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

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

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

Evaluate this documentation on the following site:

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

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

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


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

Table of Contents

Preface

Preface ................................................................................................................. ix
Documentation ................................................................................................... x
Audience ............................................................................................................. xi
Document Conventions ................................................................................... xi
About Trend Micro ............................................................ xii

Chapter 1: Introduction

Overview of Deep Discovery Web Inspector ............................................ 1-2
   Features and Benefits ................................................................. 1-2

A New Threat Landscape ................................................................. 1-5
   Advanced Persistent Threats ................................................... 1-5
   C&C Callback ......................................................................... 1-6

A New Solution ......................................................................................... 1-7
   Predictive Machine Learning .................................................. 1-8
   Virtual Analyzer ........................................................................ 1-8
   Advanced Threat Scan Engine ............................................... 1-9
   Web Reputation Services ....................................................... 1-10
   Trend Micro Control Manager ............................................. 1-10

Chapter 2: Preparing for Deployment

Pre-deployment Tasks .............................................................. 2-2

Network Deployment Mode Overview .............................................. 2-2
   Forward Proxy Mode .............................................................. 2-3
   Transparent Bridge Mode ......................................................... 2-3
   Bridge Mode Not Supported When Deployed in LACP/
   EtherChannel Links ............................................................. 2-4

Recommended Network Environment ........................................... 2-4
System Requirements ................................................................. 2-4
   Enabling and Starting the SSH Service ...................................... 2-5
Ports Used by the Appliance ................................................................. 2-6
Items to Prepare ..................................................................................... 2-8
Control Manager Deployment ................................................................. 2-9

Chapter 3: Deployment

Setting up the Hardware ........................................................................ 3-2
Configuring Management Console Access ............................................. 3-2
Opening the Management Console .......................................................... 3-5
   Changing Your Password ................................................................ 3-6
Activating the License ............................................................................ 3-6
Performing the Initial Deployment ........................................................... 3-8
   Initial Configuration for Forward Proxy Mode ................................. 3-8
   Initial Configuration for Transparent Bridge Mode ......................... 3-11

Chapter 4: Getting Started

Management Console Navigation ............................................................ 4-2
Getting Started Tasks ............................................................................. 4-2

Chapter 5: Dashboard

Dashboard Overview ............................................................................. 5-2
   Default Dashboard View ................................................................ 5-3
Threat Monitoring Tab ........................................................................... 5-3
   Advanced Threat Indicators Widget ................................................. 5-4
   C&C Callback Detections Over Time Widget ................................. 5-5
   Ransomware Detections Over Time Widget ................................. 5-6
   Top Affected Hosts Widget .............................................................. 5-6
   Top Detected URLs Widget ............................................................. 5-7
   Virtual Analyzer Sandbox Analysis Widget .................................... 5-7
System Status Tab ................................................................................... 5-8
   Hardware Status Widget ................................................................. 5-8
Chapter 6: Detections

Understanding Risk Levels ................................................................. 6-2
Detection Risk Levels ........................................................................ 6-2
Virtual Analyzer Risk Levels ............................................................. 6-3

Threat Indicator and Detected By Classifications ............................... 6-4
Threat Indicator Classifications ......................................................... 6-4
Detected By Classifications ................................................................. 6-5

Viewing Detections ................................................................................ 6-7
Viewing All Detections ........................................................................ 6-7
Viewing Detections for Hosts ............................................................. 6-13
Viewing Detections for URLs ............................................................. 6-14
Viewing Detections for Files ............................................................... 6-16

Viewing Suspicious Objects ................................................................. 6-18
Viewing Suspicious IP Address Objects ............................................ 6-18
Viewing Suspicious Domain Objects ................................................. 6-19
Viewing Suspicious URLs ................................................................. 6-20
Viewing Suspicious File Objects ....................................................... 6-21

Chapter 7: Policy

Policy Overview .................................................................................. 7-2
Managing Policies ................................................................. 7-3
  Information About How Policies Work ............................... 7-3
  How Patient Zero Protection Works ................................. 7-4
  The Default Policy ....................................................... 7-5
  Viewing Policies .......................................................... 7-5
  Adding Policies ......................................................... 7-6

Managing HTTPS Inspection Rules .......................... 7-8
  HTTPS Inspection ................................................. 7-9
  Viewing HTTPS Inspection Rules ............................... 7-10
  Adding/Editing HTTPS Inspection Rules ...................... 7-11
  Generating a CSR .................................................. 7-14

Managing User-Defined Settings .......................... 7-15
  Managing Network Objects ..................................... 7-16
  Managing Domain Objects ..................................... 7-17
  Managing the Approved/Blocked List ....................... 7-19
  Managing Notifications ......................................... 7-22

Chapter 8: Alerts and Reports

  Alerts ........................................................................ 8-2
    Managing Triggered Alerts ................................... 8-2
    Viewing Triggered Alerts ...................................... 8-2
    Configuring Alert Notifications ............................... 8-5

  Reports ....................................................................... 8-20
    Scheduling Reports ............................................... 8-20
    Generating On-Demand Reports ............................. 8-21

Chapter 9: Administration

  Deployment Wizard .................................................. 9-2
    Accessing the Deployment Wizard ............................ 9-2
    Configuring Forward Proxy Mode .......................... 9-2
    Configuring Transparent Bridge Mode .................. 9-5

  Component Updates ............................................... 9-7
    Components ...................................................... 9-7
    Updating Components ....................................... 9-9
    Rolling Back Components .................................. 9-10
# Table of Contents

Scheduling Component Updates ....................................................... 9-10

Product Updates ........................................................................ 9-11
  Hotfixes and Patches Overview ................................................. 9-11
  Managing Patches .................................................................. 9-12
  Upgrading Firmware ............................................................... 9-12

System Settings ........................................................................ 9-14
  Configuring Network Settings ............................................... 9-14
  Managing Static Routes ......................................................... 9-15
  Configuring Proxy Settings ................................................... 9-17
  Configuring the Notification SMTP Server ................................ 9-18
  Configuring System Time ...................................................... 9-19
  Configuring SNMP ............................................................... 9-20

Integrated Products/Services ...................................................... 9-25
  Control Manager .................................................................. 9-25
  Threat Intelligence Sharing .................................................. 9-28
  Log Settings ......................................................................... 9-29

Virtual Analyzer ......................................................................... 9-39
  Virtual Analyzer Overview .................................................. 9-40
  Virtual Analyzer Status ....................................................... 9-41
  Virtual Analyzer Images ...................................................... 9-43
  Virtual Analyzer Network .................................................... 9-47

System Maintenance ................................................................... 9-50
  Configuring Storage Maintenance ......................................... 9-51
  Debug Logs .......................................................................... 9-51
  Testing Network Connections .............................................. 9-53
  Network Packet Capture ...................................................... 9-54
  Enabling/Disabling Bypass Mode .......................................... 9-56
  Configuring Bypass/Redirect Policies .................................... 9-56
  Backing Up or Restoring a Configuration ............................... 9-62
  Power Off / Restart .............................................................. 9-66

Accounts / Contacts ................................................................... 9-67
  Managing Accounts ............................................................ 9-68
  Managing Contacts ............................................................. 9-71

License ..................................................................................... 9-72
About Deep Discovery Web Inspector ............................................................ 9-72

Chapter 10: Licensing and Maintenance

Maintenance Agreement .............................................................................. 10-2
Activation Codes ........................................................................................... 10-2
Product License Description ...................................................................... 10-2
Product License Status ............................................................................... 10-3
Viewing Your Product License .................................................................. 10-4
Managing Your Product License ............................................................... 10-5

Chapter 11: Technical Support

Troubleshooting Resources ....................................................................... 11-2
Using the Support Portal .......................................................................... 11-2
Threat Encyclopedia ............................................................................... 11-2
Contacting Trend Micro ......................................................................... 11-3
Speeding Up the Support Call ............................................................... 11-4
Sending Suspicious Content to Trend Micro .......................................... 11-4
Email Reputation Services ....................................................................... 11-4
File Reputation Services .......................................................................... 11-5
Web Reputation Services ......................................................................... 11-5
Other Resources ...................................................................................... 11-5
Download Center ..................................................................................... 11-5
Documentation Feedback ........................................................................ 11-6

Appendices

Appendix A: Using the Command Line Interface

Entering the CLI .......................................................................................... A-2
Normal and Privileged Commands ............................................................ A-3
Entering Privileged Mode ......................................................................... A-3
CLI Command Reference .................................................................................. A-3

Appendix B: SNMP Object Identifiers

SNMP Query Objects ........................................................................................ B-2
SNMP Traps ......................................................................................................... B-6
SNMP Registration Objects ............................................................................. B-12

Index

Index ................................................................................................................. IN-1
Preface

Topics include:

• Documentation on page x
• Audience on page xi
• Document Conventions on page xi
• About Trend Micro on page xii
Documentation

The documentation set for Deep Discovery Web Inspector includes the following:

**Table 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator’s Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator’s Guide contains detailed instructions on how to deploy, configure, and manage Deep Discovery Web Inspector, and provides explanations on Deep Discovery Web Inspector concepts and features.</td>
</tr>
<tr>
<td>Installation and Deployment Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide discusses requirements and procedures for installing and deploying Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Syslog Content Mapping Guide</td>
<td>The Syslog Content Mapping Guide contains information on event logging formats supported by Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Web Inspector to your network and on performing the initial configuration.</td>
</tr>
<tr>
<td>Readme</td>
<td>The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Web-based documentation that is accessible from the Deep Discovery Web Inspector management console. The Online Help contains explanations of Deep Discovery Web Inspector components and features, as well as procedures needed to configure Deep Discovery Web Inspector.</td>
</tr>
</tbody>
</table>
Support Portal

The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website:

http://esupport.trendmicro.com

View and download Deep Discovery Web Inspector documentation from the Trend Micro Documentation Center:


Audience

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

- Network topologies
- Policy management and enforcement

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

Document Conventions

The documentation uses the following conventions:

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
</tbody>
</table>
## Convention

<table>
<thead>
<tr>
<th><strong>CONVENTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documents</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>

## About Trend Micro

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

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

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

Introduction

Topics include:

• Overview of Deep Discovery Web Inspector on page 1-2
• A New Threat Landscape on page 1-5
• A New Solution on page 1-7
Overview of Deep Discovery Web Inspector

Deep Discovery Web Inspector inspects and eliminates cyber threats and attacks that could threaten your network. Designed to be integrated into your existing network topology to monitor your network traffic, Deep Discovery Web Inspector acts as either a transparent bridge or a forward proxy.

Features and Benefits

The following section describes Deep Discovery Web Inspector features and benefits.

Flexible Deployment

Deep Discovery Web Inspector integrates into your existing network topology by acting as either a transparent bridge or a forward proxy.

In forward proxy mode, Deep Discovery Web Inspector is configured as a proxy server for network clients. Clients have to configure the web proxy to redirect web traffic to Deep Discovery Web Inspector.

In transparent bridge mode, Deep Discovery Web Inspector acts as a layer 2 bridge between network devices (switches, routers, or firewalls) and is transparent in the network.

Visibility, Analysis, and Action

Deep Discovery Web Inspector provides real-time threat visibility and analysis in an intuitive, multi-level format. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.

Easy-to-Use Policy Management

Deep Discovery Web Inspector provides easy-to-use, but powerful policy management.

• Create policies that specify which network and domain objects and which file types to scan.
• Create network or domain objects to use when creating policies.
• Use a pre-defined list of file types when configuring policies.
• Choose whether to allow, block, or scan objects that are a policy match.
• If matching objects are scanned, further refine actions taken by specifying whether to monitor or block the object depending on the risk level.
• Provide advanced malware protection by enabling Patient Zero Protection.

If an object is sent to Virtual Analyzer for sandbox analysis, Patient Zero Protection temporarily holds objects until analysis is complete instead of passing the object to the endpoint even before analysis determines the risk level for the object.
• Configure multiple policies and prioritize by moving them up or down in the policy order.
• Customize email notifications sent to users for policy violations.
• Create HTTPS inspection rules to decrypt and inspect HTTPS traffic.
• Configure the Approved/Blocked URL lists to allow or block traffic without need for scanning.

Advanced Detection

Deep Discovery Web Inspector advanced detection technology discovers targeted threats based on network objects, domain objects, URLs, and file types.

Deep Discovery Web Inspector uses multiple detection methods to ensure the highest level of protection, including:
• Approved/Blocked URL list to determine which URLs to allow or block without needing to scan
• Untrusted server certificate analysis to detect whether the URL or domain has an untrusted SSL server certificate
• Web Reputation Services database to block users from URLs that are known malicious sites
• True file types that you select for inclusion in a policy to trigger a detection and then can take action based on the configured policy
• Static Intelligence Engine's known pattern for detecting malware
• Script Analyzer Lineup to detect malicious scripts
• Advanced Threat Scan Engine for advanced detection of malware
• Predictive Machine Learning for intelligent analysis of unknown threats
• Virtual Analyzer sandbox for custom threat simulation analysis

HTTP/2 Scanning

Deep Discovery Web Inspector advanced detection technology can scan HTTP/2 traffic.

HTTPS Inspection

The traffic over SSL/TLS is encrypted and signed to ensure security. Because encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections, HTTPS traffic should be inspected just as HTTP traffic is. Deep Discovery Web Inspector advanced detection technology can decrypt and inspect HTTPS traffic based on criteria that you specify.

Custom Threat Simulation Sandbox

The Virtual Analyzer sandbox environment opens suspicious files submitted to test for malicious behavior. Virtual Analyzer is able to find exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

Patient Zero Protection

Patient Zero Protection provides advanced malware protection from suspicious objects that have been sent to Virtual Analyzer for sandbox analysis.

If Patient Zero Protection is enabled, Deep Discovery Web Inspector temporarily holds the suspicious object while analysis is performed. Once analysis is complete, depending
on the outcome of the analysis, the appropriate action is taken. Deep Discovery Web Inspector delivers the object to the endpoint if it is riskless. If sandbox analysis determines that the risk level for that object is low, medium, or high, the malicious object is blocked or monitored, according to the actions configured for the policy that triggered the analysis.

**Access Log Offload to a Syslog Server**

Deep Discovery Web Inspector supports an access log. You can configure syslog settings to offload the access logs to an external syslog server. Additionally, you can customize which access log entries are sent so that you send only the data that is useful to your business environment.

**A New Threat Landscape**

Where once attackers were content to simply deface a website or gain notoriety through mass system disruption, they now realize that they can make significant money, steal important data, or interfere with major infrastructure systems via cyber warfare instead.

A targeted attack is a long-term cyber-espionage campaign against a person or organization to gain persistent access to the target network. This allows them to extract confidential company data and possibly damage the target network. These compromised networks can be used for attacks against other organizations, making it harder to trace the attack back to its originator.

**Advanced Persistent Threats**

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

In targeted attacks, the APT life cycle follows a continuous process of six key phases.
TABLE 1-1. APT Attack Sequence

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

Deep Discovery Web Inspector can detect APT and targeted attacks by identifying malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

**C&C Callback**

The following actions usually occur when malicious software installs and communicates back to a C&C server:
• Software called a “downloader” automatically downloads and installs malware.

• A human monitoring the C&C server (attacker) responds to the connection with an action. Software called a “remote access Trojan” (RAT) gives an attacker the ability to examine a system, extract files, download new files to run on a compromised system, turn on a system’s video camera and microphone, take screen captures, capture keystrokes, and run a command shell.

Attackers will attempt to move laterally throughout a compromised network by gaining additional persistent access points. Attackers will also attempt to steal user credentials for data collection spread throughout the network. If successful, collected data gets exfiltrated out of the network to another environment for further examination.

Attackers move at a slow pace to remain undetected. When a detection occurs, they will temporarily go dormant before resuming activity. If an organization eradicates their presence from the network, the attackers will start the attack cycle all over again.

A New Solution

Deep Discovery Web Inspector prevents network-based attacks and cyber threats by investigating suspicious domain and network objects and associated file types and social engineering attack patterns in web content before they can threaten your network. Designed to integrate into your existing network topology, Deep Discovery Web Inspector monitors your network for cyber threats using either transparent bridge or forward proxy mode.

Whichever deployment method is chosen, Deep Discovery Web Inspector investigates web traffic for suspicious file types, domains, URLs, or embedded links (URLs). If an object exhibits malicious behavior, Deep Discovery Web Inspector can block the threat and notify security administrators about the malicious activity.

After Deep Discovery Web Inspector scans a network object for known threats in the Trend Micro Smart Protection Network, it passes suspicious files to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

After investigating the suspicious object, Deep Discovery Web Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Web Inspector calculates the risk
level based on the highest risk assigned between the Deep Discovery Web Inspector scanners and Virtual Analyzer.

Deep Discovery Web Inspector acts upon network objects according to the assigned risk level and policy settings. Configure Deep Discovery Web Inspector to block the content or monitor the network content and allow the network content to pass to the end user. While Deep Discovery Web Inspector monitors your network for threats, you can access dashboard widgets and reports for further investigation.

**Predictive Machine Learning**

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

After detecting an unknown or low-prevalence file, Deep Discovery Web Inspector scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

Depending on how you configure your policies, Deep Discovery Web Inspector can block the object to prevent the threat from continuing to spread across your network. Alternatively, you can configure the policy to monitor and log information about the object without blocking it.

**Virtual Analyzer**

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, and administrators and investigators (through SSH).
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.

**Advanced Threat Scan Engine**

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
• Enhanced parsers for handling file deformities

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web Reputation Services assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Trend Micro Control Manager

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.

In a network topology containing multiple Deep Discovery Web Inspector appliances, Control Manager can aggregate suspicious objects data. With Control Manager integration, Deep Discovery Web Inspector appliances can defend from threats happening in the world in real time. Deep Discovery Web Inspector supports synchronizing two type suspicious objects from Control Manager: Virtual Analyzer suspicious objects and user-defined suspicious objects. Deep Discovery Web Inspector can block the traffic if matched in the synchronized high-risk suspicious objects list.
Chapter 2

Preparing for Deployment

Topics include:

- Pre-deployment Tasks on page 2-2
- Network Deployment Mode Overview on page 2-2
- Recommended Network Environment on page 2-4
- System Requirements on page 2-4
- Ports Used by the Appliance on page 2-6
- Items to Prepare on page 2-8
- Control Manager Deployment on page 2-9
Pre-deployment Tasks

The following procedure provides an overview of items to consider and tasks to perform before deploying Deep Discovery Web Inspector.

Procedure

1. Decide which deployment mode to use.
   See Network Deployment Mode Overview on page 2-2.

2. Review the recommended network environment information.
   See Recommended Network Environment on page 2-4.

3. Review the system requirements.
   See System Requirements on page 2-4.

4. Review the information about ports used by the appliance and open ports as needed.
   See Ports Used by the Appliance on page 2-6.

5. Prepare the items for deployment.
   See Items to Prepare on page 2-8.

6. Prepare Control Manager if used as part of the deployment.
   See Control Manager Deployment on page 2-9.

Network Deployment Mode Overview

You can configure Deep Discovery Web Inspector in one of two network topology modes.

- Forward Proxy Mode on page 2-3.
•  *Transparent Bridge Mode on page 2-3.*

**Forward Proxy Mode**

With forward proxy mode, Deep Discovery Web Inspector is configured as a proxy server for network clients. Client browser settings must be configured to redirect traffic to Deep Discovery Web Inspector.

Deep Discovery Web Inspector policies are compared against both incoming and outgoing traffic. Deep Discovery Web Inspector performs security scans and takes action if there is a traffic match according to configured policies. Deep Discovery Web Inspector can bypass scanning and forward the traffic straight to the endpoints, block traffic without scanning it, or scan the traffic and then either block or monitor traffic, depending on actions configured in policies.

Forward proxy mode also provides the additional capability to forward all traffic to another upstream proxy server.

**Transparent Bridge Mode**

With transparent bridge mode, Deep Discovery Web Inspector acts as a layer 2 bridge between network devices (core switch, router, or firewall) and is transparent on the network.

Deep Discovery Web Inspector inspects HTTP/HTTPS traffic that passes through it and applies configured actions according to matching policies. It can allow, monitor, or block traffic.

Deep Discovery Web Inspector policies are compared against traffic coming into the ingress port and out of the egress port. Deep Discovery Web Inspector performs security scans and takes action if there is a traffic match according to configured policies. Deep Discovery Web Inspector can bypass scanning and let the traffic pass straight through the appliance, block the traffic without scanning, or scan the traffic and then either block or monitor the traffic, depending on actions configured in policies.

Transparent bridge mode is suitable when you want to use Deep Discovery Web Inspector as an inline device and there is only one network path that you want to monitor and secure.
If you set up Deep Discovery Web Inspector in transparent bridge mode, you do not need to reconfigure your network as you need only place Deep Discovery Web Inspector in the network path that you want to secure.

**Bridge Mode Not Supported When Deployed in LACP/EtherChannel Links**

You should be aware that Deep Discovery Web Inspector does not support bridge mode when deployed in LACP/EtherChannel links.

LACP (Link Aggregation Control Protocol) is a layer 2 protocol that provides functionality when aggregating one or more Ethernet interfaces to form a single logical link (link aggregation groups).

Deep Discovery Web Inspector in bridge mode behaves like a normal layer 2 switch. Therefore, when LACP packets reach the Deep Discovery Web Inspector appliance, the packets are not forwarded between the Deep Discovery Web Inspector incoming and outgoing interfaces. Instead, Deep Discovery Web Inspector keeps and processes the LACP packets. To devices that are using LACP links, the link appears to be abnormal.

**Recommended Network Environment**

Deep Discovery Web Inspector requires connection to a management network. After deployment, administrators can perform configuration tasks from any computer on the management network.

**System Requirements**

Deep Discovery Web Inspector is a hardware appliance with all software pre-installed. It is ready to deploy on your network as shipped from the manufacturer.

