL	MAXIMUM NUMBER OF INSTANCES (TOTAL)	NUMBER OF WINDOWS 7 INSTANCES	NUMBER OF WINDOWS 8.1 INSTANCES
Primary appliance	1200 or 1100	60	40	20
Secondary appliance	1200 or 1100	60	40	20

Removing a Secondary Appliance from the Cluster

Removing a disconnected secondary appliance from the cluster reduces the clutter in the nodes list and widgets of the active primary appliance.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Wait for **Remove** to appear next to the secondary appliance in the nodes list.

Note

Secondary appliances attempt to connect to the active primary appliance every 10 seconds. If the active primary appliance does not receive a heartbeat within one minute, **Remove** appears next to the secondary appliance in the **Nodes** list.

Secondary appliances automatically rejoin the cluster if they reconnect to the active primary appliance.

3. Click **Remove** to remove the secondary appliance from the cluster.

   The secondary appliance is removed from the nodes list and widgets of the active primary appliance.

Replacing the Active Primary Appliance with a Secondary Appliance

If the active primary appliance is unresponsive or cannot be restored, and no passive primary appliance is deployed, it can be replaced by a secondary appliance from the same cluster.

Tip

Trend Micro recommends deployment of a passive primary appliance for high availability. For details, see *Adding a Passive Primary Appliance to the Cluster on page 6-68*.

Important

Submissions do not have a result if they were being analyzed on the active primary appliance when it becomes unresponsive.

Procedure

1. Power off the active primary appliance.
2. Select a secondary appliance from the same cluster and configure it as the new active primary appliance.

a. On the management console of the secondary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

b. Select **Primary mode (active)**.

c. Click **Save**.

3. Configure the IP address of the new active primary appliance.

   For details, see *Network Tab on page 6-50*.

   Note

   Trend Micro recommends using the same IP address as the original active primary appliance. This allows secondary appliances and integrated products to connect without reconfiguration.

4. Verify the settings on the new active primary appliance.

   Note

   Settings take up to one day to propagate to secondary appliances.

Moving High Availability Cluster Appliances

Important

If you need to move high availability cluster appliances to another location, the passive node must always be powered off first and powered on last.

Procedure

1. Power off the passive primary appliance.
2. Power off the active primary appliance on the **Administration** > **System Maintenance** > **Power Off/Restart** tab.
3. Move both appliances to the new location.
4. Connect each appliance to the management network using eth0.

5. Connect both appliances directly to each other using eth3.
6. Power on the active primary appliance.
7. Power on the passive primary appliance.

Changing the IP Segment of High Availability Clusters

The management console supports changing the virtual IP address and management IP address only if they are in the same network segment. However, if you need to move the IP address to another network segment, nodes must be detached, re-configured and then set up again.

Procedure

1. Detach the passive primary appliance.
2. On active primary appliance UI, delete the virtual IP address, and then configure the management IP address and virtual IP address to match the IP address in the new network segment.
3. On passive primary appliance UI, configure the management IP address to match the IP address in the new network segment
4. Add the passive primary appliance to the cluster again.

High Availability Tab

Specify the IPv4 and IPv6 virtual addresses when using the appliance in a high availability configuration. The IPv4 and IPv6 virtual addresses are used to provide integrated products with fixed IP addresses for configuration, and also determine the URLs to access the management console.

Trend Micro recommends using the original IP address of the appliance as virtual IP address so that integrated products can continue submitting objects to Deep Discovery Analyzer without any modifications to their settings.

You can select the **Switch to passive primary appliance when external connection for Virtual Analyzer becomes unavailable** option to have Deep

Discovery Analyzer automatically switch to the passive primary appliance when the external connection for Virtual Analyzer becomes unavailable.

The following table lists configuration limitations.

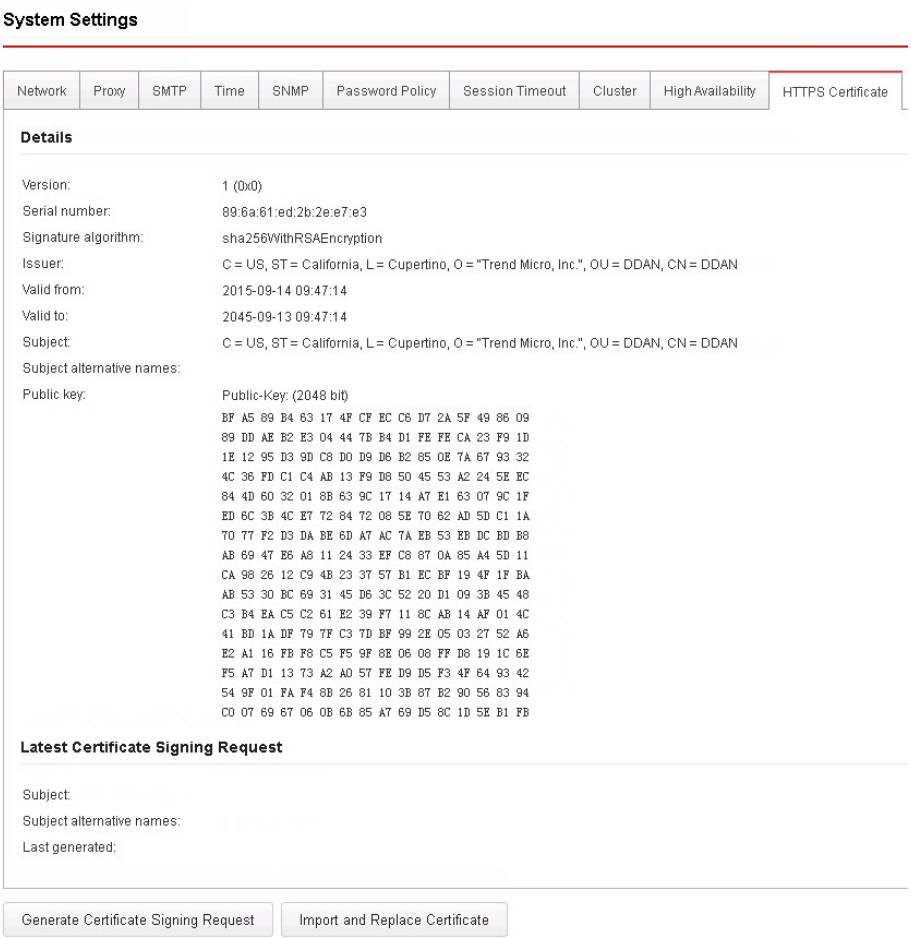
TABLE 6-15. Configuration Limitations when Using High Availability

FIELD	LIMITATION
IPv4 virtual address	• Cannot be used by another host • Must differ from IPv4 address • Must be in the same network segment as IPv4 address
IPv6 virtual address	• Cannot be used by another host • Must differ from IPv6 address • Must be in the same network segment as IPv6 address • Cannot be link-local • Can only be configured when IPv6 address has been configured

HTTPS Certificate Tab

You can update the HTTPS certificate in Deep Discovery Analyzer to enhance network communication security.