The following table lists the minimum software requirements to access the command line interface and the web management console that are used to manage Deep Discovery Web Inspector. Before deployment, you should review the list and ensure that you can meet the browser and SSH client software requirements.
### Table 2-1. Minimum Software Requirements

<table>
<thead>
<tr>
<th>Application</th>
<th>Requirements</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH client</td>
<td>SSH protocol version 2</td>
<td>Set the Command Line Interface terminal window size to 80 columns and 24 rows.</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Version 11</td>
<td>Use only a supported browser to access the management console.</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Windows 10</td>
<td>Using the data port IP address you set during the initial configuration, specify the following URL:</td>
</tr>
<tr>
<td>Mozilla® Firefox®</td>
<td>Version 55 or later</td>
<td>https://[Appliance_IP_Address]</td>
</tr>
<tr>
<td>Google Chrome™</td>
<td>Version 59 or later</td>
<td></td>
</tr>
<tr>
<td>Mac® Safari®</td>
<td>Mac OS</td>
<td></td>
</tr>
</tbody>
</table>

- Trend Micro recommends viewing the console using a monitor that supports 1280 x 1024 resolution or greater.
- By default, the SSH service is disabled and is not started when enabled. To use SSH, you must first enable and then start the SSH service.
- Make sure that the management interface eth0 (on the back of the appliance) is accessible via TCP port 22 for the Command Line Interface (SSH) and TCP port 443 for the management console (HTTPS).

### Related information

- Enabling and Starting the SSH Service

### Enabling and Starting the SSH Service

By default, the SSH service is disabled and is not started when enabled. You must use the command line interface to first enable and then start the SSH service.

#### Procedure

1. To enable and start the SSH service, first enter the CLI.

   *Entering the CLI on page A-2.*
2. Enable the SSH service.

```
configure service ssh enable
```

3. Start the SSH service.

```
start service ssh
```

## Ports Used by the Appliance

The following table shows the ports that are used with Deep Discovery Web Inspector and why they are used.

**Table 2-2. Ports used by Deep Discovery Web Inspector**

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22*</td>
<td>TCP</td>
<td>Listening</td>
<td>Endpoints connect to Deep Discovery Web Inspector through SSH. *Because SSH is disabled by default, this port is not used by default. If you enable and start SSH, Deep Discovery Web Inspector then listens on this port.</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Deep Discovery Web Inspector uses this port for DNS resolution.</td>
</tr>
<tr>
<td>80*</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Deep Discovery Web Inspector listens on this port when uploading Virtual Analyzer images. *All other access to Deep Discovery Web Inspector is secured by SSL, which uses 443.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Outbound</td>
<td>Deep Discovery Web Inspector connects to the NTP server to synchronize time.</td>
</tr>
</tbody>
</table>
### Preparing for Deployment

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>UDP</td>
<td>Listening</td>
<td>Deep Discovery Web Inspector uses this port to listen for requests from SNMP managers.</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>Outbound</td>
<td>Deep Discovery Web Inspector connects to SNMP managers to send SNMP trap messages.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Deep Discovery Web Inspector uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Query the Predictive Machine Learning engine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Access the management console with a computer through HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communicate with Trend Micro Control Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to the Smart Protection Network and query Web Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to Trend Micro Threat Connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send anonymous threat information to Smart Feedback</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Update components by connecting to the ActiveUpdate server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send product usage information to Trend Micro feedback servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Share threat intelligence information and exception list with other products</td>
</tr>
</tbody>
</table>
### Items to Prepare

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Monitor and VGA cable</td>
<td>Connects to the VGA port of the appliance</td>
</tr>
<tr>
<td>USB keyboard</td>
<td>Connects to a USB port of the appliance</td>
</tr>
<tr>
<td>Ethernet cables</td>
<td>Connect to the management and data ports</td>
</tr>
<tr>
<td></td>
<td>• Required: eth0</td>
</tr>
<tr>
<td></td>
<td>• Forward proxy: This is the data interface, used for both management and data.</td>
</tr>
<tr>
<td></td>
<td>• Transparent bridge: This is the management interface.</td>
</tr>
<tr>
<td></td>
<td>• Required for Transparent Bridge: eth4 and eth5</td>
</tr>
<tr>
<td></td>
<td>These interfaces are the data ingress (eth4) and data egress (eth5) interfaces.</td>
</tr>
</tbody>
</table>
Preparing for Deployment

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet-enabled computer</td>
<td>Access to the management console from a computer with the following software installed:</td>
</tr>
<tr>
<td></td>
<td>A supported web browser:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Edge Windows 10</td>
</tr>
<tr>
<td></td>
<td>• Mozilla® Firefox® 55 or later</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome™ 59 or later</td>
</tr>
<tr>
<td></td>
<td>• Mac® Safari®</td>
</tr>
<tr>
<td>IP addresses</td>
<td>• Forward Proxy Required: One IPv4 address for the data interface</td>
</tr>
<tr>
<td></td>
<td>• Transparent Bridge Required: One IPv4 address for the management interface</td>
</tr>
</tbody>
</table>

**Note**

In transparent bridge mode, eth4 and eth5 act as layer 2 interfaces and are not assigned IP addresses.

| Third party software licenses | Licenses for all third-party software installed on sandbox images   |

Control Manager Deployment

In a network topology containing multiple Deep Discovery Web Inspector appliances, Trend Micro Control Manager can aggregate suspicious objects data.

With Trend Micro Control Manager integration, Deep Discovery Web Inspector appliances can defend from threats happening in the world in real time. Deep Discovery Web Inspector supports synchronizing two types of suspicious objects from Control Manager: Virtual Analyzer suspicious objects and user-defined suspicious objects. Deep Discovery Web Inspector can block the traffic if matched in the synchronized high-risk suspicious objects list.
See Registering to Control Manager on page 9-27 for details about configuring Control Manager settings:
Chapter 3

Deployment

Topics include:

• Setting up the Hardware on page 3-2
• Configuring Management Console Access on page 3-2
• Opening the Management Console on page 3-5
• Activating the License on page 3-6
• Performing the Initial Deployment on page 3-8
  • Initial Configuration for Forward Proxy Mode on page 3-8
  • Initial Configuration for Transparent Bridge Mode on page 3-11
Setting up the Hardware

Your appliance shipped with the software installed and licensed. Before you can deploy and configure Deep Discovery Web Inspector, you must set up the hardware.

Procedure

1. Use the Deep Discovery Web Inspector Quick Start Card that came with your appliance to set up the hardware and cable the appliance to the network.
2. Connect a USB keyboard and monitor to the appliance.

What to do next

After, power on is complete, you can log in to the command line interface (CLI) to configure management console access.

Configuring Management Console Access

Before you can perform the initial deployment of Deep Discovery Web Inspector, you must log on to the Command Line Interface (CLI) and configure access to the Deep Discovery Web Inspector management console.

The following procedure explains how to log on to the CLI and configure the required network settings:

Procedure

1. Power up the appliance if it is not already up.
2. To make a direct connection, connect a monitor and keyboard to the Deep Discovery Web Inspector appliance.
The appliance's command line interface is displayed on the monitor. You can log in to the CLI and perform basic tasks.

3. Log in to the CLI with the default credentials.
   • User name: admin
   • Password: ddwi

4. At the prompt, type `enable` and press Enter to enter privileged mode.

5. Type the default password, `trend#1`, and then press Enter.

The prompt changes from > to #.

6. Configure network settings with the following command:

   `configure network basic`
7. Configure the following network settings and press Enter after typing each setting.

   **Note**
   The default management IP address / subnet mask is 192.168.252.1 / 255.255.0.0.

   - Host name
   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - Preferred IPv4 DNS
   - Alternate IPv4 DNS

---

8. Type **Y** to confirm settings and restart.

Deep Discovery Web Inspector implements the specified network settings and then restarts network services.

You can now access the Deep Discovery Web Inspector management console using a supported Web browser by accessing https://<management_IP_address>.

   **Note**
   You can log on to the CLI later to perform additional configuration, troubleshooting, or maintenance tasks:

   **Using the Command Line Interface on page A-1.**
Opening the Management Console

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

You can connect to the management console using any supported web browser.

See *System Requirements on page 2-4*.

---

**Procedure**

1. In a web browser, type the IP address of the Deep Discovery Web Inspector server.

   `https://<management_IP_address>`

   The default URL is `https://192.168.252.1`.

   The log on screen appears.

2. Specify the log on credentials (user name and password).

   **Note**

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

   - User name: `admin`
   - Password: `ddwi`

3. Click **Log On**.

   The **Dashboard** screen opens.

   **Important**

   Trend Micro recommends changing the password to prevent unauthorized changes to the management console.
Related information

→ Changing Your Password

Changing Your Password

You can change your password when you are logged on to the management console.

Procedure

1. On the management console banner, click your account name and then click Change password.
   
   The Change Password screen appears.

2. Specify password settings.
   
   • Old password
   
   • New password
   
   • Confirm password

3. Click Save.

Activating the License

You must activate the Deep Discovery Web Inspector license before performing the initial deployment.

Procedure

1. Go to Administration > License.
2. Click **New Activation Code**.

The **Activation Code** screen displays.

3. Specify the new activation code.

4. Read the license agreement and select **I have read and accept the terms of the Trend Micro License Agreement**.

5. Click **Save**.
The Deep Discovery Web Inspector activates.

Performing the Initial Deployment

After activating the Deep Discovery Web Inspector license, you can use the Deployment Wizard to configure your Deep Discovery Web Inspector appliance's basic settings.

Perform one of the following initial deployments, depending on the desired deployment mode.

- Initial Configuration for Transparent Bridge Mode on page 3-11
- Initial Configuration for Forward Proxy Mode on page 3-8

Related information

- Network Deployment Mode Overview

Initial Configuration for Forward Proxy Mode

You can use the Deployment Wizard to configure the basic settings for forward proxy mode on your Deep Discovery Web Inspector appliance.
Deployment

Note
You can exit the Deployment Wizard at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure

1. Go to Administration > Deployment Wizard.

   The Welcome page opens.

2. In the Deployment Mode section, select Forward proxy.

3. Click Next.

4. In the Working Mode Settings page, specify the following details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP listening port</td>
<td>Specify the port that the proxy server uses to listen.</td>
</tr>
<tr>
<td>Enable upstream proxy</td>
<td>Select this option if the network uses an upstream proxy server and specify</td>
</tr>
<tr>
<td></td>
<td>the IPv4 address and port number in Proxy server and Port number.</td>
</tr>
</tbody>
</table>

5. Click Next.

6. In the Network page, specify the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify a host name.</td>
</tr>
<tr>
<td>Primary DNS server</td>
<td>Specify the IP address of the DNS server. This is a required setting.</td>
</tr>
<tr>
<td>Secondary DNS server</td>
<td>Optionally, specify the IP address for a secondary DNS server.</td>
</tr>
<tr>
<td>Data interface</td>
<td>This is a read-only field and is pre-set to eth0. This interface is also</td>
</tr>
</tbody>
</table>
<pre><code>                    |   used for management.                                                      |
</code></pre>
7. Click **Next**.

The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv4 address, IPv4 netmask, and Default IPv4 gateway</strong></td>
<td>Specify the IPv4 network settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NTP server</strong></td>
<td>Enter the NTP server IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System time zone</strong></td>
<td>Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select <strong>Etc</strong> and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.</td>
</tr>
</tbody>
</table>

9. Click **Next**.

The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

a. If the settings are not as desired, click on **Prev** and modify settings as required.

b. If the settings are verified, click on **Finish** to save the configuration.
Note
After you click Finish, a dialog box opens asking if you want to reboot the appliance. After you click OK, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the Log On page is displayed.

If you do not want to reboot, you can click Cancel instead of OK. If you click Cancel, the Summary page reopens.

Important
If you exit the wizard before saving settings, the configuration is not saved.

Related information
¬ Network Deployment Mode Overview

Initial Configuration for Transparent Bridge Mode

You can use the Deployment Wizard to configure the basic settings for transparent bridge mode on your Deep Discovery Web Inspector appliance.

You can exit the Deployment Wizard at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

Procedure
1. Go to Administration > Deployment Wizard.
   The Welcome page opens.
2. In the Deployment Mode section, select Transparent bridge.
3. Click Next.
4. In the Network page, specify the following details:
### Host name
- Specify a host name.

### Primary DNS server
- Specify the IP address of the DNS server. This is a required setting.

### Secondary DNS server
- Optionally, specify the IP address for a secondary DNS server.

### Data egress interface
- This is a read-only field and is pre-set to `eth5`.

### Data ingress interface
- This is a read-only field and is pre-set to `eth4`.

### Management interface
- This is a read-only field and is pre-set to `eth0`.

### Mode
- This is a read-only field and is pre-set to `static`.

### IPv4 address, IPv4 netmask, and Default IPv4 gateway
- Specify the IPv4 network settings.

---

5. Click **Next**.

The **Time** page opens.

6. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server</td>
<td>Enter the NTP server IP address.</td>
</tr>
<tr>
<td>System time zone</td>
<td>Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Option: instead of selecting a location,你 can select <strong>Etc</strong> and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.</td>
</tr>
</tbody>
</table>

7. Click **Next**.

The **Summary** page opens.
8. Review and verify the settings and then perform the appropriate action:

a. If the settings are not as desired, click on **Prev** and modify settings as required.

b. If the settings are verified, click on **Finish** to save the configuration.

---

**Note**

After you click **Finish**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the **Log On** page is displayed.

If you do not want to reboot, you can click **Cancel** instead of **OK**. If you click **Cancel**, the Summary page reopens.

---

**Important**

If you exit the wizard before saving settings, the configuration is not saved.

---

**Related information**

➥ *Network Deployment Mode Overview*
Chapter 4

Getting Started

This chapter describes how to get started with Deep Discovery Web Inspector after initial deployment is complete.

Topics include:

• Management Console Navigation on page 4-2
• Getting Started Tasks on page 4-2
Management Console Navigation

The management console consists of the following elements:

**TABLE 4-1. Management Console Elements**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner</td>
<td>The management console banner contains:</td>
</tr>
<tr>
<td></td>
<td>• Product logo and name: For details, see <a href="#">Dashboard Overview on page 5-2</a>.</td>
</tr>
<tr>
<td></td>
<td>• Name of the user currently logged on: Click and select <strong>Change password</strong> to change the account password (see <a href="#">Changing Your Password on page 3-6</a>) or select <strong>Log off</strong> to log out of the management console.</td>
</tr>
<tr>
<td></td>
<td>• System time: Displays the current system date and time.</td>
</tr>
<tr>
<td></td>
<td>• Appliance IP address: Displays the IP address of the Deep Discovery Web Inspector appliance.</td>
</tr>
<tr>
<td></td>
<td>• Network traffic: Displays the incoming and outgoing network throughput.</td>
</tr>
<tr>
<td>Main Menu Bar</td>
<td>The main menu bar contains several menu items that allow you to configure product settings. For some menu items, such as <strong>Dashboard</strong>, clicking the item opens the corresponding screen.</td>
</tr>
<tr>
<td></td>
<td>For other menu items, sub-menu items appear when you click or mouse over the menu item. Clicking a sub-menu item opens the corresponding screen.</td>
</tr>
<tr>
<td>Context-sensitive Help</td>
<td>Use <strong>Help</strong> (?) to find more information about the screen that is currently displayed.</td>
</tr>
</tbody>
</table>

Getting Started Tasks

After you complete the initial deployment, there are additional tasks you must perform to get Deep Discovery Web Inspector up and running as quickly as possible. The following steps provide a high-level overview of these additional tasks. Each step links to more detailed instructions later in the document.
Note
If you have not completed the initial deployment, see Deployment on page 3-1.

Procedure

1. Open the management console.
   For details, see Opening the Management Console on page 3-5.

2. Manage your Deep Discovery Web Inspector product license as needed.
   For details, see Managing Your Product License on page 10-5.

3. Configure additional network settings as needed.
   For details, see Configuring Network Settings on page 9-14.

4. Configure the notification SMTP server.
   For details, see Configuring the Notification SMTP Server on page 9-18.

5. Import Virtual Analyzer images.
   For details, see Virtual Analyzer Images on page 9-43.

   Important
   At least one Virtual Analyzer image is required to perform analysis.

6. Configure a network connection for Virtual Analyzer sandbox instances.

   Note
   No network access is the default.

   For details, see Virtual Analyzer Network on page 9-47

7. Add at least one notification recipient to all critical and important alerts.
   For details, see Alerts on page 8-2.
8. Configure policies used to determine how objects are scanned and what actions to take with policy matches.

For details, see *Managing Policies on page 7-3* and *Managing User-Defined Settings on page 7-15*.


For details, see *Managing HTTPS Inspection Rules on page 7-8*.

10. (Optional) Register with Trend Micro Control Manager to download the suspicious objects.

    For details, see *Control Manager on page 9-25*. 
Chapter 5

Dashboard

Topics include:

- Dashboard Overview on page 5-2
- Default Dashboard View on page 5-3
- Threat Monitoring Tab on page 5-3
- System Status Tab on page 5-8
- Virtual Analyzer Tab on page 5-10
- Tabs on page 5-12
- Widgets on page 5-15
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:

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tabs</td>
<td>Tabs provide a container for widgets. For details, see Tabs on page 5-12.</td>
</tr>
<tr>
<td>Widgets</td>
<td>Widgets represent the core dashboard components. For details, see Widgets on page 5-15.</td>
</tr>
</tbody>
</table>
Note

The Add Widget button appears with a star when a new widget is available.

Click Play Tab Slide Show to show a dashboard slide show.

Default Dashboard View

The default dashboard view comes with predefined tabs, each with a set of widgets. You can rename, delete, and add widgets to these tabs.

The predefined tabs include:

- Threat Monitoring Tab on page 5-3
- System Status Tab on page 5-8
- Virtual Analyzer Tab on page 5-10

Threat Monitoring Tab

The Threat Monitoring tab is displayed on the dashboard by default.
You can view threat-monitoring widgets to understand what is threatening your network and the pattern of the threats over time.

The following threat-monitoring widgets are displayed by default:

- Advanced Threat Indicators on page 5-4
- C&C Callback Detections Over Time on page 5-5
- Ransomware Detections Over Time on page 5-6
- Top Affected Hosts on page 5-5
- Top Detected URLs on page 5-7
- Virtual Analyzer Sandbox Analysis on page 5-7

**Advanced Threat Indicators Widget**

The **Advanced Threat Indicators** widget displays the total advanced detections for each threat indicator type per selected time period and the change between the number of detections from the last period for each indicator.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Total</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware Detections</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Coin Miners</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CSC Callbacks</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Suspicious Domains/URLs</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Suspicious Documents</td>
<td>4</td>
<td>(67%)</td>
</tr>
<tr>
<td>Suspicious Scripts</td>
<td>58</td>
<td>(397%)</td>
</tr>
<tr>
<td>Suspicious Malware</td>
<td>11</td>
<td>(8%)</td>
</tr>
</tbody>
</table>

- Click a number under the **Total** column to learn more about the detections for that indicator. Clicking a number opens the **All Detections** screen with the appropriate threat indicator filter set to see detections only for that indicator type.
• Threat indicators include:
  • **Ransomware Detections**
    All ransomware detections found by URL category or Scan Engine.
  • **Coin Miners**
    All coin miner detections found by URL category or Scan Engine.
  • **C&C Callbacks**
    Detections found for C&C Callbacks by URL category or Scan Engine
  • **Suspicious Domains/URLs**
    Detections that are part of the Suspicious Object blacklist domain/URL detections.
  • **Suspicious Documents**
    High risk detections for Office and PDF documents.
  • **Suspicious Scripts**
    High risk detections for certain scripts including html/html application, javascript, java jar/class, vb, windows shell or script, .bat, or .svg files.
  • **Suspicious Malware**
    High risk file detections that do not fall into the SO suspicious document or suspicious script indicators

**C&C Callback Detections Over Time Widget**

You can view the **C&C Callback Detections Over Time** widget to see the number of C&C callback detections over the selected time period.

• Deep Discovery Web Inspector uses the C&C URL category for detections.
• You can hover over a specific entry to see the C&C callbacks count for that time.
• If you click on an entry, the **All Detections** screen opens and displays results for the selected time with results filtered for the C&C callback threat indicator.
You can view detailed information about each detection including the time, risk level, host, URL, threat name, and action for each detection.

- If you click **View all C&C callbacks**, the **Detections > All Detections** screen opens with the **C&C Callbacks Threat Indicator** filter applied.

You can view detailed information about C&C callback detections in this screen.

### Ransomware Detections Over Time Widget

You can view the **Ransomware Detections Over Time** widget to see the number of ransomware detections over the selected time period.

- Deep Discovery Web Inspector uses all available Trend Micro detections engines for ransomware detection.
- You can hover over a specific ransomware entry to see the ransomware count for that time.
- If you click on an entry, the **All Detections** screen opens and displays results for the selected time with results filtered for the ransomware threat indicator.

You can view detailed information about each detection including the time, risk level, host, URL, threat name, and action for each detection.

- If you click **View all ransomware detections**, the **Detections > All Detections** screen opens with the **Ransomware Threat Indicator** filter applied.

You can view detailed information about ransomware detections in this screen.

### Top Affected Hosts Widget

You can view the **Top Affected Hosts** widget to see the hosts (listed by IP address) with the highest number of critical risks detected over the selected time period.

- From the drop-down, you can adjust the top number of hosts to include in the graph: 5, 10, 15, or 20
- You can hover over a specific host entry to see the number of detections for that host.
If you click on the host entry, the All Detections screen opens with results filtered for the selected host IP address. From this page, you can view detailed information about detections for that host, including the risk level, URL, threat name, and action for each detection.

If you click View all hosts, the Detections > Hosts screen opens where you can view detailed information for all hosts with detections during the selected time period.

**Top Detected URLs Widget**

You can view the Top Detected URLs widget to see the URLs with the highest number of critical risks detected over the selected time period. Trend Micro Web Reputation Services is used to determine the URL risk level.

- You can adjust the top number of hosts to include in the graph: 5, 10, 15, or 20
- You can hover over a specific URL to see the entire URL path and the number of detections for that URL.
- If you click on the URL entry, the All Detections screen opens with results filtered for the selected URL where you can view detailed information about detections for that URL.
- If you click View all URLs, the Detections > URLs screen opens where you can view detailed information about all URLs detected during the selected time period.

**Virtual Analyzer Sandbox Analysis Widget**

You can view the Virtual Analyzer Sandbox Analysis widget to see the how many objects were analyzed over the specified time period.

- You can see the count and percentage of analyzed objects that were suspicious and the count and percentage of analyzed objects that were non-suspicious.
System Status Tab

The System Status tab is displayed on the dashboard by default.

You can view the system status widgets to monitor the Deep Discovery Web Inspector appliance hardware and the connection and throughput status.

The following system status widgets are displayed by default:

- Hardware Status Widget on page 5-8
- Connection Status Widget on page 5-9
- Traffic Status Widget on page 5-9
- Bandwidth Status Widget on page 5-10

Hardware Status Widget

The Hardware Status widget shows the Deep Discovery Web Inspector appliance's current CPU, memory, and disk usage over the selected time period.

- The time periods you can select include Realtime, Last 24 hours, Last 7 days, and Last 30 days.
- Status categories displayed include CPU usage, Memory usage, and Disk usage.
- You can hover over a specific entry to see the system usage for each category for that time.
- Click an item in the widget legend (CPU usage, Memory usage, Disk usage) to show or hide data related to that category.

Note

“Disk usage” refers to the amount of data stored on the disk partition /var/app_data.
Connection Status Widget

You can view the **Connection Status** widget to see the number of connections per protocol over the selected time period.

- The time periods you can select include **Realtime**, **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Protocol categories displayed include **Total**, **HTTP**, **HTTP2**, and **HTTPS**.
- You can hover over a specific entry to see the connection count by protocol for that time.
- Click an item in the widget legend (Total, HTTP, HTTP2, or HTTPS) to show or hide data related to that metric.

Traffic Status Widget

You can view the **Traffic Status** widget to see the total traffic (KB, GB, or TB) per protocol over the selected time period handled by Deep Discovery Web Inspector.

- The time periods you can select include **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Traffic by protocol categories displayed include **Total**, **HTTP**, **HTTP2**, and **HTTPS**.
- You can hover over a specific entry to see the total traffic by protocol for that time.
- Click an item in the widget legend (Total, HTTP, HTTP2, or HTTPS) to show or hide data related to that metric.
Bandwidth Status Widget

You can view the **Bandwidth Status** widget to see the total bps (Kbps, Gbps, or Tbps) per protocol over the selected time period handled by Deep Discovery Web Inspector.

- The time periods you can select include **Last 24 hours**, **Last 7 days**, and **Last 30 days**.
- Bps by protocol categories displayed include **Total**, **HTTP**, **HTTP2**, and **HTTPS**.
- You can hover over a specific entry to see the total bps by protocol for that time.
- Click an item in the widget legend (Total, HTTP, HTTP2, or HTTPS) to show or hide data related to that metric.

Virtual Analyzer Tab

The **Virtual Analyzer** tab is displayed on the dashboard by default.

View Virtual Analyzer widgets to assess performance based on analysis processing time, queue size, and the volume of suspicious objects discovered for a specified time period.

The following Virtual Analyzer status widgets are displayed by default:
• *Average Virtual Analyzer Processing Time on page 5-11*
• *Suspicious Objects from Virtual Analyzer on page 5-11*
• *Virtual Analyzer Queue on page 5-12*

**Average Virtual Analyzer Processing Time Widget**

The *Average Virtual Analyzer Processing Time* widget shows the average time in seconds between when Virtual Analyzer receives an object and completes analysis.

- The graph is based on the selected period. The Y-axis represents the average length of time required to analyze the object. The X-axis represents the period.
- Mouse-over a point on the graph to view the average processing time and the period.
- Click **Manage Virtual Analyzer** to reallocate instances, to add or remove images, or to make other changes to Virtual Analyzer settings.

**Suspicious Objects from Virtual Analyzer Widget**

The *Suspicious Objects from Virtual Analyzer* widget shows the suspicious objects found by Virtual Analyzer for the specified time.

Suspicious objects are objects with the potential to expose systems to danger or loss. Virtual Analyzer detects and analyzes suspicious IP addresses, domains, files, and URLs.

- The graph is based on the selected period. The Y-axis represents the number of suspicious object detected. The X-axis represents the period.
- Mouse-over a point on the graph to view the number of high risk detections for each object and the time period.
• Click an item in the widget legend to show or hide data related to that metric.

• If you click **View suspicious objects**, the **Detections > Suspicious Objects** screen opens where you can view detailed information about all suspicious objects for the selected time period.

**Virtual Analyzer Queue Widget**

The **Virtual Analyzer Queue** widget shows all files queued for analysis in Virtual Analyzer for the specified time.

• The graph is based on the selected period. The Y-axis represents the file count. The X-axis represents the period.

• Mouse-over a point on the graph to view the number of queued files and the period.

**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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a tab</td>
<td>Click the plus icon (⁺) on top of the dashboard. The New Tab window displays. For information about this window, see New Tab Window on page 5-13.</td>
</tr>
<tr>
<td>Edit a tab's settings</td>
<td>Click Tab Settings. A window similar to the New Tab window opens, where you can edit settings.</td>
</tr>
<tr>
<td>Move a tab</td>
<td>Use drag-and-drop to change a tab’s position.</td>
</tr>
<tr>
<td>Delete a tab</td>
<td>Click the delete icon (✗) next to the tab title. Deleting a tab also deletes all the widgets in the tab.</td>
</tr>
</tbody>
</table>

**New Tab Window**

The New Tab window opens when you click the plus icon (⁺) on top of the dashboard.
This window includes the following options:

![New Tab Window]

**TABLE 5-1. New Tab Tasks**

<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Type the name of the tab.</td>
</tr>
<tr>
<td>Layout</td>
<td>Choose from the available layouts.</td>
</tr>
<tr>
<td>Slide Show</td>
<td>Select to include the tab in the Dashboard slide show.</td>
</tr>
<tr>
<td>Duration</td>
<td>Type the number of seconds to display the tab during the</td>
</tr>
<tr>
<td></td>
<td>Dashboard slide show.</td>
</tr>
<tr>
<td>TASK</td>
<td>STEPS</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auto-fit</td>
<td>Choose <strong>On</strong> or <strong>Off</strong>. This feature works when there is only one widget in a column. Choose <strong>On</strong> to adjust the height of the single widget to match the highest column.</td>
</tr>
</tbody>
</table>

**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.

**List of Widgets**

You can add any of the following widgets to the dashboard:

- System Status widgets (4)
  - Connection Status*
  - Hardware Status*
  - Traffic Status*
  - Bandwidth Status*
- Threat Monitoring widgets (6)
  - Advanced Threat Indicators*
  - C&C Callback Detections Over Time*
  - Ransomware Detections over Time*
  - Top Affected Hosts*
  - Top Detected URLs*
  - Virtual Analyzer Sandbox Analysis*
- Virtual Analyzer widgets (3)
• Average Virtual Analyzer Processing Time*
• Suspicious Objects from Virtual Analyzer*
• Virtual Analyzer Queue*

* denotes widgets displayed by default.

Adding New Widgets

You can add new widgets to tabs on the dashboard.

Procedure

1. Go to Dashboard.

2. Select the tab to which you want to add a widget.

3. Click the Add Widgets icon (➕) in the upper-right corner of the tab selected on the dashboard.

   The Add Widgets selection screen appears.

4. Select one or more widgets from the widget list by selecting the check box next to the widget's title.

Tip

• To sort widgets by category, click a category on the left side of the screen.

• To search for a widget, specify the widget name in the search text box at the top.

• To switch between the Detailed and Summary views, click the display icons (டட்டட்ட) at the top right.

• To change the widget count per page, select a number from the Records drop-down menu.

5. Click Add.

   After adding the widget, you can drag-and-drop the widget to various locations within the tab.
Managing Widgets

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

### Table 5-2. Widget Options Menu

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access widget options</td>
<td>Click the options icon (✓) at the widget's top-right corner to view the menu options.</td>
</tr>
<tr>
<td>Edit a widget</td>
<td>Click the edit icon (✓) to change settings.</td>
</tr>
<tr>
<td>Refresh widget data</td>
<td>Click the refresh icon (✓) to refresh widget data.</td>
</tr>
<tr>
<td></td>
<td>Click the refresh settings icon (✓) to set the frequency that the widget refreshes or to automatically refresh widget data.</td>
</tr>
<tr>
<td>Get help</td>
<td>Click the question mark icon (✓) to get help. The online help appears explaining how to use the widget.</td>
</tr>
<tr>
<td>Delete a widget</td>
<td>Click the delete icon (✗) to close the widget. This action removes the widget from the tab that contains it, but not from any other</td>
</tr>
<tr>
<td></td>
<td>tabs that contain it or from the widget list in the Add Widgets screen.</td>
</tr>
<tr>
<td>Move a widget within the</td>
<td>Use drag-and-drop to move the widget to a different location within the tab.</td>
</tr>
<tr>
<td>same tab</td>
<td></td>
</tr>
</tbody>
</table>

**Dashboard**

5-17
<table>
<thead>
<tr>
<th><strong>TASK</strong></th>
<th><strong>STEPS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Move a widget to a different tab</td>
<td>Use drag-and-drop to move the widget to the tab title. An option appears to either copy or move the widget to the destination tab location.</td>
</tr>
<tr>
<td>Resize a widget</td>
<td>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.</td>
</tr>
<tr>
<td>Change period</td>
<td>If available, click the <strong>Period</strong> drop-down menu to select the time period.</td>
</tr>
</tbody>
</table>
Chapter 6

Detections

- Understanding Risk Levels on page 6-2
- Threat Indicator and Detected By Classifications on page 6-4
- Viewing Detections on page 6-7
  - Viewing All Detections on page 6-7
  - Viewing Detections for Hosts on page 6-13
  - Viewing Detections for URLs on page 6-14
  - Viewing Detections for Files on page 6-16
  - Investigating Details About a Detection on page 6-11
- Viewing Suspicious Objects on page 6-18
  - Viewing Suspicious IP Address Objects on page 6-18
  - Viewing Suspicious Domain Objects on page 6-19
  - Viewing Suspicious URLs on page 6-20
  - Viewing Suspicious File Objects on page 6-21
Understanding Risk Levels


If the object has unknown or suspicious characteristics, the detected object is sent to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious behavior to identify potential threats.

Deep Discovery Web Inspector assigns a risk level to the object based on the highest risk assigned between the Deep Discovery Web Inspector scanners and Virtual Analyzer.

For details about how Deep Discovery Web Inspector investigates objects, see A New Solution on page 1-7.

Detection Risk Levels

The following table explains the detected risk levels after investigation. View the table to understand why detected objects are classified as high, medium, low, or user-defined risk.

**TABLE 6-1. Risk Definitions**

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| High       | High-risk detections have with malicious characteristics. A high-risk object contains:  
  • Files with unknown threats detected as high risk by Virtual Analyzer Filter  
  • Objects detected as high risk based on analysis by Trend Micro multi-layered threat detection |
Medium-risk detections have characteristics that are most likely malicious. A medium-risk object contains:

- Known malware
- Known dangerous links
- Objects detected as medium risk by Virtual Analyzer Filter

Low-risk detections have suspicious characteristics. A low-risk object contains:

- Known highly suspicious or suspicious links
- Links detected as low risk by Virtual Analyzer
- Files detected as low risk by Virtual Analyzer
- URLs detected as low risk based on suspicious URL matching

User Defined

An object that is blocked/receives warning under the following scenarios:

- Untrusted server certificate
- User-defined policy

**Virtual Analyzer Risk Levels**

The following table explains the Virtual Analyzer risk levels after object analysis. View the table to understand why a suspicious object was classified as high, medium, or low risk.
### Risk Level and Description

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| High       | 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 |
| Medium     | The sample exhibited moderately suspicious characteristics that are also associated with benign applications. |
| Low        | The object exhibited mildly suspicious characteristics that are most likely benign. |

### Threat Indicator and Detected By Classifications

Understanding what the threat indicators are and what type of Trend Micro detection technology detected each threat can be useful in understanding how to interpret detection data.

### Threat Indicator Classifications

The following table explains the threat indicators detected during scanning or analysis.  
View the table to understand the malicious activity affecting your network.
### Table 6-2. Threat Indicator Classifications

<table>
<thead>
<tr>
<th>Threat Indicator</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>Malware that limits user access to a system either by locking the user out of the system or encrypts the user's files unless a ransom is paid.</td>
</tr>
<tr>
<td>Coin Miners</td>
<td>Malware used by attackers for cryptocurrency mining.</td>
</tr>
<tr>
<td>C&amp;C Callbacks</td>
<td>Communication used by Command and Control (C&amp;C) servers which are used to remotely send commands to, download malicious content to, or exfiltrate data from infected clients.</td>
</tr>
<tr>
<td>Suspicious Malware</td>
<td>Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems. Detections are included in this category if they are not included in the Suspicious Documents or Suspicious Scripts indicator categories.</td>
</tr>
<tr>
<td>Suspicious URLs</td>
<td>A domain or URL that links to an unknown malicious website.</td>
</tr>
<tr>
<td>Suspicious Documents</td>
<td>High risk detections for Office and PDF documents.</td>
</tr>
<tr>
<td>Suspicious Scripts</td>
<td>High risk detections for script files that exhibits malicious characteristics. Script files include HTML, HTML application, JavaScript, Java jar/class, VB, Windows shell/script, BAT, and SVG files.</td>
</tr>
</tbody>
</table>

**Important**

Always handle suspicious files with caution.

### Detected By Classifications

The following table explains the categories that you can select in the Detected By advanced filter field. View the table to understand how objects are detected.
<table>
<thead>
<tr>
<th>DETECTED BY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Objects detected by all detection sources.</td>
</tr>
<tr>
<td>Untrusted Server Certificate</td>
<td>The secure URL or domain has an untrusted SSL server certificate.</td>
</tr>
<tr>
<td>Blocked URLs</td>
<td>URL accessed is listed in the blocked URL list.</td>
</tr>
<tr>
<td>Temporary Blocked URLs</td>
<td>URL is blocked by Deep Discovery Web Inspector cache because the same violation is detected again within four hours.</td>
</tr>
<tr>
<td>Web Reputation Services</td>
<td>Web Reputation Services is a part of the Trend Micro Smart Protection Network and scrutinizes URLs before users access potentially dangerous websites.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>URL accessed was included in a policy. When a user requests a URL, Deep Discovery Web Inspector looks up the category for that URL and then blocks the access to the dangerous URL category, such as the category for “Ransomware” or “C&amp;C Callback”.</td>
</tr>
<tr>
<td>True File Type</td>
<td>True file type accessed was included the file types section of a policy. Including file types in the policy can trigger a detection based on certain defined true file types (archives, executables, Office documents, PDF files, and scripts).</td>
</tr>
<tr>
<td>Anti-Malware (Advanced Threat Scan Engine)</td>
<td>Malware detected by the Advanced Threat Scan Engine.</td>
</tr>
<tr>
<td>Anti-Malware (Static Intelligence Engine)</td>
<td>Malware detected by the Static Intelligence Engine. Static signature-based detection involves searching for known patterns of data within executable code or behavior analysis.</td>
</tr>
<tr>
<td>Anti-Malware (Script Analyzer Lineup)</td>
<td>Malware detected by the Script Analyzer Lineup.</td>
</tr>
<tr>
<td>Anti-Botnet</td>
<td>Monitoring and analyzing network traffic to help identify bot activity so it can be blocked or eradicated.</td>
</tr>
</tbody>
</table>
Suspicious Objects Analysis (Virtual Analyzer)  
Suspicious object detected through Virtual Analyzer. Virtual Analyzer can analyze IP address, domain, URL, and file objects.

Suspicious Objects Filtering (Virtual Analyzer)  
Violations detected by Virtual Analyzer reported IP addresses, domains, URLs, and files objects.

### Viewing Detections

You can query and view detections to:

- Better understand the threats affecting your network and their relative risk
- Discover trends and learn about related detections
- See how Deep Discovery Web Inspector handled the detected object

### Related information

- Viewing All Detections
- Viewing Detections for Hosts
- Viewing Detections for URLs
- Viewing Detections for Files
- Investigating Details About a Detection

### Viewing All Detections

All detections are the cumulative detections for hosts, URLs, and files that contain malicious or suspicious content. Deep Discovery Web Inspector assigns a risk rating to each detection based on the investigation results.

By viewing all detections, you can gain intelligence about the context of suspicious detections by investigating a wide array of information facets. You can investigate attacks trending on your network by correlating common characteristics.
Based on the detections, you can change your policy configuration and warn your users to take preventive measures against similar attacks.

You can narrow your results by applying basic and advanced filters.

---

**Procedure**

1. Go to **Detections > All Detections**.
2. Specify the search criteria.

   *Applying Basic Filters on page 6-8*

   *Applying Advanced Filters on page 6-9*

3. Click on the Search (🔍) icon or press **Enter** to filter the results.
   All detections matching the search criteria appear.

4. Click the expansion icon (▶) beside a detection to view detailed results.

   *Detection Details on page 6-12*

---

**Related information**

* Threat Indicator and Detected By Classifications
* Understanding Risk Levels

---

**Applying Basic Filters**

When viewing all detections, you can use basic filters to narrow the results.

---

**Procedure**

1. Go to **Detections > All Detections**.
2. Specify the information to filter.

   The following table explains the basic search filters for querying detections.
Note

Search filters do not accept wildcards. Deep Discovery Web Inspector uses fuzzy logic to match search criteria to detection data.

<table>
<thead>
<tr>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level</td>
<td>Select All, High and Medium, High, Medium, Low, or User Defined.</td>
</tr>
<tr>
<td></td>
<td>The default risk level is High and Medium. For details about risk levels, see Understanding Risk Levels on page 6-2.</td>
</tr>
<tr>
<td>Action</td>
<td>Select All, Block, or Warning.</td>
</tr>
<tr>
<td>Host</td>
<td>Search for a specific host by specifying a host IP address.</td>
</tr>
<tr>
<td>Period</td>
<td>Select a predefined time range or specify a custom range.</td>
</tr>
<tr>
<td></td>
<td>If specifying a custom range, specify a starting and ending time for the range.</td>
</tr>
</tbody>
</table>

When applying basic filters, Deep Discovery Web Inspector dynamically displays the filtered results.

3. Click on Clear filters before staring a new filter search.

### Applying Advanced Filters

When viewing all detections, in addition to basic search filters, you can use advanced search filters to narrow the results.

**Procedure**

1. Go to Detections > All Detections.
2. Enter any basic search filters you would like to use.  
   
   Applying Basic Filters on page 6-8
3. Click Show advanced filters.
The advanced filters appear.

4. Specify the information in the advanced filter fields.

   **Note**
   
   Search filters do not accept wildcards. Deep Discovery Web Inspector uses fuzzy logic to match search criteria to detection data.

<table>
<thead>
<tr>
<th><strong>FILTER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specify the domain associated with the detection.</td>
</tr>
<tr>
<td>URL</td>
<td>If the detection type is URL, specify a URL.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Specify the server IP associated with the detection.</td>
</tr>
<tr>
<td>File SHA1</td>
<td>If the detection type is File, specify the file SHA1 associated with the detection.</td>
</tr>
<tr>
<td>Policy name</td>
<td>Specify the name of the policy that triggered the detection match.</td>
</tr>
<tr>
<td>Detected by</td>
<td>Select a detected by category from the list.</td>
</tr>
<tr>
<td>Threat indicator</td>
<td>Select a threat indicator from the list.</td>
</tr>
</tbody>
</table>

   For details, see [Detected By Classifications on page 6-5.](#)

5. Click **Search**.
Investigating Details About a Detection

Procedure

1. Search for the detection.

   See Viewing All Detections on page 6-7.

2. Click the arrow next to the detection in the table.

   The table row expands to display detailed information.
3. Examine the detection details.

See Detection Details on page 6-12.

Detection Details

The following table explains the detection details viewable after expanding a detection entry. Detection details are divided into two categories: Detection Information and Connection Information. The contents of each display field varies depending on the type of detected threat.

Detection Information

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk level</td>
<td>High, Medium, Low, or User Defined.</td>
</tr>
<tr>
<td></td>
<td>See Detection Risk Levels on page 6-2.</td>
</tr>
<tr>
<td>Detected by</td>
<td>See Detected By Classifications on page 6-5.</td>
</tr>
<tr>
<td>Threat type</td>
<td>See Threat Indicator Classifications on page 6-4.</td>
</tr>
<tr>
<td>Threat name</td>
<td>Click the listed threat name to get correlated information about suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network, which provides relevant and actionable intelligence.</td>
</tr>
<tr>
<td>File name</td>
<td>The name of the file, if any, for the detection.</td>
</tr>
<tr>
<td>File SHA1</td>
<td>The file SHA1, if any, for the detection.</td>
</tr>
<tr>
<td>Policy name</td>
<td>The name of the policy applied to the detection.</td>
</tr>
<tr>
<td>Action</td>
<td>Monitor or Block.</td>
</tr>
</tbody>
</table>

Connection Information

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>The latest detection time.</td>
</tr>
<tr>
<td>Host IP</td>
<td>The destination for the object.</td>
</tr>
</tbody>
</table>
### Viewing Detections for Hosts

Detected hosts are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.

#### Procedure

1. Go to **Detections > Hosts**.
2. Optionally, filter the result set by specifying search criteria.
   - **Host**
   - **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a host, click on the Search (균) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.
3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>View the IP address of the host with detections of suspicious objects.</td>
</tr>
<tr>
<td>HEADER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected object.</td>
</tr>
<tr>
<td>High Risk</td>
<td>View the number of high risk detections for the selected object. These are detections with malicious characteristics.</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.</td>
</tr>
<tr>
<td>Low Risk</td>
<td>View the number of low risk detections for the selected object. These are detections with suspicious characteristics.</td>
</tr>
<tr>
<td>User Defined</td>
<td>View the number of detections for user-defined objects. These detections might include the following: “Untrusted Server Certificate” or user-defined policy.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
</tbody>
</table>

4. Under **Detections**, click on the number to view more detailed information about detections for that host.

The **All Detections** screen opens with the results filtered for that host.

See *Viewing All Detections on page 6-7*.

**What to do next**

After viewing host detections, you can export the results by clicking on **Export All**.

**Viewing Detections for URLs**

Detected URLs are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.
Procedure

1. Go to Detections > URLs.

2. Optionally, filter the result set by specifying search criteria.
   - URL
   - Period

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a URL, click on the Search ( Mug ) icon or press Enter to filter the results.

   All detections matching the search criteria appear.