To view current certificate information, go to **Administration** > **System Settings** and click the **HTTPS Certificate** tab.



The following table describes the fields in the **Details** section.

TABLE 6-16. HTTPS certificate details

ITEM	DESCRIPTION
Version	Certificate version number

Item	Description
Serial number	Certificate unique identification number
Signature algorithm	Algorithm used to create the signature
Issuer	Entity that verified the information and issued the certificate
Valid from	Date the certificate is first valid
Valid to	Certificate expiration date
Subject	Person or entity identified
Subject alternative name	Additional user-specified domain names associated with the certificate
Public key	The 2048-bit or higher public key used for encryption

You can use the **HTTPS Certificate** screen to perform the following tasks:

- Generate a certificate signing request (CSR) to obtain a new certificate from a certificate authority (CA)

  For more information, see *Generating a Certificate Signing Request on page 6-81*.

- Import a new certificate to replace the existing certificate in Deep Discovery Analyzer

  For more information, see *Importing and Replacing a Certificate on page 6-83*.

Generating a Certificate Signing Request

You can generate a certificate signing request (CSR) in Deep Discovery Analyzer to apply for a new certificate from a certificate authority (CA).

Note

Deep Discovery Analyzer supports certificates in X.509 PEM format.

Procedure

1. Go to **Administration** > **System Settings** and click the **HTTPS Certificate** tab.
2. Click **Generate Certificate Signing Request**.
3. Configure the certificate signing request settings.

   The following table describes the fields.

Field	Description
Common name (CN)	Specify a domain name or the server host name.
Subject alternative names	Specify one or more domain names to associate with the generated certificate.
Organization (O)	Specify your company name.
Organization unit (OU)	Specify the name of your department within your company.
Country (C)	Specify the 2-character code for the country where your company is located.
State/Region (ST)	Specify the state or region where your company is located.
City/Locality (L)	Specify the city where your company is located.
Email address	Specify your email address.
Key type and size	Select one of the following options: • RSA (2048 bits) • RSA (4096 bits)

4. Click **Generate and Download**.

   After the certificate signing request is generated, the system automatically downloads the .csr file.

Importing and Replacing a Certificate

Important

Importing a certificate replaces the exiting certificate in Deep Discovery Analyzer.

Note

- To enhance web browser security, it is recommended you replace the default certificate in Deep Discovery Analyzer.
- Deep Discovery Analyzer supports certificates in X.509 PEM format.

Procedure

1. Go to **Administration** > **System Settings** and click the **HTTPS Certificate** tab.
2. Click **Import and Replace Certificate**.
3. Select the certificate file.
4. Click **Import and Replace**.

   After the process is complete, you can view the information for the new certificate on the **HTTPS Certificate** screen.

Accounts / Contacts

The **Accounts / Contacts** screen, in **Administration** > **Accounts / Contacts**, includes the following tabs:

- *Accounts Tab on page 6-84*
- *SAML Tab on page 6-88*
- *Contacts Tab on page 6-90*

Accounts Tab

Use the **Accounts** tab to create and manage user accounts.

Note

- In a cluster environment, the secondary Deep Discovery Analyzer appliance synchronizes all local user accounts (except the default administrator account (admin)) from the active primary appliance.
- If a synchronized account is used to log into the management console on the secondary appliance and the user has not changed the account password, the system prompts the user to change the account password.

Procedure

1. Go to **Administration** > **Accounts / Contacts**.
2. Click the **Accounts** tab.
3. Use the following options to manage user accounts:
   - To add a new user account, click **Add** .

     The **Add Account** window opens. For details, see *Configuring User Accounts on page 6-85*.
   - To delete an account, select one or more user accounts and click **Delete**.

     Important

     - You cannot delete the default Deep Discovery Analyzer administrator account.
     - You cannot delete the logged-on account.
   - To manually unlock an account, select a user account and click **Unlock**.

     Deep Discovery Analyzer includes a security feature that locks an account in case the user typed an incorrect password five

times in a row. This feature cannot be disabled. Locked accounts automatically unlock after ten minutes. The administrator can manually unlock accounts that have been locked.

Only one user account can be unlocked at a time.

4. To make changes to an existing account, click the user name of the account.

   The **Edit Account** window opens. For details, see *Configuring User Accounts on page 6-85*.

5. If there are many entries in the table, use the following options to manage the user accounts list:

   - Select an account type from the **Type** drop down to show only the accounts for a specific type.
   - Click the **Name** column to sort names alphabetically.
   - Type a few characters in the **Search** text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed. Deep Discovery Analyzer searches all cells in the current page for matches.
   - The panel at the bottom of the screen shows the total number of user accounts. If all user accounts cannot be displayed at the same time, use the pagination controls to view the accounts that are hidden from view.

Configuring User Accounts

Procedure

1. Go to **Administration** > **Accounts / Contacts**, and then go to the **Account** tab.
2. Do one of the following:
   - Click **Add** to create a new user account.

- Click the name of an existing user account to change the account settings.

3. To add a local account, select **Local user** as the account **Type** and provide the following details.

   - **Name**: Name of the account owner.
   - **User name**: User name supports a maximum of 40 characters.

     Note

     The user name is case insensitive for new account creation and management console logon process.

   - **Password**: Type a password that contains at least 8 characters and includes uppercase letters, lowercase letters, numbers, and special characters.

     Note

     - To increase password complexity requirements, configure the global password policy in **Administration** > **System Settings** > **Password Policy** tab. The password policy is displayed in the window and must be satisfied before you can add a user account.
     - When a user exceeds the number of retries allowed while entering incorrect passwords, Deep Discovery Analyzer sets the user account to inactive (locked). You can unlock the account on the **Accounts** screen.

   - **Confirm password**: Type the password again.
   - (Optional) **Description**: Description supports a maximum of 40 characters.

Note

If a new local user account is used to log into the management console for the first time, the system will prompt the user to change the account password.

4. To add an Active Directory user, select **Active Directory user** as the account **Type**, and provide the following details.

   - **User name or group**: Specify the User Principal Name (UPN) or user group name.

     Note

     To quickly locate a specific user name or group, type a few characters in the text box and click **Search**.

   - (Optional) **Description**: Description supports a maximum of 40 characters.

5. To change the password of a local account, select **Change password** and configure the required fields.

   Note

   - If you are logged in as an administrator, you can change the password of a local user account by typing the new password twice. You do not have to provide the original password for the local user account.
   - If the password of a local user account is changed by an administrator, the system will prompt the user to change the account password again upon login.

6. Select the role and associated permissions of the user account.

   - **Administrator**: Users have full access to submitted objects, analysis results, and product settings

- **Investigator**: Users can reanalyze submitted objects, submit objects, and download the investigation package (including submitted objects), and have read-only access to analysis results and product settings
- **Operator**: Users have read-only access to submitted objects, analysis results, and product settings

7. (Optional) Select **Add to contacts** to add the user account to the **Contacts** list, and provide the following details:

Note

Contacts receive email alert notifications by default.