3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>View the URL with detections of suspicious objects.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected object.</td>
</tr>
<tr>
<td>High Risk</td>
<td>View the number of high risk detections for the selected object. These are detections with malicious characteristics.</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.</td>
</tr>
<tr>
<td>Low Risk</td>
<td>View the number of low risk detections for the selected object. These are detections with suspicious characteristics.</td>
</tr>
<tr>
<td>User Defined</td>
<td>View the number of detections for user-defined objects. These detections might include the following: &quot;Untrusted Server Certificate&quot; or user-defined policy.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
</tbody>
</table>
4. Under **Detections**, click on the number to view more detailed information about detections for that URL.

   The **All Detections** screen opens with the results filtered for that URL.

   See *Viewing All Detections on page 6-7*.

**What to do next**

After viewing URL detections, you can export the results by clicking on **Export All**.

**Viewing Detections for Files**

Detected files are objects that have been compromised with malicious or suspicious activity. Gain intelligence about who in your network is targeted and understand the attack behavior.

**Procedure**

1. Go to **Detections > Files**.

2. Optionally, filter the result set by specifying search criteria.
   
   • **File SHA1**
   
   • **Period**

   When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

   When specifying a file SHA1, click on the Search (🔍) icon or press **Enter** to filter the results.

   All detections matching the search criteria appear.

3. View the results.
### Table

<table>
<thead>
<tr>
<th><strong>HEADER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>File SHA1</td>
<td>View the file SHA1s that Deep Discovery Web Inspector detected as suspicious objects.</td>
</tr>
<tr>
<td>Threat Name</td>
<td>View the threat name of the discovered suspicious file.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected object.</td>
</tr>
<tr>
<td>High Risk</td>
<td>View the number of high risk detections for the selected object. These are detections with malicious characteristics.</td>
</tr>
<tr>
<td>Medium Risk</td>
<td>View the number of medium risk detections for the selected object. These are detections with characteristics that are most likely malicious.</td>
</tr>
<tr>
<td>Low Risk</td>
<td>View the number of low risk detections for the selected object. These are detections with suspicious characteristics.</td>
</tr>
<tr>
<td>User Defined</td>
<td>View the number of detections for user-defined objects. These detections might include the following: “Untrusted Server Certificate” or user-defined policy.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
</tbody>
</table>

4. Under **Detections**, click on the number to view more detailed information about detections for that file.

The **All Detections** screen opens with the results filtered for that file SHA1.

See *Viewing All Detections on page 6-7*.

### What to do next

After viewing file detections, you can export the results by clicking on **Export All**.
Viewing Suspicious Objects

Suspicious objects are objects that Virtual Analyzer analysis determined have the potential to expose systems to danger or loss.

Query suspicious objects to:

• Better understand the threats affecting your network and their relative risk
• Assess the prevalence of suspicious IP addresses, domains, URLs, and files
• Find infected endpoints in your network
• Proactively contain or block infections

Related information

➥ Viewing Suspicious IP Address Objects
➥ Viewing Suspicious Domain Objects
➥ Viewing Suspicious URLs
➥ Viewing Suspicious File Objects

Viewing Suspicious IP Address Objects

A suspicious IP address has the potential to expose systems to danger or loss.

View suspicious IP addresses to understand your risk and assess the relative prevalence of the suspicious IP address. Find out detailed information about the detections found for a specific IP address.

Procedure

1. Go to Detections > Suspicious Objects > IP Addresses.
2. Specify the search criteria.
   • IP Address
   • Period
When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

When specifying an IP address, click on the Search (Q) icon or press Enter to filter the results.

All detections matching the search criteria appear.

3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Object</td>
<td>View the IP address used by the suspicious object.</td>
</tr>
<tr>
<td>Port</td>
<td>View the port number used by the suspicious object.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>View the level of potential danger in an suspicious object.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected suspicious IP address.</td>
</tr>
</tbody>
</table>

**Viewing Suspicious Domain Objects**

A suspicious domain has the potential to expose systems to danger or loss.

View suspicious domains to understand your risk and assess the relative prevalence of the suspicious domain. Find out detailed information about the detections found for a specific domain.

**Procedure**

1. Go to **Detections > Suspicious Objects > Domains**.

2. Specify the search criteria.
   - **Domain**
   - **Period**
When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

When specifying a domain, click on the Search (🔍) icon or press Enter to filter the results.

All detections matching the search criteria appear.

3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Object</td>
<td>View the domain name used by the suspicious object.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>View the level of potential danger in an suspicious object.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected suspicious domain.</td>
</tr>
</tbody>
</table>

### Viewing Suspicious URLs

A suspicious URL has the potential to expose systems to danger or loss.

View suspicious URLs to understand your risk and assess the relative prevalence of the suspicious URL. Find out detailed information about the detections found for a specific URL.

#### Procedure

1. Go to **Detections > Suspicious Objects > URLs**.
2. Specify the search criteria.
   - **URL**
   - **Period**

When specifying a period, Deep Discovery Web Inspector dynamically filters the results.
When specifying a URL, click on the Search (Q) icon or press Enter to filter the results.

All detections matching the search criteria appear.

3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Object</td>
<td>View the web address of the suspicious object.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>View the level of potential danger in an suspicious object.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected suspicious URL.</td>
</tr>
</tbody>
</table>

Viewing Suspicious File Objects

A suspicious file has the potential to expose systems to danger or loss.

View suspicious file SHA1s to understand your risk and assess the relative prevalence of the suspicious file. Find out detailed information about the detections found for a specific file SHA1.

Procedure

1. Detections > Suspicious Objects > Files.

2. Specify the search criteria.
   - File SHA1
   - Period

When specifying a period, Deep Discovery Web Inspector dynamically filters the results.

When specifying a file SHA1, click on the Search (Q) icon or press Enter to filter the results.
All detections matching the search criteria appear.

3. View the results.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Object</td>
<td>View the SHA1 value that uniquely identifies a file.</td>
</tr>
<tr>
<td>Risk Level</td>
<td>View the level of potential danger in an suspicious object.</td>
</tr>
<tr>
<td>Latest Detection</td>
<td>View the date and time for the most recent occurrence of the suspicious object detected in Deep Discovery Web Inspector.</td>
</tr>
<tr>
<td>Detections</td>
<td>View the number of detections with malicious or suspicious characteristics for the selected suspicious file SHA1.</td>
</tr>
</tbody>
</table>
Chapter 7

Policy

Topics include:

• Policy Overview on page 7-2
• Managing Policies on page 7-3
• Managing HTTPS Inspection Rules on page 7-8
• Managing User-Defined Settings on page 7-15
  • Managing Network Objects on page 7-16
  • Managing Domain Objects on page 7-17
  • Managing the Approved/Blocked List on page 7-19
  • Managing Notifications on page 7-22
Policy Overview

Deep Discovery Web Inspector integrates with a variety of powerful Trend Micro security filtering engines and technologies to scan web traffic coming in and out of your organization. Policy-related functionality allows you to control what happens to web traffic going through the Deep Discovery Web Inspector appliance.

Policies

You can create one or more policies to take action on specific network events reported by Deep Discovery Web Inspector. Policies are compared against incoming traffic in sequence, with the first policy that matches the traffic being applied. This provides flexibility while helping protect your network from advanced persistent threats and emerging unknown threats according to the configured policies.

You can configure risk-level actions for each policy that determines what happens for detections at each risk level. Possible actions are scan, allow, and block.

HTTPS Inspection Rules

You can configure HTTPS inspection rules that define which objects and URL categories Deep Discovery Web Inspector should decrypt for scanning. HTTPS traffic is encrypted, and must be decrypted before Deep Discovery Web Inspector can scan the traffic.

User Defined Settings

You can do the following with user defined settings:

- Create and customize network and domain objects that you use in policies and HTTPS inspection rules
- Configure approved and blocked lists to control which domains or URLs are allowed or blocked without needing to scan them
- Manage notifications that are sent to users when a violation occurs while they are requesting network resources
Managing Policies

Go to Policy > Policy to perform any of the following tasks to manage policies.

---

**Note**

The default policy is predefined and is always the last one in the policy list. You cannot select the default policy and cannot perform any action on it (move, duplicate, remove). You can only enable or disable the default policy.

---

**Procedure**

- View summary information about existing policies.
- Click **Add** to create a new policy.
- Click a policy's name to view or modify settings, including enabling or disabling the policy.
- Select a policy and then click **Move Up**, **Move Down**, or **Move Top** to change the policy order.
- Select a policy and then click **Duplicate** to make a copy of the policy.
- Select a policy and then click **Remove** to remove the policy.

---

**Information About How Policies Work**

Each policy can be as general or specific as needed. Policies are compared against incoming traffic in sequence, and because the first policy that matches the traffic is applied, the more specific policies must precede the more general ones. For example, a policy for a single IP address must come before a rule for a network range that includes the single IP address if all other traffic-related settings are the same.

Policies are composed of network and domain objects that contain specified policy parameters and selected file types along with the actions to take if there is a traffic match.
• The network and domain objects are configured under user-defined settings, and can be created ahead of time or at the time of policy creation.

• The file types are predefined and include archives, executables, Office documents, PDF files, and script files.

### How Patient Zero Protection Works

Patient Zero Protection provides advanced malware protection from suspicious objects that have been sent to Virtual Analyzer for sandbox analysis.

When Patient Zero Protection is enabled, Deep Discovery Web Inspector temporarily holds the suspicious object while analysis is performed. Once analysis is complete, depending on the outcome of the analysis, the appropriate action is taken.

By enabling Patient Zero Protection, you ensure that malicious objects are not passed through to the destination while waiting for sandbox analysis to complete. This provides a higher level of protection against malware intrusions and attacks.

• Deep Discovery Web Inspector takes no action and delivers the object to the endpoint if it is marked as “No risk”.

• If sandbox analysis determines that the risk level for that object is low, medium, or high, the malicious object is blocked or monitored, according to the actions configured for the policy that triggered the analysis.

The default risk-level actions for a policy are to block high-risk and medium-risk objects and monitor low-risk objects.

• If Virtual Analyzer did not finish the sandbox analysis or even start the analysis during the allotted time, Deep Discovery Web Inspector allows the object to pass through to the destination.

If Deep Discovery Web Inspector encounters the object that did not finish or even start analysis again, the object is not sent to Virtual Analyzer for sandbox analysis; Deep Discovery Web Inspector allows the object to pass through.
Note

If Patient Zero Protection is disabled, suspicious objects are not held while analysis is ongoing. The suspicious objects are passed straight through.

The Default Policy

The default policy is a predefined default policy and is always the last one in the policy list.

The only operation that you can perform on the default policy is to enable or disable it.

You cannot do the following to the default policy:

• Select it or move it up or down in the policy rule list
• Delete the default policy
• Change the policy name or description
• Change the policy settings such as which network objects, domain objects, and file types are scanned
• Change the policy action and risk-level scan actions
• Enable or disable Patient-Zero

Viewing Policies

Procedure

1. Go to Policy > Policy.
2. View summary information about existing policies including:
   • The name of the policy and the network objects, domain objects, and file types included in the policy.
   • The action for each policy (Scan, Allow, or Block).
• The action to take for each risk level when a scanned object matches the policy if the action is **Scan**.

• Whether **Patient-Zero** is enabled or disabled if the action is **Scan**.

• The **default** policy is predefined and is always the last one in the policy list.

---

**Related information**

➥ **The Default Policy**

---

**Adding Policies**

Policies are composed of policy objects that contain specified policy parameters.

---

**Procedure**

1. Go to **Policy > Policy**.

2. Click **Add**.

3. Specify a policy name between 1 and 64 characters.

4. Optionally, specify a description between 1 and 128 characters.

5. Enable or disable the policy.

6. Configure **Network objects** by performing one of the following:
   - Select **Any** for the policy to affect all network objects.
   - Select **Selected network objects** for the policy to affect only specific network objects and then move one or more objects from the available network objects box to the selected network objects box.

You can create a new network object to include in the policy by clicking **Add New Network Object**.

See **Managing Network Objects on page 7-16**.
7. If you want to specify network objects to which this rule does not apply, select **Exceptions** and then move one or more objects from the available network objects box to the selected network objects box.

If an IP address is included in both the selected network objects list and the exceptions list, the presence in the exceptions list has higher priority.

If the client's IP address is part of a network object in the exception list of a policy, this policy will not be matched. Instead, Deep Discovery Web Inspector will look at the next policy to search for a match to this client's IP address.

8. Configure **Domain objects** by performing one of the following:
   - Select **Any** for the policy to affect all domain objects.
   - Select **Selected domain objects** for the policy to affect only specific domain objects and then move one or more objects from the available domain objects box to the selected domain objects box.

   You can create a new domain object to include in the policy by clicking on **Add New Domain Object**.

   See *Managing Domain Objects on page 7-17*.

9. Configure **File types** by performing one of the following:
   - Select **Any** for the policy to affect all defined file types.
   - Select **Selected file types** for the policy to affect only specific file types and then move one or more file types from the available file types box to the selected file types box.

   The available file types are predefined and cannot be configured.

10. Select the **Action**.
    - **Allow**
      
      If the traffic matches the policy, allow the traffic while bypassing scanning.
    - **Block**
      
      If the traffic matches the policy, block the traffic.
• **Scan**

11. If you configured **Scan** as the action, perform the following:
   a. Configure which action to take (**Block** or **Monitor**) for each risk level if this policy is matched.
   b. Enable or disable **Patient-Zero**.
      
      If Patient Zero Protection is enabled, objects that are sent to the Virtual Analyzer sandbox for analysis are temporarily held (neither delivered to the endpoint nor blocked) while waiting for sandbox analysis to complete. Once analysis is complete, depending on the outcome of the analysis, the appropriate action is taken.

12. Click **Save**.

---

**What to do next**

Move the policy to the desired location within the policy list.

### Managing HTTPS Inspection Rules

Go to **Policy > HTTPS Inspection** to perform any of the following tasks to manage HTTPS inspection rules.

**Procedure**

- View summary information about existing HTTPS inspection rules.
- Click **Add** to create a new rule.
- Click a rule's name to view or modify settings, including enabling or disabling the rule.
- Select a rule and then click **Move Up**, **Move Down**, or **Move Top** to change the rule order and to prioritize rules as needed.
- Select a rule and then click **Duplicate** to copy the selected rule.
• Select one or more rules and then click **Remove** to remove the rules.
• Generate a CSR to request a certificate from the Certificate Authority. You can import this certificate into an HTTPS Inspection rule.

HTTPS Inspection

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols widely adopted and deployed in network communication today. The traffic over SSL/TLS is encrypted and signed to ensure security. Because encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections, you can configure Deep Discovery Web Inspector to decrypt and scan selected HTTPS traffic for potential risks and threats.

You can configure HTTPS inspection rules to enable decryption and HTTPS inspection of specific network traffic based on the following criteria:

• All or selected network objects
• Selected URL categories
• Selected domain objects

To scan HTTPS traffic, Deep Discovery Web Inspector identifies the SSL connection at the first packet of the SSL handshake, acquires the client IP address information from the session, and identifies the URL categories of the target domain.

If the client IP is included in the configured Decryption Network Objects of an HTTPS Inspection policy and the target domain is in the configured Decryption Categories or if
If certain traffic matches multiple policies, the policy with the highest priority will take effect, and the traffic will be re-signed using the certificate configured in that policy. Deep Discovery Web Inspector will not decrypt the connection if it does not match any network objects, URL categories, or domain objects specified in the HTTPS Inspection policies.

After the HTTPS traffic to be inspected and the policy to use is identified, Deep Discovery Web Inspector re-signs the website certificate using that policy's CA certificate and decrypts and inspects the traffic and then determines the appropriate actions for traffic based on configured policies.

**Viewing HTTPS Inspection Rules**

**Procedure**

1. Go to **Policy > HTTPS Inspection**.
2. View summary information about existing rules including:
   - The name of the rule and the decryption network objects, decryption URL categories, and decryption domain objects included in the rule.
• Whether the rule is enabled.
• Information about the subject and issuer of the Certificate Authority (CA) used to re-sign the website certificate.

Adding/Editing HTTPS Inspection Rules

HTTPS inspection rules are composed of decryption network objects, decryption categories, and decryption domain objects that contain specified parameters. When Deep Discovery Web Inspector determines that network traffic matches an HTTPS inspection rule, the HTTPS traffic is decrypted and inspected and action taken according to the configured policy rules. HTTPS Inspection rules also provide the means to import and save CA certificates used to re-sign the website certificate.

Procedure

1. Go to Policy > HTTPS Inspection.
2. Click Add or click the item to edit.
3. Specify a policy name between 1 and 64 characters.
4. Optionally, specify a description between 1 and 128 characters.
5. Enable or disable the rule.
6. Configure Decryption network objects by performing one of the following:
   • Select Any for the rule to apply to all networks.
   • Select Selected network object for the rule to affect only specific network objects and then move one or more objects from the available network objects list to the selected network objects list.
     You can create a new network object to include in the HTTPS inspection rule.
     See Adding/Editing Network Objects on page 7-17.
7. Configure Decryption categories:
a. Click on the **Decryption categories** box to open the list of URL categories.

b. Select or deselect URL categories on which to apply the HTTPS inspection rule.

The available categories are predefined and cannot be configured. The categories are organized in a hierarchical structure with main categories and subcategories. Click the arrow by a main category to view the sub-categories. You can choose entire categories or only sub-categories to add to the list.

See *HTTPS Inspection on page 7-9.*

8. Configure **Decryption domain objects** by moving one or more objects from the available domain objects list to the selected domain objects list.

You can create a new domain object to include in the HTTPS inspection rule.

See *Adding/Editing Domain Objects on page 7-18.*

9. If you do not want to use the default Deep Discovery Web Inspector CA, you can use a private CA by doing one of the following under **Certificate:**

   a. If the certificate is not based on the CSR generated by Deep Discovery Web Inspector, do the following to import a certificate:

      i. In **Certificate**, browse and choose the certificate file.

      ii. In **Private key**, browse and choose the private key file for the certificate file.

      iii. Enter the password of the private key and then confirm it.

      iv. Click on **Verify Certificate** to verify that the certificate is valid.

   b. If the certificate is based on the CSR generated by Deep Discovery Web Inspector, do the following to import the certificate:

      i. Select **Certificate with CSR generated by DDWI**.

      ii. In **Certificate**, browse and choose the certificate file.

      iii. Click on **Verify Certificate** to verify that the certificate is valid.
Note
Deep Discovery Web Inspector uses the certificate to re-sign the website certificate and decrypt the traffic for inspection. You can use your own private CA certificate; however, you cannot use a CA certificate that is signed by a public certificate authority.

10. Click Save.

Note
You can also restore the certificate settings to the default Trend Micro Deep Discovery Web Inspector CA, from the Certificate section by clicking on Restore to Default.

What to do next
If you are using the default Trend Micro Deep Discovery Web Inspector CA, end-users can go to the following link or use the code to download the default CA:


Trend Micro provides a tool that Windows users can use to directly install and trust the Deep Discovery Web Inspector default CA. To download the tool go to the following link:

The file is password protected with the password: ddwi.

Generating a CSR

When Deep Discovery Web Inspector determines that network traffic matches an HTTPS inspection rule, the HTTPS traffic is decrypted and inspected and action taken according to the configured policy rules. You can generate a CSR to request a certificate from a Certificate Authority. You can import this certificate into an HTTPS Inspection rule. The certificate is used to re-sign the website certificate.

Procedure

1. Go to Policy > HTTPS Inspection.
2. Click Generate CSR to generate the CSR file.
   The Generate CSR window opens.
3. Specify the following parameters:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>The Common Name (CN) is typically composed of Host + Domain Name. It can also be the name of the server.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.</td>
</tr>
<tr>
<td>State/Province</td>
<td>Name of the state or province where your organization is located. Do not abbreviate.</td>
</tr>
<tr>
<td>Locality</td>
<td>Name of the city where your organization is registered or located. Do not abbreviate.</td>
</tr>
<tr>
<td>Organization</td>
<td>The legally-registered name for your business.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The name of the department or organization unit making the request.</td>
</tr>
</tbody>
</table>
4. Click **Generate CSR**.

   The following message is displayed: “CSR generated successfully, please click to download”.

5. Click **Download** to download the CSR to your local computer.

---

**Note**

Deep Discovery Web Inspector only archives one CSR and Private Key. If multiple certificates are needed, generate a CSR after the previous certificate has been imported successfully. Otherwise, the previous CSR and Private Key are replaced.

---

**Managing User-Defined Settings**

Go to **Policy > User Defined Settings** to perform any of the following tasks to manage user-defined settings.

---

**Procedure**

- Click on the **Network Objects** tab to configure network objects used when defining policies and HTTPS inspection rules.

- Click on the **Domain Objects** tab to configure domain objects used when defining policies and HTTPS inspection rules.

- Click on the **Approved/Blocked List** tab to configure which domains and URLs to add to the approved list or the blocked list.

- Click on the **Notifications** tab to customize notifications sent when violations occur to end-users that are requesting network resources.
Managing Network Objects

Go to Policy > User Defined Settings > Network Objects to perform any of the following tasks to manage network objects.

**Procedure**

- View summary information about existing objects.
- Click **Add** to create a new object.
- Click an object's name to view or modify settings.
- Select an object and then click **Remove** to remove the object.
- Click **Import/Export** to export a copy of the defined objects.

**Network Objects**

Network objects contain configurable parameters and are used by policies, HTTPS inspections rules, and alert notifications. Network objects are used to:

- Select the networks on which to apply a policy
- Select the networks on which to perform decryption for HTTPS inspection
- Select the networks to add to a policy's exceptions list.

Policy actions are not applied to networks in the exceptions list, even if they otherwise would meet the criteria for a configured policy action.

- Select the networks to add to an HTTPS inspection policy's exceptions list.
- Select the networks to use as a parameter in an alert notification rule.

The following notification rules can use network objects as a parameter:

- Security: Multiple Advanced Threat Detections in Specified Network Groups
- Security: Multiple Ransomware Detections in Specified Network Groups
• Security: Multiple C&C Callback Detections in Specified Network Groups
• Security: Multiple Coin Miner Detections in Specified Network Groups

Adding/Editing Network Objects

Network objects contain configurable parameters and are used by policies and HTTPS inspections rules.

Procedure

1. Go to Policy > User Defined Settings > Network Objects.
2. Click Add or click the item to edit.
   The Add/Edit Network Object screen opens.
3. Specify a name that describes the network object.
4. Optionally, enter a description.
5. Specify IP addresses as a single entry or comma-delimited list of IP addresses, Class InterDomain Routing (CIDR) networks, or IP address ranges.
   Example:
   • 10.0.0.8/23
   • 192.168.0.1, 10.0.0.1-10.0.0.4, 10.0.0.8/23
6. Click Save.