- **Email address**
- (Optional) **Phone number**

8. Click **Save**.

SAML Tab

Once Deep Discovery Analyzer and the identity provider have established a trust relationship, Deep Discovery Analyzer can access the user identities on the identity provider's directory server. However, before Deep Discovery Analyzer can actually perform user authentication and authorization using the user identity information, you need to configure account types and SAML groups using groups, roles and claims.

The following provides a configuration overview to map a SAML account from identity provider to a user role in Deep Discovery Analyzer:

1. Create user accounts.
   a. Create user accounts.
   b. Create user groups and assign user accounts to the groups.

   For more information, see the documentation that comes with your identity provider.

2. In Deep Discovery Analyzer, create SAML groups with the specified roles and claims.

   For more information, see *Configuring SAML Groups on page 6-89*.

Configuring SAML Groups

Configure SAML groups in Deep Discovery Analyzer to map to user groups in your identity provider.

Procedure

1. Go to **Administration** > **Accounts / Contacts** and click the **SAML** tab.
2. Do one of the following:
   - Click **Add** to create a SAML group.
   - Click the name of a SAML group to configure the settings.
3. Select a status option to enable or disable the SAML group.
4. Type the group name for Deep Discovery Analyzer as the claim value.

   Important

   A claim value is case insensitive when you configure a new SAML group on the **SAML** screen. During the single sign-on process, SAML group mapping is also case insensitive.

5. (Optional) Type a description for the SAML group.
6. Select the role and associated permissions of the SAML group.
   - **Administrator**: Users have full access to submitted objects, analysis results, and product settings
   - **Investigator**: Users can reanalyze submitted objects, submit objects, and download the investigation package (including submitted objects), and have read-only access to analysis results and product settings

- **Operator**: Users have read-only access to submitted objects, analysis results, and product settings

7. Click **Save**.

Note

You cannot delete a SAML group with a logged-on account.

Contacts Tab

Use the **Contacts** tab, in **Administration** > **Accounts / Contacts**, to maintain a list of contacts who are interested in the data that your logs collect.

This screen includes the following options.

TABLE 6-17. Contacts Tasks

TASK	STEPS
Add Contact	Click **Add Contact** to add a new account. This opens the **Add Contact** window, where you specify contact details. For details, see *Add Contact Window on page 6-91*.
Edit	Select a contact and then click **Edit** to edit contact details. This opens the **Edit Contact** window, which contains the same settings as the **Add Contact** window. For details, see *Add Contact Window on page 6-91*. Only one contact can be edited at a time.
Delete	Select one or more contacts to delete and then click **Delete**.
Sort Column Data	Click a column title to sort the data below it.
Search	If there are many entries in the table, type some characters in the Search text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed. Deep Discovery Analyzer searches all cells in the table for matches.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of contacts. If all contacts cannot be displayed at the same time, use the pagination controls to view the contacts that are hidden from view.

Add Contact Window

The **Add Contact** window appears when you click **Add Contact** on the **Contacts** tab.

This window includes the following options.

TABLE 6-18. Add Contact Window

FIELD	DETAILS
Name	Type the contact name.
Email address	Type the contact's email address.
Phone	(Optional) Type the contact's phone number.
Description	(Optional) Type a description that does not exceed 40 characters.

System Logs

Deep Discovery Analyzer maintains system logs that provide summaries about user access, component updates, setting changes, and other configuration modifications that occurred using the management console.

Deep Discovery Analyzer stores system logs in the appliance hard drive.

Querying System Logs

Procedure

1. Go to **Administration** > **System Logs**.
2. Select a type.
   - **All**
   - **System Setting**
   - **Account Logon/Logoff**
   - **System Update**

3. Select a period or specify a custom range using the calendar and sliders.
4. (Optional) Type a keyword in the **User name** field and click the Loupe icon to only display system logs whose user names contain the keyword.
5. Click **Export All** to export the system log to a `.csv` file.

System Maintenance

The **System Maintenance** screen, in **Administration** > **System Maintenance**, includes the following tabs:

- *Back Up Tab on page 6-92*
- *Restore Tab on page 6-96*
- *Configuring Storage Maintenance Settings on page 6-97*
- *Network Services Diagnostics Tab on page 6-98*
- *Power Off / Restart Tab on page 6-99*
- *Debug Tab on page 6-99*

Back Up Tab

The **Back Up** tab contains the following sections:

- *Configuration Settings Backup on page 6-93*
- *Data Backup on page 6-94*
- *Data Backup Status on page 6-95*

Note

The Data Backup Status section displays on the **Data Backup** screen if you configure Deep Discovery Analyzer to back up data on both primary and secondary nodes in a cluster.

For more information, see *Configuring Storage Maintenance Settings on page 6-97*.

Configuration Settings Backup

Deep Discovery Analyzer can export a backup file of most configuration settings.

To download the configuration settings backup file, click **Export**.

The following table shows the screens and tabs with backed up configuration settings.

TABLE 6-19. Backed Up Configuration Settings

SCREEN	TAB
Dashboard	Widget settings only
Virtual Analyzer > **Submissions**	Custom column and advanced filter settings
Virtual Analyzer > **Suspicious Objects**	**User-defined Suspicious Objects**
Virtual Analyzer > **Exceptions**	Not applicable
Virtual Analyzer > **Sandbox Management**	**File Passwords**
	Scan Settings
	Interactive Mode
	Smart Feedback
	Sandbox for macOS
	YARA Rules
Virtual Analyzer > **Network Shares**	Not applicable
Alerts / Reports > **Alerts**	**Rules**
Alerts / Reports > **Report**	**Schedules**
	Customization
Administration > **Updates**	**Component Update Settings**
Administration > **Integrated Products/ Services**	**Smart Protection**

Screen	Tab
	ICAP
	Microsoft Active Directory
	Email Submission
	Syslog
Administration > **System Settings**	**Network** (secure protocol settings)
	Proxy
	SMTP
	Time (time zone and format)
	SNMP
	Password Policy
	Session Timeout
Administration > **Accounts / Contacts**	**Accounts**
	SAML
	Contacts
Administration > **System Maintenance**	Data back up
	Storage Maintenance

Data Backup

Deep Discovery Analyzer automatically exports submission records, analysis results, and objects to a remote server you specify on the **Storage Maintenance** screen.

Investigation package data is periodically purged based on available storage space. To ensure availability of the data, Trend Micro recommends backing up the data to an external server. For details, see *Investigation Package Data Retention on page 4-37*.

Procedure

1. On the **Administration** > **System Maintenance** screen, click the **Back Up** tab.
2. Select **Automatically back up to remote server**.
3. Select the server type.
   - **SFTP server**
   - **FTP server**
4. Type the following information.
   a. **Host name or IP address**: The host name, IPv4 address, or IPv6 address of the backup server.
   b. **Port**: The port number of the backup server.
   c. (Optional) **Folder**: The backup folder path. The default value is the root folder.
   d. **User name**: The user name used for authentication.
   e. **Password**: The password used for authentication.
5. Click **Test Server Connection** to verify the connection to the primary backup server.
6. Select the scope of the data to back up.
   - **All submissions**
   - **High/Medium/Low risk**
   - **High risk only**
7. Click **Save**.

Data Backup Status

If you configure Deep Discovery Analyzer to back up data on both primary and secondary nodes in a cluster, you can view the data backup status on secondary nodes on the **Data Backup** screen.

For more information about configuring data backup settings on cluster nodes, see *Configuring Storage Maintenance Settings on page 6-97*.

The following table describes the information in the Data Backup Status section.

Field	Description
Mode	This field displays the cluster configuration mode associated with the appliance.
IP address	This field displays the IP address of the appliance.
Host name	This field displays the host name of the appliance.
Last backup	This field displays the data backup status or the time the appliance last updated data from the primary node.

Restore Tab

The **Restore** tab restores configuration settings from a backup file.

For information on creating a backup file of the configuration settings, see *Back Up Tab on page 6-92*.

Important

If the Deep Discovery Analyzer license is not activated, the **Sandbox for macOS** setting is not restored.

Procedure

1. Click **Choose File** or **Browse**.
2. Select the backup file.
3. Select one of the following restore options:
   - Restore all configuration settings
   - Restore all configuration settings except network share settings

- Restore only network share settings

4. Click **Restore**.

Configuring Storage Maintenance Settings

You can use the **Storage Maintenance** screen to specify the cluster node to store analysis results and control the amount of logs that Deep Discovery Analyzer saves.

Procedure

1. Go to **Administration** > **System Maintenance** and click the **Storage Maintenance** tab.
2. In the Analysis Results section, select the node location to store analysis results.
   - **Primary node**: Select this option to store all analysis results (for samples analyzed on both the primary and secondary nodes) on the primary node

     Note

     Selecting this option may increase storage utilization on the primary node.

   - **Primary and secondary nodes**: Select this option to store analysis results on the node that scanned the sample. For example, if a sample is analyzed on a secondary node, the result is stored on the node itself and is not sent to the primary node.

     Note

     You can view the data backup status for secondary nodes on the **Data Backup** screen.

3. In the Detection Logs section, configure the following settings:

- **Delete logs older than**: Specify the number of days to keep logs

  Note

  The specified value must be between 1 and 100.

- **Delete logs when the total free disk space is lower than**: Specify the disk space threshold for automatic log deletion and select the type of logs to delete (all logs or prioritize log deletion based on detection risk)

  Note

  - The threshold value must be between 10 and 90.
  - Deep Discovery Analyzer purges 10% more than the specified percentage.
  - If you select **Delete logs for non-malicious sample detections first**, system performance may be affected since Deep Discovery Analyzer checks and deletes one log at a time.

4. Click **Save**.

Network Services Diagnostics Tab

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.

Procedure

1. Select one or more enabled services and click **Test**.

   Wait for the connection test to complete. The time required depends on the network environment and the number of services selected. View the connection test result in the **Result** column.

Power Off / Restart Tab

You can power off or restart the Deep Discovery Analyzer appliance on the management console.

- **Power Off**: All active tasks are stopped, and then the appliance gracefully shuts down.
- **Restart**: All active tasks are stopped, and then the appliance is restarted.

Powering off or restarting the appliance affects the following:

- Virtual Analyzer object analysis: Integrated products may queue objects or skip submission while the appliance is unavailable.
- Active configuration tasks initiated by all users: Trend Micro recommends verifying that all active tasks are completed before proceeding.

Debug Tab

You can use the **Debug** tab to generate and configure debug logs for troubleshooting.

Procedure

1. Specify how events will be shown in the debug logs.
   a. Under the **Debug Level Settings** section, review the default debug levels assigned to the following events:
      - Virtual Analyzer Sensor
      - Virtual Analyzer
      - Scan Flow
      - Cluster
      - Notification
      - Trend Micro Apex Central
      - SNMP

- Deep Discovery Director
- Product Integration
- Operational Report
- ICAP Server
- Management Console
- Network Shares
- Trend Vision One
- Email Submission
- Others

b. To customize the debug level for the following events, click the current level assigned and select another value.

c. Click **Save**.

d. To return all debug level settings to their default values, click **Restore Default**.

2. Collect debug logs.

a. In the **Log Collection** section, determine the appliance where the log collection task should run.

For active primary appliances, Deep Discovery Analyzer always shows the active primary appliance as the first entry.

For passive primary appliances, Deep Discovery Analyzer shows the host name of the passive primary appliance for easier identification.

b. Click **Collect Debug Logs** for the selected appliance.

c. Wait for the task to complete.

d. Click **Download Debug log** to save the debug logs.

Note

For debug logs of the passive primary appliance, go to the management console of the active primary appliance.

For debug logs of a secondary appliance, go to the management console of the secondary appliance.

Tools

Use the **Tools** screen, in **Administration** > **Tools**, to view and download special tools for Deep Discovery Analyzer.

Each tool displayed on this screen has the following two options:

- **Usage Instructions**: This links to a relevant page in the online help with instructions about how to use the tool.
- **Download**: This links to the relevant page in the download center that has the tool.

Virtual Analyzer Image Preparation Tool

Use the Virtual Analyzer Image Preparation Tool before importing an image to Virtual Analyzer. The Virtual Analyzer Image Preparation Tool checks that an image has the correct virtual machine settings, supported platforms and required applications.

For details about the Virtual Analyzer Image Preparation Tool, see the *Virtual Analyzer Image Preparation Tool User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Manual Submission Tool

Use the Manual Submission Tool to remotely submit samples from locations on users' computers to Deep Discovery Analyzer. This feature allows users to submit multiple samples at once, which are added to the **Submissions** queue.

Follow the steps below to download, configure and use the Manual Submission Tool.

Procedure

1. Record the following information to use with the Manual Submission Tool.

   a. API key: This is available on the Deep Discovery Analyzer management console, in **Help** > **About**.

   b. Deep Discovery Analyzer IP address: If unsure of the IP address, check the URL used to access the Deep Discovery Analyzer management console. The IP address is part of the URL.

2. In **Administration** > **Tools**, click the **Download** link for the Manual Submission Tool.

   The Trend Micro **Software Download Center** window appears.

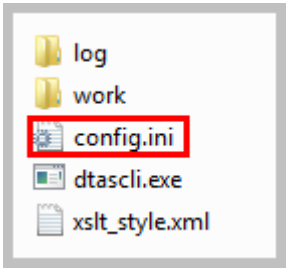
3. Click the download icon next to the latest version.

   A window providing different download options appears.