Related information

➥ Network Objects

Managing Domain Objects

Go to Policy > User Defined Settings > Domain Objects to perform any of the following tasks to manage domain objects.
Procedure

- View summary information about existing objects.
- Click **Add** to create a new object.
- Click an object’s name to view or modify settings.
- Select a object and then click **Remove** to remove the object.
- Click **Import/Export** to export a copy of the defined objects.

Domain Objects

Domain objects contain configurable parameters and are used by policies and HTTPS inspections rules. Domain objects are used to:

- Select the domains on which to apply a policy
- Select the domains on which to perform decryption for HTTPS inspection

Adding/Editing Domain Objects

Domain objects are used when creating policies or HTTPS exception rules.

Procedure

1. Go to Policy > User Defined Settings > Domain Objects.
2. Click **Add** or click the item to edit.
   
   The **Add/Edit Domain Object** screen opens.
3. Specify a name that describes the domain object.
4. Optionally, enter a description.
5. Note that the **Domain type** is Domain.
   
   Domain is the only available domain type.
6. Specify the domain to add.


If no wildcard is used, a match is found for the whole domain only. An IP address is a valid entry for a domain match.

Examples:

• Domain: mydomain.com
• Domain: *mydomain.com
• Domain: mydoma?n.com
• Domain: 192.168.2.1

7. Click Add.

8. Add additional domain entries as needed.

9. Click Save.

Related information

Domain Objects

Managing the Approved/Blocked List

Go to Policy > User Defined Settings > Approved/Blocked List to perform any of the following tasks to manage the approved and blocked list.

Procedure

• View summary information about existing URLs in the approved URLs and blocked URLs lists.
• Configure and add URLs to either the approved URLs or blocked URLs lists.
• Select a URL or domain in the approved URLs or blocked URLs list and then click **Delete** to remove the object.
• Click **Import/Export** to import or export a CSV file of the approved URLs and blocked URLs lists.

---

**Approved/Blocked List**

The approved and blocked lists allow traffic to override the defined policies, web reputation, and advanced threat protection settings.

Keep the following in mind when adding URLs to a list:

• You can create a URL to add to the lists using either a domain match or an URL match.
• An asterisk (*) or a question mark (?) denotes a wild card.
• The approved list takes precedence over the blocked list.

**Domain Match Entries**

You can add a domain match entry to the approved or blocked URL list. A match is found if the traffic matches the input domain. Wild cards can be used anywhere in the domain entry. In the examples below, the “*” wild card is used to do suffix or prefix matches. If no wild card is used, a match is found for the whole domain only. An IP address is a valid entry for a domain match.

Examples:

• **www.test.com** matches the domain site “www.test.com” only.
• ***www.test.com** matches any domain that ends with “www.test.com”.
• **www.test.com** matches any domain that starts with “www.test.com”.
• **www.test.c?m** matches “www.test.com”.
• **192.168.2.1** matches only that single IP address.

**URL Match Entries**

You can add a URL match entry to the approved or blocked URL list. A match is found if the traffic matches the input URL. In the examples below, the “*” wild card is used to
do suffix or prefix matching. If no wild card appears, Deep Discovery Web Inspector matches the whole URL only. The site prefixes http:// or https:// are insensitive and should not be included in the input for matching.

Examples:

• www.test.com matches the URL www.test.com only.
  Example: www.test.com.cn/test or www.test.com/test is not a match.

  Example: server.www.test.com is a match.

  Example: www.test.com.cn/test or www.test.com/test is a match.

Adding to the Approved/Blocked List

You can define domain and URL matches to add to the blocked or approved lists.

Procedure

1. Go to Policy > User Defined Settings > Approved/Blocked List

2. Do the following:
   • Click on the Domain tab to configure an entry using the domain match mode.
   • Click on the URL tab to configure an entry using the URL match mode.

3. Enter the domain or URL in the Domain type text box.
   For information about and examples for configuring entries for each match mode, see Approved/Blocked List on page 7-20.

4. Do the following:
   • Click Add to Approved.
• Click **Add to Blocked**.

5. Click **Save**.

---

**Managing Notifications**

Notifications are sent to end-users when a violation occurs while they are requesting network resources.

*List of User Notifications on page 7-22*

Go to **Policy > User Defined Settings > Notifications** to perform any of the following tasks to manage notifications.

---

**Procedure**

• View summary information about predefined notification templates.

• Click a notification name to view or modify the notification text or formatting.

• Click a notification name and then click **Reset** to reset the notification back to its predefined template.

---

**Note**

You cannot delete a predefined notification template or create any new templates.

---

**List of User Notifications**

<table>
<thead>
<tr>
<th><strong>NOTIFICATION</strong></th>
<th><strong>REASON NOTIFICATION SENT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Blocked: Advanced Threat Protection notification</td>
<td>When traffic was blocked because Deep Discovery Web Inspector detected an advanced threat on the page being accessed.</td>
</tr>
</tbody>
</table>
### Blocked URLs notification
When traffic was blocked by the **Blocked URLs** list.

### HTTPS Certificate Verification Failure notification
When traffic was blocked because a user tried to access an HTTPS website where the certificate is not trusted.

### Website Blocked: Patient-Zero notification
When Patient Zero Protection is enabled and a file has been submitted to Virtual Analyzer for sandbox analysis. The page will be blocked until sandbox analysis is complete. The action taken after analysis is complete is determined by the 'risk-level actions' of the matched policy. For the default settings, the high-risk and medium-risk levels will be blocked.

### Website Blocked: Scan Policy Block notification
When a policy violation occurred because the policy restricts access to inappropriate content and the action is **Block**.

## Notification Message Tokens
Deep Discovery Web Inspector sends notifications to alert end users about a security violation or if Deep Discovery Web Inspector detects other issues when a user attempts to access a web resource.

Each notification uses tokens to customize the message content and to provide information that is specific to that violation. Not all tokens are valid in every notification.

If you want to customize the notifications, you can use the following table to determine which tokens are accepted in each notification.
<table>
<thead>
<tr>
<th><strong>TOKEN</strong></th>
<th><strong>FIELD NAME</strong></th>
<th><strong>NOTIFICATIONS WHERE TOKEN VALID</strong></th>
</tr>
</thead>
</table>
| %URL%     | URL           | Website Blocked: Advanced Threat Protection notification  
Blocked URLs notification  
HTTPS Certificate Verification Failure notification  
Website Blocked: Patient-Zero notification  
Website Blocked: Scan Policy Block notification |
| %DOMAIN%  | Domain        | Website Blocked: Advanced Threat Protection notification  
Blocked URLs notification  
HTTPS Certificate Verification Failure notification  
Website Blocked: Patient-Zero notification  
Website Blocked: Scan Policy Block notification |
| %SERVER_IP% | Server IP     | Website Blocked: Advanced Threat Protection notification  
Blocked URLs notification  
HTTPS Certificate Verification Failure notification  
Website Blocked: Patient-Zero notification  
Website Blocked: Scan Policy Block notification |
| %POLICY_NAME% | Policy name   | Website Blocked: Advanced Threat Protection notification  
Website Blocked: Patient-Zero notification  
Website Blocked: Scan Policy Block notification |
<table>
<thead>
<tr>
<th><strong>TOKEN</strong></th>
<th><strong>FIELD NAME</strong></th>
<th><strong>NOTIFICATIONS WHERE TOKEN VALID</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%URL_CATEGORY%</code></td>
<td>URL Category</td>
<td>Website Blocked: Advanced Threat Protection notification&lt;br&gt;Website Blocked: Patient-Zero notification&lt;br&gt;Website Blocked: Scan Policy Block notification</td>
</tr>
<tr>
<td><code>%USER%</code></td>
<td>User</td>
<td>Website Blocked: Advanced Threat Protection notification&lt;br&gt;Blocked URLs notification&lt;br&gt;HTTPS Certificate Verification Failure notification&lt;br&gt;Website Blocked: Patient-Zero notification&lt;br&gt;Website Blocked: Scan Policy Block notification</td>
</tr>
<tr>
<td><code>%FILE_NAME%</code></td>
<td>File Name in HTTP Request or HTTP Response</td>
<td>Website Blocked: Advanced Threat Protection notification&lt;br&gt;HTTPS Certificate Verification Failure notification&lt;br&gt;Website Blocked: Patient-Zero notification&lt;br&gt;Website Blocked: Scan Policy Block notification</td>
</tr>
<tr>
<td><code>%MALWARE_NAME%</code></td>
<td>Malware name</td>
<td>Website Blocked: Advanced Threat Protection notification</td>
</tr>
<tr>
<td><code>%THREAT_TYPE%</code></td>
<td>Threat type</td>
<td>Website Blocked: Advanced Threat Protection notification</td>
</tr>
<tr>
<td><code>%RISK_LEVEL%</code></td>
<td>Risk level</td>
<td>Website Blocked: Advanced Threat Protection notification</td>
</tr>
<tr>
<td><code>%TECH_TYPE%</code></td>
<td>Detection type</td>
<td>Website Blocked: Advanced Threat Protection notification</td>
</tr>
<tr>
<td><code>%DETAIL%</code></td>
<td>Detail</td>
<td>HTTPS Certificate Verification Failure notification</td>
</tr>
</tbody>
</table>
Token | Field Name | Notifications Where Token Valid
--- | --- | ---
@HTTPS_POLICY_NAME% | HTTPS policy name | HTTPS Certificate Verification Failure notification

### Editing User Notifications

You can make changes to the messages used in the end-user notifications for security violations.

**Procedure**

1. Go to **Policy > User Defined Settings > Notifications**.
2. Click an available notification template.
   
   *List of User Notifications on page 7-22*

3. Specify changes to the notification, as required.
   
   You can use predefined tokens to customize the notification messages. You can also reset any of the notifications back to their predefined template.

   *Notification Message Tokens on page 7-23*

4. Click **Save**.
Chapter 8

Alerts and Reports

Topics include:

- Alerts on page 8-2
- Managing Triggered Alerts on page 8-2
- Configuring Alert Notifications on page 8-5
- Reports on page 8-20
- Scheduling Reports on page 8-20
- Generating On-Demand Reports on page 8-21
Alerts

Alerts provide immediate intelligence about the state of Deep Discovery Web Inspector. Alerts are classified into two categories:

• Critical alerts are triggered by events that require immediate attention.
• Important and informational alerts are triggered by events that require observation.

You can view or export information about triggered alerts.

Alert notifications are predefined and cannot be deleted; however, using alert notification rules you can make modifications to the predefined notifications to meet your needs. The rules define what the conditions are for triggering an alert as well as defining what content to include within the notification.

Managing Triggered Alerts

Perform any of the following tasks to manage alerts at Alerts / Reports > Alerts > Triggered Alerts.

Procedure

• View existing triggered alerts.
• Specify search filters to control the display and view of existing triggered alerts.
• Export up to 50,000 triggered alerts to a CSV file.
• Delete triggered alerts after review.

Related information

➥ Viewing Triggered Alerts

Viewing Triggered Alerts

Triggered alerts display existing critical, important, and informational alert notifications.
Procedure

1. Go to Alerts / Reports > Alerts > Triggered Alerts.

2. Specify the search criteria.
   - Level
   - Type
   - Rule name
   - Period

3. View alert details.

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered</td>
<td>The date and time when the alert occurred</td>
</tr>
<tr>
<td>Level</td>
<td>The importance of the alert: critical, important, or informational</td>
</tr>
<tr>
<td>Rule</td>
<td>The name of the alert rule that triggered the alert</td>
</tr>
<tr>
<td>Criteria</td>
<td>The alert rule criteria that triggered the alert</td>
</tr>
<tr>
<td>Detections</td>
<td>The number of watched detections that triggered the alert</td>
</tr>
<tr>
<td>Notification Recipients</td>
<td>The most recent alert notification recipients</td>
</tr>
<tr>
<td>Notification Subject</td>
<td>The most recent alert notification subject</td>
</tr>
</tbody>
</table>

Related information

- Critical Alerts
- Important and Informational Alerts

Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention.
Critical alerts are enabled by default.

**TABLE 8-1. Critical Alerts**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DEFAULT CRITERIA</th>
<th>DEFAULT ALERT FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security: Multiple Advanced Threats Detected in Specified Network Groups</td>
<td>10 or more advanced threats detected on hosts</td>
<td>Once every 5 minutes</td>
</tr>
<tr>
<td>Security: Multiple Ransomware Detected in Specified Network Groups</td>
<td>10 or more ransomware detections on hosts</td>
<td>Once every 5 minutes</td>
</tr>
<tr>
<td>Security: Multiple C&amp;C Callbacks Detected in Specified Network Groups</td>
<td>10 or more C&amp;C callbacks detected on hosts</td>
<td>Once every 5 minutes</td>
</tr>
<tr>
<td>Security: Multiple Coin Miners Detected in Specified Network Groups</td>
<td>10 or more coin miner detections on hosts</td>
<td>Once every 5 minutes</td>
</tr>
<tr>
<td>System: Service Stopped/Abnormal</td>
<td>Service % has stopped and cannot be restarted</td>
<td>Immediate</td>
</tr>
<tr>
<td>System: License Expiration</td>
<td>License is about to expire or has expired</td>
<td>Immediate</td>
</tr>
<tr>
<td>System: Network Is Down</td>
<td>Device %s's network is down</td>
<td>Immediate</td>
</tr>
</tbody>
</table>

**Important and Informational Alerts**

The following table explains the important and informational alerts triggered by events that require observation.

Important alerts are enabled by default. Informational alerts are disabled by default.

**TABLE 8-2. Important Alerts**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DEFAULT CRITERIA</th>
<th>DEFAULT ALERT FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>System: High CPU Usage</td>
<td>CPU usage is at least 90%</td>
<td>Once a day</td>
</tr>
</tbody>
</table>
### Configuring Alert Notifications

Each alert notification has a default configuration that is defined in alert notification rules. You can modify the parameters for each alert notification rule.

---

**Important**

You must configure an SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-18.*

---

**Procedure**

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

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

   The alert rule configuration screen appears.

3. Configure the alert parameters.
The list of message tokens that are valid for a specific notification is shown to the right of the message body.

4. Click **Save**.

5. Click **Back** to return to the **Rules** screen.

---

### Alert Notification Parameters

You can modify the parameters for each rule such as the notification message header and body, alert frequency, and other parameters. You can also enable or disable the notification.

The default recipient setting is to send the alert notifications to all contacts. If you want to send an alert notification to specific recipients, you must add recipients to the corresponding notification alert rule.

If using the default recipient setting and you want to configure the list of contacts, see *Managing Contacts on page 9-71*.

For some notifications, you can configure the parameter that triggers the alert notification and the network objects to which the rule applies.

---

### Critical Alert Parameters

You can customize alert notification parameters for the following critical alerts:

- Security: Multiple Advanced Threats Detected in Specified Network Groups
- Security: Multiple Ransomware Detected in Specified Network Groups
- Security: Multiple C&C Callbacks Detected in Specified Network Groups
- Security: Multiple Coin Miners Detected in Specified Network Groups
- System: Service Stopped/Abnormal
- System: License Expiration
- System: Network Is Down
Important

You must configure an SMTP server to send notifications. For details, see Configuring the Notification SMTP Server on page 9-18.

Security: Multiple Advanced Threats Detected in Specified Network Groups

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Detections</td>
<td>Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20</td>
</tr>
<tr>
<td></td>
<td>The default is 10.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td>Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day</td>
</tr>
<tr>
<td></td>
<td>The default is once every 5 minutes.</td>
</tr>
<tr>
<td>Network Object</td>
<td>Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks.</td>
</tr>
<tr>
<td></td>
<td>If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.</td>
</tr>
<tr>
<td>Exception</td>
<td>Select to include exceptions to the alert rule.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
### Parameter Description

**Message**
- Specifies the body of the triggered alert email message. You can customize this parameter.
- Use the following tokens to customize your message:
  - `%ConsoleURL%`
  - `%DateTime%`
  - `%DeviceName%`
  - `%DeviceIP%`
  - `%Threshold%`
  - `%ThreatCount%`

**Security: Multiple Ransomware Detected in Specified Network Groups**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Detections</td>
<td>Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20. The default is 10.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td>Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day. The default is once every 5 minutes.</td>
</tr>
<tr>
<td>Network Object</td>
<td>Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.</td>
</tr>
<tr>
<td>Exception</td>
<td>Select to include exceptions to the alert rule.</td>
</tr>
</tbody>
</table>
### Alerts and Reports

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select <strong>Send to all contacts</strong> to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
| Message     | Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:  
- %ConsoleURL%  
- %DateTime%  
- %DeviceName%  
- %DeviceIP%  
- %Threshold%  
- %ThreatCount%                                                                                       |

Security: Multiple C&C Callbacks Detected in a Specified Network Groups

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Detections</td>
<td>Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20. The default is 10.</td>
</tr>
</tbody>
</table>
| Alert frequency | Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria.  
Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day  
The default is once every 5 minutes.                                                                 |
<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Object</td>
<td>Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.</td>
</tr>
<tr>
<td>Exception</td>
<td>Select to include exceptions to the alert rule.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:</td>
</tr>
<tr>
<td></td>
<td>• %ConsoleURL%</td>
</tr>
<tr>
<td></td>
<td>• %DateTime%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceName%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceIP%</td>
</tr>
<tr>
<td></td>
<td>• %Threshold%</td>
</tr>
<tr>
<td></td>
<td>• %ThreatCount%</td>
</tr>
</tbody>
</table>

Security: Multiple Coin Miners Detected in Specified Network Groups

<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Detections</td>
<td>Specifies the detection threshold that will trigger the alert. You can customize this parameter. Valid detection options: 5, 10, or 20 The default is 10.</td>
</tr>
</tbody>
</table>
### Alerts and Reports

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert frequency</td>
<td>Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day. The default is once every 5 minutes.</td>
</tr>
<tr>
<td>Network Object</td>
<td>Select whether the alert rule applies to any network object or to the selected network objects. The default is to apply to all networks. If using selected network objects, select existing network objects or create new network objects to which the alert rule applies.</td>
</tr>
<tr>
<td>Exception</td>
<td>Select to include exceptions to the alert rule.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:</td>
</tr>
<tr>
<td></td>
<td>• %ConsoleURL%</td>
</tr>
<tr>
<td></td>
<td>• %DateTime%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceName%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceIP%</td>
</tr>
<tr>
<td></td>
<td>• %Threshold%</td>
</tr>
<tr>
<td></td>
<td>• %ThreatCount%</td>
</tr>
</tbody>
</table>

**System: Service Stopped/Abnormal**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td><strong>Note</strong>&lt;br&gt;You cannot configure alert frequency for this notification. The default is to send the notification immediately.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies the body of the triggered alert email message. You can customize this parameter.&lt;br&gt;Use the following tokens to customize your message:&lt;br&gt;• %ConsoleURL%&lt;br&gt;• %DateTime%&lt;br&gt;• %DeviceName%&lt;br&gt;• %DeviceIP%&lt;br&gt;• %ServiceName%</td>
</tr>
</tbody>
</table>

**System: License Expiration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td><strong>Note</strong>&lt;br&gt;You cannot configure alert frequency for this notification. The default is to send the notification immediately.</td>
</tr>
</tbody>
</table>
### Alerts and Reports

<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:</td>
</tr>
<tr>
<td></td>
<td>• %ConsoleURL%</td>
</tr>
<tr>
<td></td>
<td>• %DateTime%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceName%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceIP%</td>
</tr>
<tr>
<td></td>
<td>• %DaysBeforeExpiration%</td>
</tr>
<tr>
<td></td>
<td>• %ExpirationDate%</td>
</tr>
<tr>
<td></td>
<td>• %LicenseStatus%</td>
</tr>
<tr>
<td></td>
<td>• %LicenseType%</td>
</tr>
</tbody>
</table>

### System: Network Is Down

<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
</tbody>
</table>
| Alert frequency | **Note**  
You cannot configure alert frequency for this notification. The default is to send the notification immediately. |
| Recipients    | Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list. |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
| Message   | Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:  
- %ConsoleURL%  
- %DateTime%  
- %DeviceName%  
- %DeviceIP%  
- %PortName% |

### Important and Informational Alert Parameters

You can customize important and informational alert parameters.

You can customize the following informational alert:

- System: Component Update/Rollback Successful

You can customize the following important alerts:

- System: High CPU Usage
- System: Low Free Disk Space
- System: Component Update/Rollback Unsuccessful
- System: High Memory Usage
- System: Network Is Up

---

**Important**

You must configure an SMTP server to send notifications. For details, see *Configuring the Notification SMTP Server on page 9-18.*
### System: Component Update/Rollback Successful

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td><strong>Note</strong> You cannot configure alert frequency for this notification. The default is to send the notification immediately.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select <em>Send to all contacts</em> to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
| Message | Specifies the body of the triggered alert email message. You can customize this parameter.

Use the following tokens to customize your message:

- `%ConsoleURL%`
- `%DateTime%`
- `%DeviceName%`
- `%DeviceIP%`
- `%ComponentList%`

### System: High CPU Usage

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average CPU usage</td>
<td>Specifies the average CPU usage threshold that will trigger the alert. You can customize this parameter. The default is 90%.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td>Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once a day.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select <strong>Send to all contacts</strong> to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
| Message | Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:  
  - `%ConsoleURL%`  
  - `%DateTime%`  
  - `%DeviceName%`  
  - `%DeviceIP%`  
  - `%CPUUsage%`  
  - `%CPUThreshold%` |

**System: Low Free Disk Space**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
</tbody>
</table>
## Alerts and Reports

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free disk space</td>
<td>The lowest disk space threshold in GB that triggers the alert. You can customize this parameter. The default is 20 GB.</td>
</tr>
<tr>
<td>Alert frequency</td>
<td>Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria. Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day The default is once every hour.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
</tbody>
</table>
| Message         | Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:  
  - %ConsoleURL%
  - %DateTime%
  - %DeviceName%
  - %DeviceIP%
  - %DiskSpace% |

### System: Component Update/Rollback Unsuccessful

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
</tbody>
</table>
### Alert frequency

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot configure alert frequency for this notification. The default is to send the notification immediately.</td>
<td></td>
</tr>
</tbody>
</table>

### Recipients

Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list.