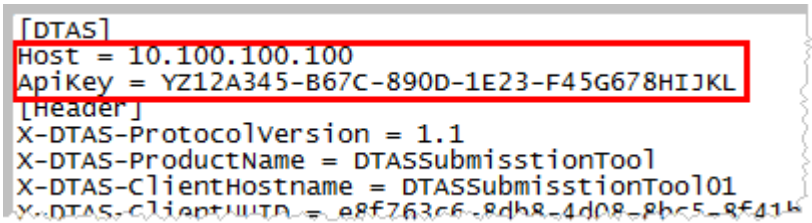
4. Click **Use HTTP Download**.

5. Extract the tool package.

6. In the folder where the tool was extracted, open `config.ini`.



7. Next to `Host`, type the Deep Discovery Analyzer IP address. Next to `ApiKey`, type the Deep Discovery Analyzer API Key. Save `config.ini`.



8. Submit the samples. For details, see *Manually Submitting Objects on page 4-27*.

License

Use the **License** screen, in **Administration** > **License**, to view, activate, and renew the Deep Discovery Analyzer license.

The Deep Discovery Analyzer license includes product updates (including ActiveUpdate) and basic technical support ("Maintenance") for one (1) year from the date of purchase. The license allows you to upload threat samples for analysis, and to access Trend Micro Threat Connect from Virtual Analyzer. In addition, the license allows you to send samples to the Trend Micro cloud sandboxes for analysis.

After the first year, Maintenance must be renewed on an annual basis at the current Trend Micro 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.

The Maintenance Agreement has an expiration date. Your License Agreement does not. If the Maintenance Agreement expires, you will no longer be entitled to receive technical support from Trend Micro or access Trend Micro Threat Connect.

Typically, 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 Customer Licensing Portal at:

https://clp.trendmicro.com/fullregistration

The **License** screen includes the following information and options.

TABLE 6-20. Product Details

FIELD	DETAILS
Product name	Displays the name of the product.
Firmware version	Displays the full build number of the product.
License agreement	Displays a link to the **Trend Micro License Agreement**. Click the link to view or print the license agreement.

TABLE 6-21. License Details

FIELD	DETAILS
Activation Code	View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code. The **License** screen reappears displaying the number of days left before the product expires.
Status	Displays either **Activated**, **Not Activated**, **Grace Period**, **Expired**, or **Evaluation Expired**. Click **View details online** to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated in the screen, click **Refresh**.
Type	• Full: Provides access to all product features • Evaluation: Provides access to all product features
Expiration date	View the expiration date of the license. Renew the license before it expires.

The following table describes the consequences when the product license expires.

TABLE 6-22. License expiry

LICENSE TYPE	STATUS	DETAILS
Full	Grace period	Technical support and component updates are available.
Full	Expired	Technical support and component updates are not available. Deep Discovery Analyzer still analyzes samples using out-of-date components. These components may not be able to protect your network completely from the latest security risks.
Evaluation	Expired	Deep Discovery Analyzer disables the following: • Component updates • Virtual Analyzer sample analysis • Trend Micro Sandbox for macOS sample analysis

About Screen

Use the **About** screen in **Help** > **About** to view the firmware version, API key, and other product details.

Note

The API key is used by Trend Micro products to register and send samples to Deep Discovery Analyzer. For a list of products and supported versions, see *Integration with Trend Micro Products on page 2-6*.

Chapter 7

Technical Support

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

   Tip

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

   https://success.trendmicro.com/smb-new-request

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

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

Contacting Trend Micro

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

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

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- ※

  ※

- Trend Micro product documentation:

https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://servicecentral.trendmicro.com/en-us/ers/

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

https://success.trendmicro.com/solution/1112106

File Reputation Services

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

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

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

https://global.sitesafety.trendmicro.com/

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

Other Resources

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

Download Center

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

https://www.trendmicro.com/download/

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

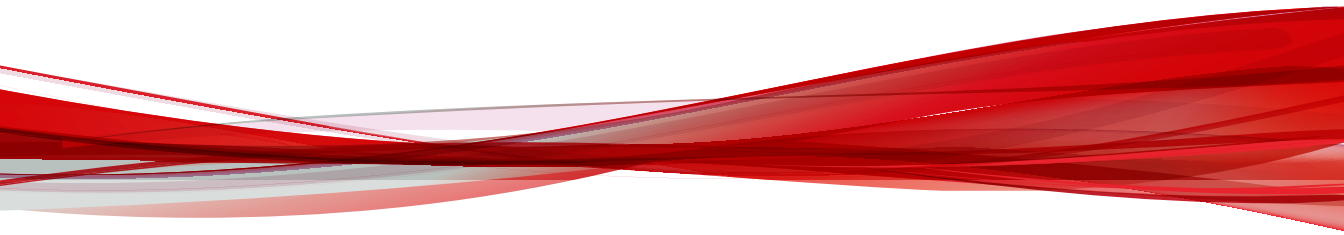
Documentation Feedback

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

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

Appendices

Appendices



Appendix A

Service Addresses and Ports

Deep Discovery Analyzer accesses several Trend Micro services to obtain information about emerging threats and to manage your existing Trend Micro products. The following table describes each service and provides the required address and port information accessible to the product version in your region.

TABLE A-1. Service Addresses and Ports

SERVICE	DESCRIPTION	ADDRESS AND PORT
ActiveUpdate Server	Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.	`ddan70-p.activeupdate.trendmicro.com/activeupdate/:443`
Certified Safe Software Service (CSSS)	Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources.	`grid-global.trendmicro.com/ws/level-0/files:443`
Sandbox as a Service (for macOS)	A hosted service that analyzes possible threats for macOS.	`ddaaas.trendmicro.com:443`

Service	Description	Address and Port
Community Domain/IP Reputation Service	Determines the prevalence of detected domains and IP addresses. Prevalence is a statistical concept referring to the number of times a domain or IP address was detected by Trend Micro sensors at a given time.	`ddan750-en-domaincensus.trendmicro.com:443`
Community File Reputation	Determines the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time.	`ddan750-en-census.trendmicro.com`
Customer Licensing Portal	Manages your customer information, subscriptions, and product or service license.	`licenseupdate.trendmicro.com/ollu/license_update.aspx:443`
Dynamic URL Scanning	Performs real-time analysis of URLs to detect zero-day attacks.	`ddan7-5-en-t0.url.trendmicro.com` `ddan7-5-en-backup-t0.url.trendmicro.com`
Predictive Machine Learning engine	Through use of malware modeling, Predictive Machine Learning compares samples to the malware models, assigns a probability score, and determines the probable malware type that a file contains.	`ddan70-en-f.trx.trendmicro.com:443`
Smart Feedback	Shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains.	`ddan700-en.fbs25.trendmicro.com:443`

Service	Description	Address and Port
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.	`ddan70-threatconnect.trendmicro.com:443`
Web Inspection Service	Web Inspection Service is an auxiliary service of Web Reputation Services, providing granular levels of threat results and comprehensive threat names to users. The threat name and severity can be used as filtering criteria for proactive actions and further intensive scanning.	`ddan7-5-en-wis.trendmicro.com:443`

Web Reputation Services	Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis.	`ddan7-5-en.url.trendmicro.com`
		
		`ddan7-5-en-backup.url.trendmicro.com`

Appendix B

SNMP Object Identifiers

Topics include:

SNMP Query Objects

TABLE B-1. system

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1
Object name	system
Description	System

TABLE B-2. sysDescr

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1.1
Object name	sysDescr
Description	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.