### Subject

Specifies the subject of the triggered alert email message. You can customize this parameter.

### Message

Specifies the body of the triggered alert email message. You can customize this parameter.

Use the following tokens to customize your message:

- `%ConsoleURL%`
- `%DateTime%`
- `%DeviceName%`
- `%DeviceIP%`
- `%ComponentList%`

### System: High Memory Usage

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
<tr>
<td>Average memory usage</td>
<td>Specifies the memory usage threshold that will trigger the alert. You can customize this parameter. The default is 90%.</td>
</tr>
</tbody>
</table>
### Alerts and Reports

<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Alert frequency | Select the time interval that Deep Discovery Web Inspector checks for the alert rule criteria.  
Valid alert frequency options: Immediate, Once every 5 minutes, Once every 30 minutes, Once every hour, Once a day  
The default is once a day. |
| Recipients | Specify the recipients who will receive the triggered alert email message or select Send to all contacts to send the alert to all recipients in the contact list. |
| Subject | Specifies the subject of the triggered alert email message. You can customize this parameter. |
| Message | Specifies the body of the triggered alert email message. You can customize this parameter.  
Use the following tokens to customize your message:  
• %ConsoleURL%  
• %DateTime%  
• %DeviceName%  
• %DeviceIP%  
• %MemoryUsage%  
• %MemoryThreshold% |

**System: Network Is Up**

<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Select an option to enable or disable the alert.</td>
</tr>
<tr>
<td>Alert level</td>
<td>Displays the alert level in email messages.</td>
</tr>
</tbody>
</table>
| Alert frequency | **Note**  
You cannot configure alert frequency for this notification. The default is to send the notification immediately.|
<table>
<thead>
<tr>
<th><strong>PARAMETER</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients</td>
<td>Specify the recipients who will receive the triggered alert email message or select <strong>Send to all contacts</strong> to send the alert to all recipients in the contact list.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject of the triggered alert email message. You can customize this parameter.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies the body of the triggered alert email message. You can customize this parameter. Use the following tokens to customize your message:</td>
</tr>
<tr>
<td></td>
<td>• %ConsoleURL%</td>
</tr>
<tr>
<td></td>
<td>• %DateTime%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceName%</td>
</tr>
<tr>
<td></td>
<td>• %DeviceIP%</td>
</tr>
<tr>
<td></td>
<td>• %PortName%</td>
</tr>
</tbody>
</table>

**Reports**

Deep Discovery Web Inspector provides reports to assist in mitigating threats and optimizing system settings. Generate reports on demand or set a daily, weekly, or monthly schedule. Deep Discovery Web Inspector offers flexibility in specifying the content for each report.

The reports generate in PDF format.

**Scheduling Reports**

Scheduled reports automatically generate according to the configured schedules.

---

**Procedure**

1. Go to Alerts / Reports > Reports > Schedules.
2. Enable scheduled reports by selecting one or more of the associated intervals.
   - Generate daily report
   - Generate weekly report
   - Generate monthly report

3. Specify when to generate each of the selected reports.

   When a monthly report schedule is set to generate reports on the 29th, 30th, or 31st day, the report generates on the last day of the month for months with fewer days.

   For example, if you select 31, the report generates on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Specify the recipients for each selected report.

   You can choose to send each specified report to all contacts (the default) or specify a list of recipients who should receive the report. If specifying recipients, separate multiple recipients with a semicolon.

   If using the default option and you want to configure the list of contacts, see Managing Contacts on page 9-71.

   **Important**
   You must configure the SMTP server to send notifications. For details, see Configuring the Notification SMTP Server on page 9-18.

5. Click Save.

---

### Generating On-Demand Reports

You can generate on-demand reports at any time.

**Procedure**

1. Go to Alerts / Reports > Reports > On Demand.
2. Configure report settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Select the scope and start time or end time for report generation.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Specify the recipients. Separate multiple recipients with a semicolon.</td>
</tr>
</tbody>
</table>

**Important**
You must configure the SMTP server to send notifications. For details, see Configuring the Notification SMTP Server on page 9-18.

3. Click **Generate**.

The report generates and the following actions occur:

- The report appears at Alerts / Reports > Reports > Generated Reports.
- Report notifications are sent to specified recipients.
Chapter 9

Administration

Topics include:

- Deployment Wizard on page 9-2
- Component Updates on page 9-7
- Product Updates on page 9-11
- System Settings on page 9-14
- Integrated Products/Services on page 9-25
- Virtual Analyzer on page 9-39
- System Maintenance on page 9-50
- Accounts / Contacts on page 9-67
- License on page 9-72
- About Deep Discovery Web Inspector on page 9-72
Deployment Wizard

Topics include:

- Accessing the Deployment Wizard on page 9-2
- Configuring Transparent Bridge Mode on page 9-5
- Configuring Forward Proxy Mode on page 9-2

Accessing the Deployment Wizard

If you want to change basic configuration parameters after the initial deployment is complete, you can access the Deployment Wizard at any time and make any desired changes.

When you open the Deployment Wizard, the wizard will display the last saved parameters. To save changes, you must proceed through the entire wizard just as you did for the initial configuration and click Finish.

- Configuring Transparent Bridge Mode on page 9-5
- Configuring Forward Proxy Mode on page 9-2

Configuring Forward Proxy Mode

You can open the Deployment Wizard screen after the appliance is configured and modify deployment mode settings.

Note

You can exit the Deployment Wizard at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

If you are performing the initial deployment, see Deployment on page 3-1.
Procedure

1. Go to Administration > Deployment Wizard.
   The Welcome page opens.
2. In the Deployment Mode section, select Forward proxy.
3. Click Next.
4. In the Working Mode Settings page, specify the following details.

<table>
<thead>
<tr>
<th>HTTP listening port</th>
<th>Specify the port that the proxy server uses to listen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable upstream proxy</td>
<td>Select this option if the network uses an upstream proxy server and specify the IPv4 address and port number in Proxy server and Port number.</td>
</tr>
</tbody>
</table>

5. Click Next.
6. In the Network page, specify the following details:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify a host name.</td>
</tr>
<tr>
<td>Primary DNS server</td>
<td>Specify the IP address of the DNS server. This is a required setting.</td>
</tr>
<tr>
<td>Secondary DNS server</td>
<td>Optionally, specify the IP address for a secondary DNS server.</td>
</tr>
<tr>
<td>Data interface</td>
<td>This is a read-only field and is pre-set to eth0. This interface is also used for management.</td>
</tr>
<tr>
<td>Mode</td>
<td>This is a read-only field and is pre-set to static.</td>
</tr>
</tbody>
</table>
### Option Description

**IPv4 address, IPv4 netmask, and Default IPv4 gateway**

Specify the IPv4 network settings.

---

**Note**

After you click **Finish**, a dialog box opens asking if you want to reboot the appliance. After you click **OK**, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the Log On page is displayed.

---

7. Click **Next**.

The **Time** page opens.

8. In the **Time** section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server</td>
<td>Enter the NTP server IP address.</td>
</tr>
</tbody>
</table>
| **System time zone** | Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance.  
  Optionally, instead of selecting a location, you can select **Etc** and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance. |

9. Click **Next**.

The **Summary** page opens.

10. Review and verify the settings and then perform the appropriate action:

    a. If the settings are not as desired, click on **Prev** and modify settings as required.

    b. If the settings are verified, click on **Finish** to save the configuration.
Important

If you exit the wizard before saving settings, the configuration is not saved.

Related information

➥ Network Deployment Mode Overview

Configuring Transparent Bridge Mode

You can open the Deployment Wizard screen after the appliance is configured and modify deployment mode settings.

Note

You can exit the Deployment Wizard at any time by clicking on another menu item in the management console. If you exit the wizard before finishing the configuration process, all data entered will be lost.

If you are performing the initial deployment, see Deployment on page 3-1.

Procedure

1. Go to Administration > Deployment Wizard.
   The Welcome page opens.

2. In the Deployment Mode section, select Transparent bridge.

3. Click Next.

4. In the Network page, specify the following details:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify a host name.</td>
</tr>
<tr>
<td>Primary DNS server</td>
<td>Specify the IP address of the DNS server. This is a required setting.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secondary DNS server</td>
<td>Optionally, specify the IP address for a secondary DNS server.</td>
</tr>
<tr>
<td>Data egress interface</td>
<td>This is a read-only field and is pre-set to eth5.</td>
</tr>
<tr>
<td>Data ingress interface</td>
<td>This is a read-only field and is pre-set to eth4.</td>
</tr>
<tr>
<td>Management interface</td>
<td>This is a read-only field and is pre-set to eth0.</td>
</tr>
<tr>
<td>Mode</td>
<td>This is a read-only field and is pre-set to static.</td>
</tr>
<tr>
<td>IPv4 address, IPv4 netmask, and Default IPv4 gateway</td>
<td>Specify the IPv4 network settings.</td>
</tr>
</tbody>
</table>

Note
After you click Finish, a dialog box opens asking if you want to reboot the appliance. After you click OK, the connection to the appliance disconnects and the appliance reboots. After the appliance restarts, the Log On page is displayed.

5. Click Next.

The Time page opens.

6. In the Time section, configure the time and location settings for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server</td>
<td>Enter the NTP server IP address.</td>
</tr>
<tr>
<td>System time zone</td>
<td>Set the appropriate time zone by selecting the location closest to the Deep Discovery Web Inspector appliance. Optionally, instead of selecting a location, you can select Etc and then choose the offset that matches the location closest to the Deep Discovery Web Inspector appliance.</td>
</tr>
</tbody>
</table>
7. Click Next.
   
The Summary page opens.

8. Review and verify the settings and then perform the appropriate action:
   a. If the settings are not as desired, click on Prev and modify settings as required.
   b. If the settings are verified, click on Finish to save the configuration.

---

**Important**
If you exit the wizard before saving settings, the configuration is not saved.

---

**Related information**

- [Network Deployment Mode Overview](#)
- [Bridge Mode Not Supported When Deployed in LACP/EtherChannel Links](#)

---

**Component Updates**

Download and deploy product components used to investigate threats. Because Trend Micro frequently creates new component versions, perform regular updates to address the latest ransomware and malware attacks.

- [Components on page 9-7](#)
- [Updating Components on page 9-9](#)
- [Rolling Back Components on page 9-10](#)
- [Scheduling Component Updates on page 9-10](#)

---

**Components**

The Components tab at Administration > Component Updates shows the security components currently in use.
### TABLE 9-1. Components

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Threat Scan Engine for Deep Discovery (64-bit)</td>
<td>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.</td>
</tr>
<tr>
<td>Bot Pattern</td>
<td>The Bot Pattern is used by the Network Content Inspection Engine to perform bot network scanning.</td>
</tr>
<tr>
<td>Deep Discovery Malware Pattern</td>
<td>The Deep Discovery Malware Pattern contains the detection routines for virus and malware scanning. Trend Micro updates the Deep Discovery Malware Pattern regularly with detection routines for new identified threats.</td>
</tr>
<tr>
<td>Deep Discovery Trusted Certificate Authorities</td>
<td>Deep Discovery Trusted Certificate Authorities provides the trusted certificate authorities to verify PE signatures.</td>
</tr>
<tr>
<td>IntelliTrap Exception Pattern</td>
<td>The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning.</td>
</tr>
<tr>
<td>IntelliTrap Pattern</td>
<td>The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats.</td>
</tr>
<tr>
<td>Network Content Correlation Pattern</td>
<td>The Network Content Correlation Pattern implements detection rules defined by Trend Micro.</td>
</tr>
<tr>
<td>Network Content Inspection Engine (Linux, User mode, 64-bit)</td>
<td>The Network Content Inspection Engine is used to perform network scanning.</td>
</tr>
<tr>
<td>Network Content Inspection Pattern</td>
<td>The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning.</td>
</tr>
<tr>
<td>Predictive Machine Learning Pattern</td>
<td>The Predictive Machine Learning Pattern is used by Predictive Machine Learning to help classify malware.</td>
</tr>
</tbody>
</table>
### Updating Components

Update components to immediately download the component updates from the update source server.

**Procedure**

1. Go to Administration > Component Updates > Components.
2. Select one or more components.
3. Click Update.
“Updating” displays while the update is in progress. And after the update finishes, “Update succeeded” displays.

Rolling Back Components

Roll back components to revert all components to the most recent version.

Procedure

1. Go to Administration > Component Updates > Components.
2. Select one or more components.
3. Click Roll Back.
   “Rolling back” displays while the rollback is in progress. And after the rollback finishes, the message changes to say that rollback was successful.
   The components revert to the most recent version.

Scheduling Component Updates

Procedure

1. Go to Administration > Component Updates > Schedule.
   The Schedule tab appears.
2. Enable the scheduled update.
3. Select the update interval.
4. Click Save.
Product Updates

Use the **Product Updates** screen to apply hotfixes and patches, or perform a firmware upgrade to Deep Discovery Web Inspector.

Hotfixes and Patches Overview

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

**TABLE 9-2. Hotfixes and Patches**

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

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

[http://downloadcenter.trendmicro.com](http://downloadcenter.trendmicro.com)
Managing Patches

From time to time, Trend Micro releases a patch for a reported known issue or an upgrade that applies to the product. Find available patches at http://downloadcenter.trendmicro.com.

Use the following method to install a patch file on Trend Micro:

**Procedure**

1. Go to Administration > Product Updates > Hotfixes / Patches.
2. Under History, verify the firmware version number.
3. Manage the product patch.
   - Upload a patch by browsing to the patch file provided by Trend Micro Support and then clicking Install under Install Hotfix / Patch.
   - Roll back a patch by clicking Roll Back under History.

   After rollback, Deep Discovery Web Inspector uses the most recent previous configuration. For example, rolling back patch 3 returns Deep Discovery Web Inspector to a patch 2 state.

Upgrading Firmware

From time to time, Trend Micro releases a firmware upgrade that applies to the product. Find available firmware upgrades at http://downloadcenter.trendmicro.com.

Updating the firmware ensures that Deep Discovery Web Inspector has access to new and improved security features when they become available.

Upgrade the firmware on Deep Discovery Web Inspector using the following method:
Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete. Trend Micro recommends starting the upgrade during off-peak office hours. Installing the update restarts Deep Discovery Web Inspector.

Procedure

1. Obtain the firmware image.
   • Download the Deep Discovery Web Inspector firmware package from the Trend Micro Download Center at:

   http://downloadcenter.trendmicro.com
   • Obtain the firmware package from your Trend Micro reseller or support provider.

2. Save the package to any folder on a local computer.

3. Go to Administration > Product Updates > Firmware.

4. Next to Firmware version, verify your firmware version.

5. Browse for the firmware update package.

6. Click Install.

Tip
You can access the command line interface to view the installation process.

After the installation has completed, Deep Discovery Web Inspector automatically restarts and the web console log on page appears.

7. Perform the following post-installation steps:
   • Clear the browser cache.
   • Manually log on to the web console.
If Deep Discovery Web Inspector is using an internal Virtual Analyzer that connects to the Internet through a proxy server, reconfigure the proxy settings for the internal Virtual Analyzer.

System Settings

Topics include:

- Configuring Network Settings on page 9-14
- Managing Static Routes on page 9-15
- Configuring Proxy Settings on page 9-17
- Configuring the Notification SMTP Server on page 9-18
- Configuring System Time on page 9-19

Configuring Network Settings

You can use the management console to make changes to the network interface settings after the initial deployment.

You can configure the host name, the IPv4 addresses of the Deep Discovery Web Inspector appliance, and other network settings.

Procedure

1. Go to Administration > System Settings > Network.

2. Specify the general network settings that affect all interfaces.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify the host name.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specify the IPv4 address of the gateway.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary DNS server and Secondary DNS server</td>
<td>Specify the IPv4 addresses of the primary DNS server and optionally, the secondary DNS server.</td>
</tr>
</tbody>
</table>

3. Specify the IPv4 address and subnet mask for the eth0 port:

The eth0 interface is known as the **Data interface** for the forward proxy deployment mode and the **Management interface** for the transparent bridge deployment mode. The eth0 interface handles management console traffic, SSH connections, Trend Micro updates, and other related Trend Micro traffic.

In transparent bridge mode, eth4 and eth5 are designated as **eth4 - Data Ingress Port** and **eth5 - Data Egress Port**. You cannot assign IP addresses to these ports in transparent bridge mode.

4. Specify the IPv4 address and subnet mask for the eth1 port if you plan on using a custom network for Virtual Analyzer sandbox instances to connect to the Internet.

The eth1 interface is known as the dirty line port for Virtual Analyzer custom network connections. If **Custom network** is selected when configuring Virtual Analyzer network connections, Virtual Analyzer connects to the Internet using eth1, which is isolated from the management network.

5. Specify the IPv4 address and subnet mask for other Ethernet interface ports that you will use in your deployment.

The available ports will vary depending on the deployment mode and your particular deployment.

6. Click **Save**.

When you save network changes, network services are restarted. After the restart, you must log on to the console again.

---

**Managing Static Routes**

Perform any of the following tasks to manage static routes at **Administration > System Settings > Static Routes**.
Procedure

- Specify search filters to control the display and view of existing static routes.
- Add, deploy (to enable), or delete static routes.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a new static route.</td>
</tr>
<tr>
<td></td>
<td><em>Adding a Static Route on page 9-16</em></td>
</tr>
<tr>
<td>Deploy</td>
<td>Deploy (enable) static routes by selecting one or more static routes from the list and clicking Deploy.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete static routes by selecting one or more static routes from the list and clicking Delete.</td>
</tr>
</tbody>
</table>

**Adding a Static Route**

When new static routes are added, Deep Discovery Web Inspector checks whether a matching route and destination already exist in the Deep Discovery Web Inspector routing table. If no match is found, Deep Discovery Web Inspector adds the route to the routing table.

You can configure IPv4 static routes.

**Procedure**

1. Go to Administration > System Settings > Static Routes.
2. Click Add.
   
   The Add Static Route window appears.
3. In Network ID, specify the network address.
4. In IPv4 netmask, enter the netmask for the network ID.
5. In Router, specify the IP address for the next hop router.
6. In **Interface**, specify the interface used to reach the next hop router.

7. Click **Save**.

---

**Configuring Proxy Settings**

Configuring proxy settings affects:

- Certified Safe Software Service
- Community File Reputation
- Component updates (pattern files and scan engines)
- Product license registration
- Script Analyzer Engine
- Web Reputation queries
- Web Inspection Service
- Predictive Machine Learning

---

**Procedure**

1. Go to **Administration > System Settings > Proxy**.

   The **Proxy** screen appears.

2. Specify the proxy server settings.

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a proxy server for Trend Micro services</td>
<td>Select to use a proxy server.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>Specify the proxy server host name or IP address.</td>
</tr>
</tbody>
</table>
Port | Specify the port that the proxy server uses to connect to the Internet.
---|---
Proxy server requires authentication | Select if your proxy server requires authentication and then specify User ID and Password.

3. Click Save.

Configuring the Notification SMTP Server

Deep Discovery Web Inspector uses the SMTP server to send alert notifications and reports to configured recipients.

Procedure

1. Go to Administration > System Settings > SMTP.
2. Specify the SMTP server settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender email address</td>
<td>This is the email address used to send notifications and reports.</td>
</tr>
<tr>
<td>Server address</td>
<td>Type the external SMTP server host name (FQDN) or IPv4 address.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the external SMTP server port number.</td>
</tr>
<tr>
<td>Connection security</td>
<td>Select a security protocol if required for the connection. Options are StartTLS or SSL/TLS.</td>
</tr>
</tbody>
</table>
**Option** | **Description**
---|---
**SMTP server requires authentication** | Select this option if the connection to the SMTP server requires authentication and then configure the user name and password.  

**Note**
Make sure that you configure the user name and password correctly. An external SMTP server may refuse connection from Deep Discovery Web Inspector after the maximum number of unsuccessful authentication attempts has been reached.

3. Click **Save**.

### Configuring System Time

Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system date and time and time zone.

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet.

**Procedure**

1. **Go to Administration > System Settings > Time.**

2. Set the system time.

   - To synchronize with an NTP server, select **Synchronize appliance time with an NTP server** and then specify the domain name or IP address of the NTP server.

   - To manually set the system time, select **Set time manually** and then select the date and time and select the time zone.
3. Click Save.

---

**Configuring SNMP**

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

On Deep Discovery Web Inspector, 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 9-20*.

- Configure the appliance to listen for manager requests
  
  For details, see *Configuring Manager Requests on page 9-22*.