TABLE B-3. sysObjectID

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1.2
Object name	sysObjectID
Description	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor `Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its `Fred Router'.

TABLE B-4. sysUpTime

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1.3

Item	Description
Object name	sysUpTime
Description	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Table B-5. sysContact

Item	Description
OID	.1.3.6.1.2.1.1.4
Object name	sysContact
Description	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.

Table B-6. sysName

Item	Description
OID	.1.3.6.1.2.1.1.5
Object name	sysName
Description	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.

Table B-7. sysLocation

Item	Description
OID	.1.3.6.1.2.1.1.6
Object name	sysLocation
Description	The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string.

TABLE B-8. sysServices

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1.7
Object name	sysServices
Description	A value which indicates the set of services that this entity may potentially offer. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., supports the IP) 4 end-to-end (e.g., supports the TCP) 7 applications (e.g., supports the SMTP) For systems including OSI protocols, layers 5 and 6 may also be counted.

TABLE B-9. sysORLastChange

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.1.8
Object name	sysORLastChange
Description	The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.

TABLE B-10. interfaces

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.2
Object name	interfaces
Description	Interfaces

TABLE B-11. ifNumber

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.2.1
Object name	ifNumber
Description	The number of network interfaces (regardless of their current state) present on this system.

TABLE B-12. ifTable

ITEM	DESCRIPTION
OID	.1.3.6.1.2.1.2.2
Object name	ifTable
Description	A list of interface entries. The number of entries is given by the value of ifNumber.

TABLE B-13. memIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.1
Object name	memIndex
Description	Bogus Index. This should always return the integer 0.

TABLE B-14. memErrorName

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.2

Item	Description
Object name	memErrorName
Description	Bogus Name. This should always return the string 'swap'.

Table B-15. memTotalSwap

Item	Description
OID	.1.3.6.1.4.1.2021.4.3
Object name	memTotalSwap
Description	The total amount of swap space configured for this host.

Table B-16. memAvailSwap

Item	Description
OID	.1.3.6.1.4.1.2021.4.4
Object name	memAvailSwap
Description	The amount of swap space currently unused or available.

Table B-17. memTotalReal

Item	Description
OID	.1.3.6.1.4.1.2021.4.5
Object name	memTotalReal
Description	The total amount of real/physical memory installed on this host.

Table B-18. memAvailReal

Item	Description
OID	.1.3.6.1.4.1.2021.4.6
Object name	memAvailReal
Description	The amount of real/physical memory currently unused or available.

TABLE B-19. memTotalFree

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.11
Object name	memTotalFree
Description	The total amount of memory free or available for use on this host. This value typically covers both real memory and swap space or virtual memory.

TABLE B-20. memMinimumSwap

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.12
Object name	memMinimumSwap
Description	The minimum amount of swap space expected to be kept free or available during normal operation of this host. If this value (as reported by 'memAvailSwap(4)') falls below the specified level, then 'memSwapError(100)' will be set to 1 and an error message made available via 'memSwapErrorMsg(101)'.

TABLE B-21. memShared

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.13
Object name	memShared
Description	The total amount of real or virtual memory currently allocated for use as shared memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose.

TABLE B-22. memBuffer

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.14
Object name	memBuffer

Item	Description
Description	The total amount of real or virtual memory currently allocated for use as memory buffers. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose.

Table B-23. memCached

Item	Description
OID	.1.3.6.1.4.1.2021.4.15
Object name	memCached
Description	The total amount of real or virtual memory currently allocated for use as cached memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as reserved for this purpose.

Table B-24. memSwapError

Item	Description
OID	.1.3.6.1.4.1.2021.4.100
Object name	memSwapError
Description	Indicates whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)').

Table B-25. memSwapErrorMsg

Item	Description
OID	.1.3.6.1.4.1.2021.4.101
Object name	memSwapErrorMsg
Description	Describes whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)').

TABLE B-26. dskIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.1
Object name	dskIndex
Description	Integer reference number (row number) for the disk mib.

TABLE B-27. dskPath

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.2
Object name	dskPath
Description	Path where the disk is mounted.

TABLE B-28. dskDevice

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.3
Object name	dskDevice
Description	Path of the device for the partition.

TABLE B-29. dskMinimum

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.4
Object name	dskMinimum
Description	Minimum space required on the disk (in kBytes) before the errors are triggered. Either this or dskMinPercent is configured via the agent's snmpd.conf file.

TABLE B-30. dskMinPercent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.5

Item	Description
Object name	dskMinPercent
Description	Percentage of minimum space required on the disk before the errors are triggered. Either this or dskMinimum is configured via the agent's snmpd.conf file.

Table B-31. dskPercent

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.9
Object name	dskPercent
Description	Percentage of space used on disk.

Table B-32. dskPercentNode

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.10
Object name	dskPercentNode
Description	Percentage of inodes used on disk.

Table B-33. dskTotalLow

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.11
Object name	dskTotalLow
Description	Total disk/partion size (kByte). Together with dskTotalHigh forms a 64-bit number.

Table B-34. dskTotalHigh

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.12
Object name	dskTotalHigh

Item	Description
Description	Total disk/partion size (kByte). Together with dskTotalLow forms a 64-bit number.

Table B-35. dskAvailLow

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.13
Object name	dskAvailLow
Description	Available disk space (kByte). Together with dskAvailHigh forms a 64-bit number.

Table B-36. dskAvailHigh

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.14
Object name	dskAvailHigh
Description	Available disk space (kByte). Together with dskAvailLow forms a 64-bit number.

Table B-37. dskUsedLow

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.15
Object name	dskUsedLow
Description	Disk space used (kByte). Together with dskUsedHigh forms a 64-bit number.

Table B-38. dskUsedHigh

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.16
Object name	dskUsedHigh

Item	Description
Description	Disk space used (kByte). Together with dskUsedLow forms a 64-bit number.

Table B-39. dskErrorFlag

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.100
Object name	dskErrorFlag
Description	Error flag indicating that the disk or partition is under the minimum required space configured for it.

Table B-40. dskErrorMsg

Item	Description
OID	.1.3.6.1.4.1.2021.9.1.101
Object name	dskErrorMsg
Description	A text description providing a warning and the space left on the disk.

Table B-41. laTable

Item	Description
OID	.1.3.6.1.4.1.2021.10
Object name	laTable
Description	Load average information

Table B-42. ssIndex

Item	Description
OID	.1.3.6.1.4.1.2021.11.1
Object name	ssIndex
Description	Bogus Index. This should always return the integer 0.