**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.
<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager server address</td>
<td>Specify the manager server address. You can specify as an IP address or a FQDN.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Select the SNMP version:</td>
</tr>
<tr>
<td></td>
<td>• SNMPv1/SNMPv2c</td>
</tr>
<tr>
<td></td>
<td>• SNMPv3</td>
</tr>
<tr>
<td>Community name</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This field is only available for SNMPv1/SNMPv2c.</td>
</tr>
<tr>
<td></td>
<td>Type a community name that is less than 255 characters and does not contain</td>
</tr>
<tr>
<td></td>
<td>double-byte encoded characters, spaces, or the following characters: [] '/ &quot;</td>
</tr>
<tr>
<td></td>
<td>{ } &lt; &gt;</td>
</tr>
<tr>
<td>Security model</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This field is only available for SNMPv3.</td>
</tr>
<tr>
<td></td>
<td>Select the security model:</td>
</tr>
<tr>
<td></td>
<td>• No authentication or privacy</td>
</tr>
<tr>
<td></td>
<td>• Authenticated</td>
</tr>
<tr>
<td></td>
<td>• Authenticated with privacy</td>
</tr>
<tr>
<td>User name</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This field is only available for SNMPv3 (all security models).</td>
</tr>
<tr>
<td></td>
<td>Specify the user name.</td>
</tr>
<tr>
<td></td>
<td>A valid user name is less than 255 characters and and does not contain</td>
</tr>
<tr>
<td></td>
<td>double-byte encoded characters, spaces, or the following characters: [] '/ &quot;</td>
</tr>
<tr>
<td></td>
<td>{ } &lt; &gt;</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td><strong>Note</strong>&lt;br&gt; This field is only available for SNMPv3 using <strong>Authenticated</strong> or <strong>Authenticated with privacy security model</strong>.</td>
</tr>
<tr>
<td></td>
<td>Specify the password.&lt;br&gt;A valid password is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / &quot; { } &lt; &gt;</td>
</tr>
<tr>
<td>Privacy passphrase</td>
<td><strong>Note</strong>&lt;br&gt; This field is only available for SNMPv3 using the <strong>Authenticated with privacy security model</strong>.</td>
</tr>
<tr>
<td></td>
<td>Specify the privacy passphrase.&lt;br&gt;A valid passphrase is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / &quot; { } &lt; &gt;</td>
</tr>
</tbody>
</table>

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 Web Inspector 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 Web Inspector 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.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device location</td>
<td>Specify the location of this appliance.</td>
</tr>
<tr>
<td></td>
<td>A valid device location is less than 255 characters and does not contain the following characters: [] ' / {} &lt;&gt;</td>
</tr>
<tr>
<td>Administrator contact</td>
<td>Specify the administrator contact of this appliance.</td>
</tr>
<tr>
<td></td>
<td>A valid administrator contact is less than 255 characters and does not contain the following characters: [] ' / {} &lt;&gt;</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Select the SNMP version:</td>
</tr>
<tr>
<td></td>
<td>• SNMPv1/SNMPv2c</td>
</tr>
<tr>
<td></td>
<td>• SNMPv3</td>
</tr>
<tr>
<td>Allowed community names</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This field is only available for SNMPv1/SNMPv2c.</td>
</tr>
<tr>
<td></td>
<td>Specify a maximum of 5 community names.</td>
</tr>
<tr>
<td></td>
<td>A valid allowed community name is less than 255 characters and does not contain double-byte encoded characters, spaces, or the following characters: [] ' / {} &lt;&gt;</td>
</tr>
<tr>
<td>Trusted manager server addresses</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This field is only available for SNMPv1/SNMPv2c.</td>
</tr>
<tr>
<td></td>
<td>Specify a maximum of 5 trusted manager server addresses.</td>
</tr>
<tr>
<td><strong>OPTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security model</td>
<td><strong>Note</strong>&lt;br&gt;This field is only available for SNMPv3.&lt;br&gt;&lt;br&gt;Select the security model:&lt;br&gt;• No authentication or privacy&lt;br&gt;• Authenticated&lt;br&gt;• Authenticated with privacy</td>
</tr>
<tr>
<td>User name</td>
<td><strong>Note</strong>&lt;br&gt;This field is only available for SNMPv3 (all security models).&lt;br&gt;&lt;br&gt;Specify the user name.&lt;br&gt;A valid manager requests user name is less than 255 characters and does not contain double-byte encoded characters, spaces, or the following characters: [ ] ' / &quot; { } &lt; &gt;</td>
</tr>
<tr>
<td>Password</td>
<td><strong>Note</strong>&lt;br&gt;This field is only available for SNMPv3 using Authenticated or Authenticated with privacy security model.&lt;br&gt;&lt;br&gt;Specify the password.&lt;br&gt;A valid manager requests password is more than 8 and less than 255 characters and does not contain spaces or the following characters: [ ] ' / &quot; { } &lt; &gt;</td>
</tr>
</tbody>
</table>
Privacy passphrase

**Note**
This field is only available for SNMPv3 using the Authenticated with privacy security model.

Specify the privacy passphrase.
A valid manager requests passphrase is more than 8 and less than 255 characters and does not contain spaces or the following characters: []'/" {} < > | & ! ( )

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 Web Inspector supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

## Integrated Products/Services

Deep Discovery Web Inspector integrates with the following products and services:

- **Control Manager on page 9-25**
- **Threat Intelligence Sharing on page 9-28**
- **Log Settings on page 9-29**

## Control Manager

Trend Micro Control Manager is a software management solution that gives you the ability to control antivirus and content security programs from a central location,
regardless of the program’s physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

In a network topology containing multiple Deep Discovery Web Inspector appliances, Control Manager can aggregate suspicious objects data.

Deep Discovery Web Inspector supports synchronizing two types of suspicious objects from Control Manager: Virtual Analyzer suspicious objects and user-defined suspicious objects. Deep Discovery Web Inspector can block the traffic if a match is found in the synchronized high-risk suspicious objects list.

For more information about Control Manager, see the Trend Micro Control Manager Administrator’s Guide.

Managing Control Manager Tasks

On Deep Discovery Web Inspector, use the Administration > Integrated Products/Services > Control Manager tab to perform the following tasks:

Procedure

• Register to a Control Manager server.

  Registering to Control Manager on page 9-27

• Check the connection status between Deep Discovery Web Inspector and Control Manager.

• Synchronize suspicious objects with Control Manager.

• Unregister from a Control Manager server.

  Unregistering from Control Manager on page 9-28

• Ensure that both Deep Discovery Web Inspector and the Control Manager server belong to the same network segment.
Registering to Control Manager

Before you can synchronize suspicious objects with Control Manager, you must register the Deep Discovery Web Inspector appliance to Control Manager.

Procedure

1. Go to Administration > Integrated Products/Services > Control Manager.
2. Under General, view the registration status.
3. Configure Server Settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server address</td>
<td>Type the Control Manager server FQDN or IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port that Deep Discovery Web Inspector uses to communicate with Control Manager via the web service.</td>
</tr>
</tbody>
</table>
4. (Optional) Under Suspicious Object Synchronization, do the following:
   a. Select Synchronize suspicious objects from Control Manager.
   b. Type the API Key.

**Note**

Log on to Control Manager to obtain an API key.

Deep Discovery Web Inspector synchronizes suspicious object lists from Control Manager every 20 seconds, and displays the time of the last synchronization.

5. Click Save.

Deep Discovery Web Inspector registers to Control Manager.
Unregistering from Control Manager

You can unregister Deep Discovery Web Inspector from Control Manager. After unregistering, Deep Discovery Web Inspector can register to another Control Manager.

**Procedure**

1. Go to Administration > Integrated Products/Services > Control Manager.
2. Under General, click the Unregister button.

Deep Discovery Web Inspector unregisters from Control Manager.

Threat Intelligence Sharing

Deep Discovery Web Inspector can share threat intelligence data (such as suspicious URLs) with other products or services (for example, a Blue Coat ProxySG device) through the HTTPS web service.

**Note**

When Deep Discovery Web Inspector is registered to Control Manager, Deep Discovery Web Inspector does not include user-defined suspicious objects synchronized from Control Manager in the shared threat intelligence data.

Configuring Threat Intelligence Sharing Settings

**Procedure**

1. On the Deep Discovery Web Inspector management console, go to Administration > Integrated Products/Services > Threat Intelligence Sharing.
2. Select Enable Threat Intelligence Sharing to allow integrated products/services to get information from Deep Discovery Web Inspector.
3. (Optional) Under Schedule Settings, select Enabled for Scheduled file generation and configure the schedule settings.
4. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.

   Options include High only, High and medium, and High, medium, and low.

5. Click **Save**.

6. Under **General**, click **Generate Now**.

   After the file generation is successfully, you can click the URL to download the threat intelligence data file to view the content.

7. Configure an integrated product/service (for example, a Blue Coat ProxySG device) to obtain threat intelligence data from Deep Discovery Web Inspector. For more information, see the documentation for the integrated product/service.

---

**Log Settings**

Deep Discovery Web Inspector maintains access and violation detection logs that can be sent to syslog servers.

**Detection Syslog Server Profiles**

Deep Discovery Web Inspector can send violation detection logs to up to three syslog servers after saving the logs to its database. You can add up to three detection syslog server profiles.

Only logs saved after enabling a syslog server will be sent to that server. Previous logs are excluded.

**The Default Access Syslog Server Profile**

Deep Discovery Web Inspector can send access logs to up to one syslog server. There is a default access syslog server profile that is built-in and is preconfigured with certain settings. It is disabled by default. You can use this profile to start sending access logs to a syslog server.

To send the access logs, you must configure the syslog server IP address and port and then enable the profile. Additionally, you can customize which access log entries are sent to the syslog server.
After access logs are sent to the syslog server, Deep Discovery Web Inspector deletes the original data.

**Adding a Detection Syslog Server Profile**

You can configure Deep Discovery Web Inspector to forward the appliance's violation detection logs to a syslog server.

**Procedure**

1. Go to *Administration > Integrated Products/Services > Log Settings.*
   
   The *Log Settings* screen appears.

2. Click *Add Detection Syslog.*
   
   The *Add Syslog Server Profile* screen appears.

3. (Optional) Enable or disable the detection syslog server profile.
   
   A new profile is enabled by default.

4. Type a profile name.

5. Type the host name (FQDN) or IP address of the syslog server.

6. Type the port number.

7. Select the protocol to be used when transporting log content to the syslog server.
   
   - TCP
   - UDP
   - SSL

8. Select the format in which event logs should be 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.

• **TMEF (Trend Micro Event Format)**: 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.

9. Click **Save**.

---

**Editing Detection Syslog Server Profiles**

**Procedure**

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

   The **Log Settings** screen appears.

2. Click a detection syslog server profile hyperlink.

   The **Edit Detection Syslog Server Profile** screen appears.

3. Make the required changes.

4. Click **Save**.

---

**Modifying the Access Syslog Server Profile**

**Procedure**

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

   The **Log Settings** screen appears.

2. Click the default access syslog server profile hyperlink.

   The **Edit Access Syslog Server Profile** screen appears.
3. Make the required changes.

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Enable or disable the access syslog server profile.</td>
</tr>
<tr>
<td>Profile name</td>
<td>Change the profile name.</td>
</tr>
<tr>
<td>Server address</td>
<td>Change the server address. If you change the address on the syslog server, you</td>
</tr>
<tr>
<td></td>
<td>must enter the new server address in this field.</td>
</tr>
<tr>
<td>Port</td>
<td>Change the port. If you change the port on the syslog server, you must</td>
</tr>
<tr>
<td></td>
<td>enter the new port in this field.</td>
</tr>
<tr>
<td>Protocol</td>
<td>A read-only field that is set to UDP.</td>
</tr>
<tr>
<td>Content format</td>
<td>You can specify that Deep Discovery Web Inspector send only certain access log</td>
</tr>
<tr>
<td></td>
<td>content to the access syslog server. Use this field, to specify what log</td>
</tr>
<tr>
<td></td>
<td>information that you want Deep Discovery Web Inspector to send.</td>
</tr>
<tr>
<td></td>
<td>For information about content format parameters that you can specify, see</td>
</tr>
<tr>
<td></td>
<td><strong>Access Syslog Server Profile - Content Format Parameters on page 9-32.</strong></td>
</tr>
</tbody>
</table>

Use the format shown in the following example when specifying parameters in the **Content format** field. Separate each entry with | (pipe):

```
{dst} | {src} | {upstream_size} | {downstream_size} | {policy_name} | {request} | {cat} | {act} | {user-agent} | {local_addr}
```

4. Click **Save**.

### Access Syslog Server Profile - Content Format Parameters

You can modify the **Content format** field in the **Access Syslog Server Profile** to customize which entries in the access logs are sent to the syslog server. Use the following configuration parameters when modifying this field.
**Note**

Configuration parameters that have the format \{text\}h represent keys that are HTTP headers, which are below the URL. HTTP headers are used by clients and servers to pass additional information with requests and responses.

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Configuration Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recv_request_begin</td>
<td>{recv_request_begin}</td>
<td>The time (UTC) that the first package in the request was received.</td>
</tr>
<tr>
<td>recv_request_end</td>
<td>{recv_request_end}</td>
<td>The time (UTC) that the last package in the request was received.</td>
</tr>
<tr>
<td>send_request_begin</td>
<td>{send_request_begin}</td>
<td>The time (UTC) that the first package in the request was sent.</td>
</tr>
<tr>
<td>send_request_end</td>
<td>{send_request_end}</td>
<td>The time (UTC) that all packages in the request were sent.</td>
</tr>
<tr>
<td>recv_response_begin</td>
<td>{recv_response_begin}</td>
<td>The time (UTC) that the first package in the response was received.</td>
</tr>
<tr>
<td>recv_response_end</td>
<td>{recv_response_end}</td>
<td>The time (UTC) that all packages in the response were received.</td>
</tr>
<tr>
<td>send_response_begin</td>
<td>{send_response_begin}</td>
<td>The time (UTC) that the first package in the response was sent.</td>
</tr>
<tr>
<td>send_response_end</td>
<td>{send_response_end}</td>
<td>The time (UTC) that all packages in the response were sent.</td>
</tr>
<tr>
<td>handle_time</td>
<td>{handle_time}</td>
<td>The time (milliseconds) it took for Deep Discovery Web Inspector to handle one transaction.</td>
</tr>
<tr>
<td><strong>Key Name</strong></td>
<td><strong>Configuration Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>request_handle_time</td>
<td>{request_handle_time}</td>
<td>The time (milliseconds) it took for Deep Discovery Web Inspector to handle the request for one transaction.</td>
</tr>
<tr>
<td>response_handle_time</td>
<td>{response_handle_time}</td>
<td>The time (milliseconds) it took for Deep Discovery Web Inspector to handle the response for one transaction.</td>
</tr>
<tr>
<td>refer</td>
<td>{referer}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>location</td>
<td>{location}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>user-agent</td>
<td>{user-agent}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>host</td>
<td>{host}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>content-length</td>
<td>{content-length}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>content-type</td>
<td>{content-type}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>x-forwarded-for</td>
<td>{x-forwarded-for}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>content-encoding</td>
<td>{content-encoding}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>accept-encoding</td>
<td>{accept-encoding}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>content-disposition</td>
<td>{content-disposition}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>x-requested-with</td>
<td>{x-requested-with}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>connection</td>
<td>{connection}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>proxy-connection</td>
<td>{proxy-connection}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>x-authenticated-user</td>
<td>{x-authenticated-user}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>method</td>
<td>{method}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>path</td>
<td>{path}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>scheme</td>
<td>{scheme}h</td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td><strong>Key Name</strong></td>
<td><strong>Configuration Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status_code</td>
<td><code>{status_code}</code></td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>ver</td>
<td><code>{ver}</code></td>
<td>Key is HTTP header.</td>
</tr>
<tr>
<td>log_type</td>
<td><code>{log_type}</code></td>
<td>Fixed value is 1, which means access log.</td>
</tr>
<tr>
<td>company_id</td>
<td><code>{company_id}</code></td>
<td>Company ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, value is default</td>
</tr>
<tr>
<td>ad_domain</td>
<td><code>{ad_domain}</code></td>
<td>AD domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, default null</td>
</tr>
<tr>
<td>user_name</td>
<td><code>{user_name}</code></td>
<td>Client IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 10.204.171.200</td>
</tr>
<tr>
<td>group_name</td>
<td><code>{group_name}</code></td>
<td>Group name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, default null</td>
</tr>
<tr>
<td>department</td>
<td><code>{department}</code></td>
<td>Department</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, default null</td>
</tr>
<tr>
<td>device</td>
<td><code>{device}</code></td>
<td>Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, default null</td>
</tr>
<tr>
<td>app</td>
<td><code>{app}</code></td>
<td>Protocol channel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1: HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2: HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3: HTTP2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4: FTP</td>
</tr>
<tr>
<td><strong>Key Name</strong></td>
<td><strong>Configuration Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>tls_version</td>
<td><code>{tls_version}</code></td>
<td>TLS version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0: None TLS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1: SSLv3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2: TLSv1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3: TLSv1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4: TLSv1.2</td>
</tr>
<tr>
<td>size</td>
<td><code>{size}</code></td>
<td>Transport bytes by Deep Discovery Web Inspector, unit bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 15</td>
</tr>
<tr>
<td>dst</td>
<td><code>{dst}</code></td>
<td>Destination IP address of request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 54.148.125.151</td>
</tr>
<tr>
<td>src</td>
<td><code>{src}</code></td>
<td>Source IP address of request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 10.204.171.200</td>
</tr>
<tr>
<td>upstream_size</td>
<td><code>{upstream_size}</code></td>
<td>The upstream payload from Deep Discovery Web Inspector to server, unit bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 54</td>
</tr>
<tr>
<td>downstream_size</td>
<td><code>{downstream_size}</code></td>
<td>The downstream payload from server to Deep Discovery Web Inspector, unit bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 49</td>
</tr>
<tr>
<td>domain</td>
<td><code>{domain}</code></td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: ca95-1.winshipway.com</td>
</tr>
<tr>
<td>Key Name</td>
<td>Configuration Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>tech_type</td>
<td>{tech_type}</td>
<td>Detection type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: 70</td>
</tr>
<tr>
<td>tech_sub_type</td>
<td>{tech_sub_type}</td>
<td>Detection sub-type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, default 0</td>
</tr>
<tr>
<td>threat_type</td>
<td>{threat_type}</td>
<td>Threat type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1: Ransomware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2: C&amp;C Callback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3: Suspicious Malware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4: Suspicious URLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5: Suspicious Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 6: Suspicious Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7: Malicious URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8: Malicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 9: Suspicious Content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10: Coin Miners</td>
</tr>
<tr>
<td>severity</td>
<td>{severity}</td>
<td>Risk level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0: user defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1: low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2: medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3: high</td>
</tr>
<tr>
<td>policy_name</td>
<td>{policy_name}</td>
<td>Policy name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: test</td>
</tr>
<tr>
<td>profile_name</td>
<td>{profile_name}</td>
<td>Profile name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved, currently displays as default</td>
</tr>
<tr>
<td><strong>Key Name</strong></td>
<td><strong>Configuration Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>wrs_threshold</td>
<td>{wrs_threshold}</td>
<td>WRS threshold&lt;br&gt;Value is set to 50</td>
</tr>
<tr>
<td>principal_name</td>
<td>{principal_name}</td>
<td>Principal name&lt;br&gt;Reserved, default is null</td>
</tr>
<tr>
<td>request</td>
<td>{request}</td>
<td>URL&lt;br&gt;Example: hxxp://ca95-1.winshipway.com/</td>
</tr>
<tr>
<td>cat</td>
<td>{cat}</td>
<td>URL category&lt;br&gt;Example: Ransomware</td>
</tr>
<tr>
<td>app_name</td>
<td>{app_name}</td>
<td>Application name&lt;br&gt;Reserved, default is null</td>
</tr>
<tr>
<td>wrs_score</td>
<td>{wrs_score}</td>
<td>WRS score&lt;br&gt;Example: 81</td>
</tr>
<tr>
<td>malware_type</td>
<td>{malware_type}</td>
<td>Malware type&lt;br&gt;Reserved, default 0</td>
</tr>
<tr>
<td>malware_name</td>
<td>{malware_name}</td>
<td>Malware name&lt;br&gt;Example: Ransomware</td>
</tr>
<tr>
<td>so_data</td>
<td>{so_data}</td>
<td>Suspicious object displayed on the Deep Discovery Web Inspector <strong>Detections</strong> page&lt;br&gt;Can be one of the following types:&lt;br&gt;- Domain&lt;br&gt;- URL&lt;br&gt;- Server IP&lt;br&gt;- File SHA1</td>
</tr>
<tr>
<td><strong>Key Name</strong></td>
<td><strong>Configuration Parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| fname | {fname} | File name  
  Example: a.txt |
| filehash | {filehash} | SHA1  
  Example: 0d3d4cdfff683b0c17843a889e867fe29095c3ac |
| act | {act} | Action  
  Can be one of the following values:  
  • allow  
  • monitor  
  • block  
  • analyze |
| msg | {msg} | Log description  
  Value is null |
| rt | {rt} | UTC timestamp  
  Example: Oct 20 2017 17:15:57 GMT+00:00 |
| local_addr | {local_addr} | The Deep Discovery Web Inspector management console IP address. |

**Virtual Analyzer**

Deep Discovery Web Inspector can send suspicious objects to Virtual Analyzer for further analysis.
Deep Discovery Web Inspector uses imported Virtual Analyzer images for sandbox analysis.

- **Virtual Analyzer Overview on page 9-40**
- **Virtual Analyzer Status on page 9-41**
- **Virtual Analyzer Images on page 9-43**
- **Types of Virtual Analyzer Networks on page 9-49**

### Virtual Analyzer Overview

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

You must import Virtual Analyzer images before Deep Discovery Web Inspector can perform sandbox analysis. You can check the status of the Virtual Analyzer sandbox environment and view the table to understand the real-time status of Virtual Analyzer and the sandbox images.

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.

**Suspicious Object Scanning**

When an scannable object enters your network, Deep Discovery Web Inspector scans the object with a series of scan engines: URL Filtering, Network Content Inspection, Advanced Threat Scan, Predictive Web Pre-Filter, Script Analyzer, and TrendX Engine.

After scanning the object for suspicious characteristics, Deep Discovery Web Inspector correlates the results to either assign a risk level and immediately execute a policy action based on the risk level, or sends the object to Virtual Analyzer for further analysis.

If the object need be submitted to the sandbox for further analysis after these engines prefilter, Virtual Analyzer gathers security intelligence from several Trend Micro Smart Protection Network services to investigate the object's risk level.

**Virtual Analyzer Status**

The Virtual Analyzer **Status** tab provides information in the following sections:

• **Overall Status**: Whether Virtual Analyzer is running.

• **Image Table**: Shows the allocated instances, status (busy or idle), and the utilization information for each sandbox image.

The following table describes the Virtual Analyzer overall statuses.

**TABLE 9-4. Virtual Analyzer Overall Statuses**

<table>
<thead>
<tr>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting...</td>
<td>Virtual Analyzer is starting all sandbox instances.</td>
</tr>
<tr>
<td>Stopping...</td>
<td>Virtual Analyzer is stopping all sandbox instances.</td>
</tr>
</tbody>
</table>
Running | Virtual Analyzer is analyzing samples.
---|---
No images | No images have been imported into Virtual Analyzer.
Maintenance | Virtual Analyzer is increasing or decreasing the number of instances for one or more images.
Importing images... | Virtual Analyzer is importing an image.
Removing images... | Virtual Analyzer is removing one or more images.

The following table describes status and available information for each image.