TABLE B-43. ssErrorName

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.2
Object name	ssErrorName
Description	Bogus Name. This should always return the string 'systemStats'.

TABLE B-44. ssSwapIn

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.3
Object name	ssSwapIn
Description	The average amount of memory swapped in from disk, calculated over the last minute.

TABLE B-45. ssSwapOut

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.4
Object name	ssSwapOut
Description	The average amount of memory swapped out to disk, calculated over the last minute.

TABLE B-46. ssIOSent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.5
Object name	ssIOSent
Description	The average amount of data written to disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'ssIORawSent(57)', which can be used to calculate the same metric, but over any desired time period.

TABLE B-47. ssIOReceive

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.6
Object name	ssIOReceive
Description	The average amount of data read from disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'ssIORawReceived(58)', which can be used to calculate the same metric, but over any desired time period.

TABLE B-48. ssSysInterrupts

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.7
Object name	ssSysInterrupts
Description	The average rate of interrupts processed (including the clock) calculated over the last minute. This object has been deprecated in favour of 'ssRawInterrupts(59)', which can be used to calculate the same metric, but over any desired time period.

TABLE B-49. ssSysContext

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.8
Object name	ssSysContext
Description	The average rate of context switches, calculated over the last minute. This object has been deprecated in favour of 'ssRawContext(60)', which can be used to calculate the same metric, but over any desired time period.

TABLE B-50. ssCpuUser

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.9
Object name	ssCpuUser

Item	Description
Description	The percentage of CPU time spent processing user-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawUser(50)', which can be used to calculate the same metric, but over any desired time period.

Table B-51. ssCpuSystem

Item	Description
OID	.1.3.6.1.4.1.2021.11.10
Object name	ssCpuSystem
Description	The percentage of CPU time spent processing system-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawSystem(52)', which can be used to calculate the same metric, but over any desired time period.

Table B-52. ssCpuIdle

Item	Description
OID	.1.3.6.1.4.1.2021.11.11
Object name	ssCpuIdle
Description	The percentage of processor time spent idle, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawIdle(53)', which can be used to calculate the same metric, but over any desired time period.

Table B-53. ssCpuRawUser

Item	Description
OID	.1.3.6.1.4.1.2021.11.50
Object name	ssCpuRawUser
Description	The number of 'ticks' (typically 1/100s) spent processing user-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-54. ssCpuRawNice

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.51
Object name	ssCpuRawNice
Description	The number of 'ticks' (typically 1/100s) spent processing reduced-priority code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-55. ssCpuRawSystem

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.52
Object name	ssCpuRawSystem
Description	The number of 'ticks' (typically 1/100s) spent processing system-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). This object may sometimes be implemented as the combination of the 'ssCpuRawWait(54)' and 'ssCpuRawKernel(55)' counters, so care must be taken when summing the overall raw counters.

TABLE B-56. ssCpuRawIdle

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.53
Object name	ssCpuRawIdle
Description	The number of 'ticks' (typically 1/100s) spent idle. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-57. ssCpuRawWait

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.54
Object name	ssCpuRawWait
Description	The number of 'ticks' (typically 1/100s) spent waiting for IO. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-58. ssCpuRawKernel

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.55
Object name	ssCpuRawKernel
Description	The number of 'ticks' (typically 1/100s) spent processing kernel-level code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-59. ssCpuRawInterrupt

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.56
Object name	ssCpuRawInterrupt
Description	The number of 'ticks' (typically 1/100s) spent processing hardware interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-60. sslORawSent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.57
Object name	sslORawSent
Description	Number of blocks sent to a block device.

TABLE B-61. sslORawReceived

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.58
Object name	sslORawReceived
Description	Number of blocks received from a block device.

TABLE B-62. ssRawInterrupts

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.59
Object name	ssRawInterrupts
Description	Number of interrupts processed.

TABLE B-63. ssRawContexts

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.60
Object name	ssRawContexts
Description	Number of context switches.

TABLE B-64. ssCpuRawSoftIRQ

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.61
Object name	ssCpuRawSoftIRQ

Item	Description
Description	The number of 'ticks' (typically 1/100s) spent processing software interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

Table B-65. ssRawSwapIn

Item	Description
OID	.1.3.6.1.4.1.2021.11.62
Object name	ssRawSwapIn
Description	Number of blocks swapped in.

Table B-66. ssRawSwapOut

Item	Description
OID	.1.3.6.1.4.1.2021.11.63
Object name	ssRawSwapOut
Description	Number of blocks swapped out.

Table B-67. ssCpuRawSteal

Item	Description
OID	.1.3.6.1.4.1.2021.11.64
Object name	ssCpuRawSteal
Description	The number of 'ticks' (typically 1/100s) spent by the CPU to run a virtual CPU (guest). This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-68. ssCpuRawGuest

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.65
Object name	ssCpuRawGuest
Description	The number of 'ticks' (typically 1/100s) spent by the CPU to run a virtual CPU (guest). This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-69. ssCpuRawGuestNice

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.66
Object name	ssCpuRawGuestNice
Description	The number of 'ticks' (typically 1/100s) spent by the CPU to run a virtual CPU (guest). This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-70. productVersion

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.1
Object name	productVersion
Description	Returns the Deep Discovery Analyzer version.

TABLE B-71. productBuild

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.2
Object name	productBuild
Description	Returns the Deep Discovery Analyzer build number.

TABLE B-72. productHotfix

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.3
Object name	productHotfix
Description	Returns the Deep Discovery Analyzer hotfix number.

TABLE B-73. componentTable

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2
Object name	componentTable
Description	A table containing a set of component information.

TABLE B-74. componentIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.1
Object name	componentIndex
Description	Returns the component index.

TABLE B-75. componentID

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.2
Object name	componentID

Item	Description
Description	Returns the component ID.

Table B-76. componentName

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.2.1.3
Object name	componentName
Description	Returns the component name.

Table B-77. componentVersion

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.2.1.4
Object name	componentVersion
Description	Returns the component version.

Table B-78. throughputTable

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3
Object name	throughputTable
Description	A table containing a set of throughput information.

Table B-79. ifIndex

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3.1.1
Object name	ifIndex
Description	Returns the interface index.

TABLE B-80. ifDescr

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.3.1.2
Object name	ifDescr
Description	Returns the interface description.

TABLE B-81. ifReceiveThroughput

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.3.1.3
Object name	ifReceiveThroughput
Description	Returns the interface receiving throughput.

TABLE B-82. ifTransmitThroughput

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.3.1.4
Object name	ifTransmitThroughput
Description	Returns the interface transmitting throughput.

TABLE B-83. ifOperStatus

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.3.1.5
Object name	ifOperStatus
Description	Returns the interface operatings status.

TABLE B-84. numberInQueue

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.1
Object name	numberInQueue

Item	Description
Description	Returns the number of samples in queue

Table B-85. numberInProcessing

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.2
Object name	numberInProcessing
Description	Returns the number of samples currently in process

Table B-86. suspiciousObjectIP

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.3.1
Object name	suspiciousObjectIP
Description	Returns the number of suspicious objects (IP address)

Table B-87. suspiciousObjectDomain

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.3.2
Object name	suspiciousObjectDomain
Description	Returns the number of suspicious objects (domain)

Table B-88. suspiciousObjectURL

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.3.3
Object name	suspiciousObjectURL
Description	Returns the number of suspicious objects (URL)

TABLE B-89. suspiciousObjectSha1

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.3.4
Object name	suspiciousObjectSha1
Description	Returns the number of suspicious objects (SHA1)

TABLE B-90. vaUtilization

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.4
Object name	vaUtilization
Description	Returns Virtual Analyzer utilization information

TABLE B-91. numberCompleted

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.5
Object name	numberCompleted
Description	Returns the number of samples that were processed completely in the past 24 hours

TABLE B-92. numberIcapPreScanned

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.6
Object name	numberIcapPreScanned
Description	Returns the number of samples that were processed by ICAP pre-scan in the past 24 hours

TABLE B-93. numberSubmissionHigh

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.4.7.1

Item	Description
Object name	numberSubmissionHigh
Description	Returns the number of submissions with high risk in the past 24 hours

Table B-94. numberSubmissionMedium

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.7.2
Object name	numberSubmissionMedium
Description	Returns the number of submissions with medium risk in the past 24 hours

Table B-95. numberSubmissionLow

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.7.3
Object name	numberSubmissionLow
Description	Returns the number of submissions with low risk in the past 24 hours

Table B-96. numberSubmissionNo

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.7.4
Object name	numberSubmissionNo
Description	Returns the number of submissions with no risk in the past 24 hours

Table B-97. numberSubmissionNot

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.4.7.5
Object name	numberSubmissionNot

Item	Description
Description	Returns the number of submissions not analyzed by Virtual Analyzer in the past 24 hours

SNMP Traps

Table B-98. coldStart

Item	Description
OID	.1.3.6.1.6.3.1.1.5.1.0
Object name	coldStart
Description	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

Table B-99. linkDown

Item	Description
OID	.1.3.6.1.6.3.1.1.5.3.0
Object name	linkDown
Description	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.

Table B-100. linkUp

Item	Description
OID	.1.3.6.1.6.3.1.1.5.4.0
Object name	linkUp

Item	Description
Description	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

Table B-101. nsNotifyShutdown

Item	Description
OID	.1.3.6.1.4.1.8072.4.0.2
Object name	nsNotifyShutdown
Description	An indication that the agent is in the process of being shut down.

Table B-102. accountLockedNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.1
Object name	accountLockedNotification
Description	A notification for when an account was locked because of multiple unsuccessful logon attempts.

Table B-103. vaStoppedNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.2
Object name	vaStoppedNotification
Description	A notification for when Virtual Analyzer is unable to recover from an error.

Table B-104. vaLongQueueNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.3

Item	Description
Object name	vaLongQueueNotification
Description	A notification for when the number of Virtual Analyzer submissions has exceeded the threshold.

Table B-105. compUpdateErrorNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.4
Object name	compUpdateErrorNotification
Description	A notification for when a component update was unsuccessful.

Table B-106. highCpuNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.5
Object name	highCpuNotification
Description	A notification for when the average CPU usage in the last 5 minutes has exceeded the threshold.

Table B-107. highMemNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.6
Object name	highMemNotification
Description	A notification for when the average memory usage in the last 5 minutes has exceeded the threshold.

Table B-108. highDiskNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.7
Object name	highDiskNotification

Item	Description
Description	A notification for when disk usage has exceeded the threshold.

Table B-109. secondaryDownNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.8
Object name	secondaryDownNotification
Description	A notification for when a secondary appliance is unable to recover from an error.

Table B-110. haPassiveActivatedNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.9
Object name	haPassiveActivatedNotification
Description	A notification for when the active primary appliance is unable to recover from an error, and the passive primary appliance has taken over the active role.

Table B-111. haSuspendedNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.10
Object name	haSuspendedNotification
Description	A notification for when the passive primary appliance is unable to recover from an error, and high availability is suspended.

Table B-112. syslogErrorNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.11
Object name	syslogErrorNotification

Item	Description
Description	A notification for when the syslog server is inaccessible.

Table B-113. backupErrorNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.12
Object name	backupErrorNotification
Description	A notification for when the backup server is inaccessible.

Table B-114. haRestoredNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.13
Object name	haRestoredNotification
Description	A notification for when the passive primary appliance has recovered and high availability has been restored.

Table B-115. vaHighRiskNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.14
Object name	vaHighRiskNotification
Description	A notification for when the number of new high-risk objects identified during the last TimeRange has reached the threshold.

Table B-116. vaConnectionFailureNotification

Item	Description
OID	.1.3.6.1.4.1.6101.3005.2.1.0.15
Object name	vaConnectionFailureNotification
Description	A notification for when the appliance is unable to establish connection to a required resource.

TABLE B-117. vaLongProcessTimeNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.16
Object name	vaLongProcessTimeNotification
Description	A notification for when the process time of Virtual Analyzer submissions has exceeded the threshold.

TABLE B-118. licenseExpireNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.17
Object name	licenseExpireNotification
Description	A notification for when the license is about to expire or has expired.

TABLE B-119. networkShareInaccessible

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.18
Object name	networkShareInaccessible
Description	A notification for when the appliance is unable to establish connection to the network share server.

Registration Objects

OID	DESCRIPTION
.1.3.6.1.4.1.2021	UC Davis
.1.3.6.1.4.1.6101	Trend Micro, Inc.
.1.3.6.1.6.3.1.1.5.1	SNMPv2-MIB MIB
.1.3.6.1.4.1.8072	NET-SNMP-AGENT-MIB

Appendix C

TLS Support for Integrated Products/ Services

The following integrated products/services use TLS 1.2 or above when the secure protocol option is enabled. For details, see *Network Tab on page 6-50*.

- Active Directory
- Email Submission over SSL
- ICAP over SSL
- Image import using HTTPS
- Internal Virtual Analyzer services
- Management console access
- Network share scanning for Azure Blob and AWS S3
- Sandbox as a Service (for macOS)
- SMTP over STARTTLS or SSL/TLS
- Syslog over SSL
- Trend Micro ActiveUpdate
- Trend Micro Certified Safe Software Service
- Trend Micro Community Domain/IP Reputation Service

- Trend Micro Community File Reputation service
- Trend Micro Customer Licensing Portal
- Trend Micro Deep Discovery Director
- Trend Micro Predictive Machine Learning engine
- Trend Micro Dynamic URL Scanning
- Trend Micro Smart Feedback
- Trend Micro Smart Protection Server version 3.3 or later
- Trend Micro Web Inspection Service
- Trend Micro Web Reputation Service
- Trend Vision One
- Web Service

Index

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

www.trendmicro.com
Item Code: APEM769913/240703