**Table 9-5. Image Status and Information Table**

<table>
<thead>
<tr>
<th>HEADER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Permanent image name</td>
</tr>
<tr>
<td>Instances</td>
<td>Number of deployed sandbox instances</td>
</tr>
<tr>
<td>Current Status</td>
<td>Distribution of idle and busy sandbox instances</td>
</tr>
<tr>
<td>Utilization</td>
<td>Overall utilization (expressed as a percentage) based on the number of sandbox instances currently processing samples</td>
</tr>
</tbody>
</table>

Related information

* Viewing Virtual Analyzer Status

**Viewing Virtual Analyzer Status**

**Procedure**

1. Go to Administration > Virtual Analyzer > Status.
2. View the overall status of Virtual Analyzer and view the summary information about existing Virtual Analyzer images.
Virtual Analyzer Images

Virtual Analyzer does not contain any images by default. You must import an image before Virtual Analyzer can analyze samples.

Virtual Analyzer supports Open Virtualization Format Archive (OVA) files.

**Note**
Before importing custom images, verify that you have secured valid licenses for all included platforms and applications.


**Virtual Analyzer Image Preparation**

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.


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*.

Deep Discovery Web Inspector supports a maximum of three images at a time.

**Importing Virtual Analyzer Images**

Virtual Analyzer supports OVA files between 1GB and 20GB in size.
Note

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 Administration > Virtual Analyzer > Images.
2. Click Import.
   The Import Image screen appears.
3. Specify a name in the Image field.
4. Specify the number of instances for this image.
5. Select an image source and configure the applicable settings.
   • Local or network folder
     See Importing an Image from a Local or Network Folder on page 9-44.
   • HTTP or FTP server
     See Importing an Image from an HTTP or FTP Server on page 9-46.

Importing an Image from a Local or Network Folder

The following procedure explains how to import an image into Virtual Analyzer from a local or network folder. Before you can import an image, your computer must be able to establish a connection to Deep Discovery Web Inspector.

Procedure

1. Select Local or network folder.
2. Specify an image name with a maximum of 260 characters/bytes.
3. Click Connect.
From the connection status under Step 1 of the Images screen, the status message verifies that the connection has been established.

4. Once connected, import the image using the Virtual Analyzer Image Import Tool.
   a. Click Download Image Import Tool.
   b. Open the file VirtualAnalyzerImageImportTool.exe.
   c. Specify the Deep Discovery Web Inspector management IP address.

   **Note**
   
   For information about configuring the Deep Discovery Web Inspector management IP address, see Configuring Network Settings on page 9-14.

   d. Click **Browse** and select the image file.
   e. Click **Import**.

   The import process will stop if:
   • The connection to the device was interrupted
   • Memory allocation was unsuccessful
   • Windows socket initialization was unsuccessful
   • The image file is corrupt

5. Wait for import to complete.
Importing an Image from an HTTP or FTP Server

The following procedure explains how to import an image into Virtual Analyzer from an HTTP or FTP server.

Procedure

1. Select HTTP or FTP server.
2. Specify the HTTP or FTP URL settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Specify the HTTP or FTP URL.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> ftp://custom_ftp:1080/tmp/test.ova</td>
</tr>
<tr>
<td>User name</td>
<td>Optional: Specify the user name if authentication is required.</td>
</tr>
<tr>
<td>Password</td>
<td>Optional: Specify the password if authentication is required.</td>
</tr>
<tr>
<td>Anonymous Login</td>
<td>Optional: Select to disable the user name and password, and authenticate anonymously.</td>
</tr>
</tbody>
</table>
3. Click Import.
4. Wait for deployment to complete.

Deleting Virtual Analyzer Images
Procedure

1. Go to Administration > Virtual Analyzer > Images.
2. Select an image by selecting the box in the left column.
3. Click Delete.
   
   The image is removed.

Modifying Instances

Procedure

1. Go to Administration > Virtual Analyzer > Images.
2. Click Modify.
   
   The Modify Instances screen appears.
3. Modify the instance number for any image.
4. Click Save.

Virtual Analyzer Network

When Deep Discovery Web Inspector is using an internal Virtual Analyzer, you can configure how Virtual Analyzer instances connect to external destinations, including the Internet. You can configure no network access, access using the management port, or access using a custom port.

Note

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

1. Go to Administration > Virtual Analyzer > Network Connection.

2. From the Network type drop-down list, select how Virtual Analyzer connects to the network.
   - No network access
   - Management network
   - Custom network

For information about network types, see Types of Virtual Analyzer Networks on page 9-49.

3. Specify network connection settings, depending on the network type specified.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No network access</td>
<td>There are no configurable settings for this network type. This is the default selection.</td>
</tr>
<tr>
<td>Management network</td>
<td>Proxy settings</td>
</tr>
<tr>
<td></td>
<td>• If a proxy server is not required for the internal Virtual Analyzer to connect to the Internet, select Do not use a proxy server from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select Use a dedicated proxy server from the drop-down list and provide the following information:</td>
</tr>
<tr>
<td></td>
<td>• Server address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Proxy server requires authentication: If authentication is required, select this check box and type the user name and password.</td>
</tr>
<tr>
<td>Custom Network</td>
<td>Sandbox port</td>
</tr>
<tr>
<td></td>
<td>• If eth1 is not already configured, click Configure IPv4 settings to configure network settings.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Proxy settings</td>
<td>If a proxy server is not required for the internal Virtual Analyzer to connect to the Internet, select <strong>Do not use a proxy server</strong> from the drop-down list. If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select <strong>Use a dedicated proxy server</strong> from the drop-down list and provide the following information:</td>
</tr>
<tr>
<td></td>
<td>• Server address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• <strong>Proxy server requires authentication</strong>: If authentication is required, select this check box and type the user name and password.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

5. After configuring the network connection, click **Test Internet Connectivity** to verify that Virtual Analyzer can connect to the Internet.

---

**Note**

If **No network access** is selected, a connection cannot be established. The default setting is **No network access**.

---

**Types of Virtual Analyzer Networks**

When simulating file behavior, Virtual Analyzer uses its own analysis engine to determine the risk of an object. The selected network type also determines whether submitted objects can connect to the Internet, and if so, which network is used to connect.

---

**Note**

Internet access improves analysis by allowing samples to access C&C callback addresses or other external links.
<table>
<thead>
<tr>
<th>NETWORK TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No network access</td>
<td>Isolates Virtual Analyzer traffic within the sandbox environment. The environment has no connection to an outside network.</td>
</tr>
</tbody>
</table>

**Note**

Virtual Analyzer has no Internet connection and relies only on its analysis engine.

<table>
<thead>
<tr>
<th>NETWORK TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management network</td>
<td>Directs Virtual Analyzer traffic through the management port.</td>
</tr>
</tbody>
</table>

**Important**

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

Important connections to the management network may result in malware propagation and other malicious activity in the network. Trend Micro recommends using an environment isolated from the management network, such as a test network with Internet connection but without connection restrictions.

<table>
<thead>
<tr>
<th>NETWORK TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom network</td>
<td>Virtual Analyzer connects to the Internet using the eth1 port.</td>
</tr>
</tbody>
</table>

**System Maintenance**

Go to the Administration > System Maintenance screen to perform the following operations:

- Configuring Storage Maintenance on page 9-51
- Debug Logs on page 9-51
- Testing Network Connections on page 9-53
- Network Packet Capture on page 9-54
- Enabling/Disabling Bypass Mode on page 9-56
Configuring Storage Maintenance

Storage maintenance settings allow you to control the amount of log data that the system saves.

Procedure

1. Go to Administration > System Maintenance > Storage Maintenance.
2. Specify the log settings.
   - For Delete logs older than, specify the number of days to keep logs.
     
     **Note**
     The specified value must be between 3 and 366.
   
   - For Delete logs when the total free disk space is equal to or lower than, specify the disk space threshold (%) for automatic log deletion.

     The threshold value must be between 10 and 50.

     Deep Discovery Web Inspector purges 10% more than the specified percentage.

3. Click Save.

Debug Logs

Deep Discovery Web Inspector creates debug logs that include information Trend Micro Support uses to troubleshoot problems.

You can export the following log levels:
• Error-level logs (for all IP addresses)
• Debug-level logs (for a single IP address or IP address range)

Configuring Debug Log Level

Configure the debug log level that Deep Discovery Web Inspector uses to save debug logs that you can provide to Trend Micro Support for troubleshooting a problem.

---

**Important**

If you change the log level, you must wait for Deep Discovery Web Inspector to collect a sufficient number of logs at the new log level before exporting/downloading the debug log.

---

**Procedure**

1. Go to Administration > System Maintenance > Debug Logs.
2. Change the log level.
   
   Options are Error (default) or Debug.
3. If log level is set to Debug, perform one of the following:
   
   • Enter an IP address in IP.
   
   • Enter an IP address range in IP Range.
4. Click Save.
   
   Changing the log level setting restarts the service.

---

Exporting and Downloading Debug Files

Export and download your debug file to provide information to Trend Micro Support for troubleshooting a problem.
**Procedure**

1. Go to **Administration > System Maintenance > Debug Logs**.
   - By default, the debug level is set to **Error**.
   - If desired, you can set the debug level to **Debug** and specify an IP address or IP address range on which to collect debug-level logs.

   Changing the log level setting restarts the service. See *Configuring Debug Log Level on page 9-52*.

---

**Important**

If you change the log level, you must wait for Deep Discovery Web Inspector to collect a sufficient number of logs at the new log level before exporting/downloading the debug log.

---

2. If log level is set to **Debug**, perform one of the following:
   - Enter an IP address in **IP**.
   - Enter an IP address range in **IP Range**.

3. Click **Export**.

4. Wait for the export to complete. The time required depends on the amount of data to export.

5. Click **Download**.

---

**What to do next**

After downloading the debug file, you must delete the current export result before performing another export.

---

**Testing Network Connections**

You can use the **Network Services Diagnostics** screen to test network connections using network tools such as ping and to test connectivity to other network services such as the ActiveUpdate and Web Reputation Service servers.
**Procedure**

1. Go to Administration > System Maintenance > Network Services Diagnostics.

2. 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.

---

**Network Packet Capture**

You can use the network packet capture to provide information to Trend Micro Support for troubleshooting a problem.

Choose a single or multiple network interfaces on which to simultaneously capture network packets and then start the capture. After enough time has elapsed to capture data, you can stop the capture. Deep Discovery Web Inspector automatically compresses the capture files. You can then download the compressed packet capture files for analysis.

The packet capture for each interface saves as an individual file using the naming convention of `capture-{interface}-{date:time}.pcap`. After the network packet capture completes, Deep Discovery Web Inspector automatically compresses all `.pcap` files for that capture and saves them in one compressed package file named `capture-{date}.tgz`. For example, if you perform a packet capture on the eth0 network interface on July 27, 2017, the capture file is named `capture-eth0-20170727082849.pcap` and the compressed file is named `capture-20170727082849.tgz`
The compressed file displays in the downloadable list. You can either download or delete the compressed file.

Once you download and uncompress the .tgz file, each individual .pcap file is available for examination.

**Capturing Network Packets**

Capture network packets to analyze traffic on selected interfaces or a single interface.

**Procedure**

1. Go to the Administration > System Maintenance > Network Packet Capture.

2. Select the appropriate interface(s) from the Available interfaces box and move them to the Selected interfaces box.

3. Click Start Capture.

   The capture begins.

4. After sufficient data is captured, click Stop Capture.

5. Select the files you want to download and click Download.

6. (Optional) You can delete any unneeded files by selecting them and clicking Delete.
Enabling/Disabling Bypass Mode

You can enable the Deep Discovery Web Inspector appliance for bypass mode, which allows traffic to bypass inspection as it traverses the appliance. Bypass mode can be used as a diagnostic tool and a fail-over mechanism to ensure that traffic continues flowing through the Deep Discovery Web Inspector appliance during software failure or system upgrade. After issues are corrected or upgrade completed, you can disable bypass mode so that traffic will again be inspected by Deep Discovery Web Inspector.

CAUTION!
Do not change the bypass mode setting if you are unsure of the impact to Deep Discovery Web Inspector functionality. Contact Trend Micro Technical Support for assistance if needed.

Procedure
1. Go to Administration > System Maintenance > Bypass Mode.
2. Perform the appropriate action:
   - To enable bypass mode and allow traffic to pass through the device without inspection, turn the option On.
   - To disable bypass mode and allow traffic to be inspected, turn the option Off.

   If set to Off or the device is down, traffic will pass through the device without inspection.

   After you change the bypass status, traffic through the Deep Discovery Web Inspector appliance is temporarily disrupted for a maximum of about 5 seconds. As most browsers and applications have TCP retransmission mechanisms, impact to the end user is limited.

Configuring Bypass/Redirect Policies

You can configure bypass/redirect policies to control how traffic is managed as it traverses the Deep Discovery Web Inspector appliance.
By default, all traffic is scanned according to configured scan policies and HTTPS inspection policies. However, you can use bypass/redirect policies to specify that some traffic is redirected to the scan daemon of Deep Discovery Web Inspector while other traffic bypasses scanning and traverses straight through the appliance to the endpoint.

**Note**

Bypass/redirect policies work only in bridge mode. In proxy mode, bypass/redirect policies do not work.

### Types of Policies

You can configure the following types of policies:

- **Bypass**
  
  Bypass traffic based on source IP addresses, destination IP addresses, or HTTPS domains.
  
  All traffic is scanned according to scan and HTTPS inspection policies except for traffic that matches source IP addresses, destination IP addresses, or HTTPS domains configured in the bypass policy.
  
  You can use a bypass policy to exclude traffic from certain devices that do not require scanning (such as printers) or that you do not want scanned.

- **Redirect**
  
  Redirect traffic based on source or destination IP addresses or source or destination MAC addresses.
  
  Traffic is scanned only for traffic that matches source or destination IP addresses or sources or destination MAC addresses configured in the redirect policy. All other traffic is bypassed with no scanning.
  
  You can use a redirect policy when most traffic that you want scanned comes only from or is destined to certain devices (such as gateways and routers).

### Bypass/Redirect Policies Priorities and Precedence

You can configure policies to control how traffic is managed as it traverses the Deep Discovery Web Inspector appliance. You can have one bypass policy with multiple
entries and one redirect policy with multiple entries. You should understand Deep Discovery Web Inspector priorities and precedence in evaluating bypass/redirect policies.

- Bypass policies are higher priority than redirect policies. If traffic matches both a bypass policy and a redirect policy, the bypass policy takes precedence and is used to evaluate the traffic.

- The bypass entries are evaluated in order. When a network packet is evaluated, the first matched entry is applied without evaluating following bypass entries.

- The redirect entries are evaluated in order. When a network packet is evaluated, the first matched entry is applied without evaluating following redirect entries.

**Example:** Deep Discovery Web Inspector is configured with both a bypass policy and a redirect policy. Traffic enters Deep Discovery Web Inspector from source IP address 10.10.10.10:

**Bypass policy:**

```
Source IP:
10.10.10.10
10.10.10.0/24
```

**Redirect policy:**

```
Source IP:
10.10.10.0/24
```

The source IP address matches the first entry in the bypass policy and is used for evaluation. The source address also matches the entry in the redirect policy. Since the bypass policy takes priority, traffic from 10.10.10.10 bypasses scanning.

**Managing Bypass/Redirect Policies**

Go to Administration > System Maintenance > Bypass/Redirect Policy to perform any of the following tasks to manage policies.
Procedure

- Click on the **Bypass** tab to view information about the existing bypass policy configuration.
- Click on the **Redirect** tab to view information about the existing redirect policy configuration.
- Add entries to the bypass or redirect policies.
- Delete existing entries from the bypass or redirect policies.
- Click **Import/Export Bypass** or **Import/Export Redirect** to export or import a copy of the defined bypass/redirect policies.

Configuring a Redirect Policy

When a redirect policy is configured and traffic matches an entry in the policy, Deep Discovery Web Inspector scans the matching network traffic for a match to scan policies and HTTPS inspection policies. You can configure redirect policies to match traffic based on the following:

- Source IP addresses
- Source MAC addresses
- Destination IP addresses
- Destination MAC addresses

**Note**

If both a redirect policy and a bypass policy are configured, you should understand the priority and precedence rules that Deep Discovery Web Inspector uses for evaluating traffic. See **Bypass/Redirect Policies Priorities and Precedence on page 9-57**.

Procedure

1. Go to **Administration > System Maintenance > Bypass/Redirect Policy > Redirect**.
2. Specify the redirect settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Add Source IP Address** | Add one or more source IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Source IP Address**. You can add an IP address entry using any of the following formats:  
10.10.10.10  
10.1.1.0/24  
192.168.1.1-192.168.1.5 |
| **Add Destination IP Address** | Add one or more destination IP address entries, one entry at a time, by adding an IP address entry and then clicking **Add Destination IP Address**. You can add an IP address entry using any of the following formats:  
10.10.10.10  
10.1.1.0/24  
192.168.1.1-192.168.1.5 |
| **Add Source MAC Address** | Add one or more source MAC address entries, one entry at a time, by adding an MAC address entry and then clicking **Add Source MAC Address**. You can add a MAC address entry using any of the following formats:  
01-23-45-67-89-ab  
01:23:45:67:89:ac  
0123.4567.89ad |
| **Add Destination MAC Address** | Add one or more destination MAC address entries, one entry at a time, by adding an MAC address entry and then clicking **Add Destination MAC Address**.  
01-23-45-67-89-ab  
01:23:45:67:89:ac  
0123.4567.89ad |
3. Click Save.

Configuring a Bypass Policy

When a bypass policy is configured and traffic matches an entry in the policy, Deep Discovery Web Inspector bypasses network traffic scanning of that traffic and sends the traffic straight to the end point. You can configure bypass policies to match traffic based on the following:

- Source IP addresses
- Destination IP addresses
- HTTPS domains

**Note**

Deep Discovery Web Inspector first evaluates matches in the Source IP address and Destination IP address bypass lists, then evaluates matches in the HTTPS domain bypass list (by comparing destination IP addresses of traffic with all IP addresses of this domain name), if any of the entries in the bypass lists are matched, traffic is bypassed.

An IP address might be associated with multiple domain names. In this case, Deep Discovery Web Inspector bypasses all the matching domains.

**Note**

If both a redirect policy and a bypass policy are configured, you should understand the priority and precedence rules that Deep Discovery Web Inspector uses for evaluating traffic. See Bypass/Redirect Policies Priorities and Precedence on page 9-57.

**Procedure**

1. Go to Administration > System Maintenance > Bypass/Redirect Policy > Bypass.

2. Specify the bypass settings.
<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Source IP Address</td>
<td>Add one or more source IP address entries, one entry at a time, by adding an IP address entry and then clicking <strong>Add Source IP Address</strong>. You can add an IP address entry using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>10.10.10.10&lt;br&gt;10.1.1.0/24&lt;br&gt;192.168.1.1-192.168.1.5</td>
</tr>
<tr>
<td>Add Destination IP Address</td>
<td>Add one or more destination IP address entries, one entry at a time, by adding an IP address entry and then clicking <strong>Add Destination IP Address</strong>. You can add an IP address entry using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>10.10.10.10&lt;br&gt;10.1.1.0/24&lt;br&gt;192.168.1.1-192.168.1.5</td>
</tr>
<tr>
<td>Add HTTPS Domain</td>
<td>Add one or more HTTPS domain entries, one entry at a time, by adding a domain name entry and then clicking <strong>Add HTTPS Domain</strong>. You can use wildcards when adding entries (* and ?). The domain prefix https:// is insensitive and should not be included in the input for matching.</td>
</tr>
<tr>
<td></td>
<td>test?.example.com&lt;br&gt;example.com&lt;br&gt;*.example2.com</td>
</tr>
</tbody>
</table>

3. Click Save.

**Back Up or Restoring a Configuration**

You can back up or restore certain Deep Discovery Web Inspector configuration settings by exporting or importing those settings using the management console.

Trend Micro recommends exporting your settings to:
• Keep a backup

If Deep Discovery Web Inspector cannot recover from a critical problem, import your configuration backup after restoring the device to automatically implement the pre-failure configuration.

Or you can create a backup on a running appliance before making changes to the configuration. Having a backup provides you with the option of quickly and conveniently reverting to the original settings saved in the backup at a later time.

• Replicate settings across several devices

If you have several devices on your network, you do not need to separately configure most settings. You can replicate a configuration across several Deep Discovery Web Inspector appliances by restoring the same configuration file into each appliance.

**Important**

Deep Discovery Web Inspector only supports restoring configurations from other Deep Discovery Web Inspector appliances running the same version. For example, you cannot restore an appliance running version 1.0 with a configuration file backed up from an appliance running a later version.

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

Trend Micro recommends:

• Backing up the current configuration before each import operation.

• Performing the operation when Deep Discovery Web Inspector is idle. Importing and exporting affects Deep Discovery Web Inspector performance.

**Settings That Are Backed Up or Restored**

You can back up settings from the screens and tabs listed in the following table.
TABLE 9-6. Backed up configuration settings

<table>
<thead>
<tr>
<th>Screen</th>
<th>Tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Policy &gt; Policy</td>
<td>All policies</td>
</tr>
<tr>
<td>Policy &gt; HTTPS Inspection</td>
<td>All HTTPS policies</td>
</tr>
<tr>
<td>Policy &gt; User Defined Settings</td>
<td>Network objects</td>
</tr>
<tr>
<td></td>
<td>Domain objects</td>
</tr>
<tr>
<td></td>
<td>Approved list and blocked list</td>
</tr>
<tr>
<td></td>
<td>All notification pages</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Alerts</td>
<td>Rules</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports</td>
<td>Schedules</td>
</tr>
<tr>
<td>Administration &gt; Component Updates</td>
<td>Enable scheduled update</td>
</tr>
<tr>
<td></td>
<td>Schedule time</td>
</tr>
</tbody>
</table>

Backed Up a Configuration

During export, do not:

- Access other management console screens or modify any settings
- Perform any database operations
- Start/stop any services on the device or in the group to which the device belongs
- Launch other export or import tasks

Note

For information on the settings that are backed up, see Settings That Are Backed Up or Restored on page 9-63.
**Procedure**

1. Go to **Administration > System Maintenance > Configure BackUp / Restore**.

2. Next to **Back Up Configuration Settings**, click **Export**.

   A confirmation dialog box appears.

3. Click **OK** to continue with the export.

   **Note**
   
   If you click **Cancel**, the export is canceled.

   A **File Download** window appears.

4. Click **OK** to save the configuration file to local storage.

**Restoring a Configuration**

Restoring Deep Discovery Web Inspector settings replaces the original settings and rules, such as policy settings, with the imported configuration.

During the restore, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Launch other export or import tasks.

**Note**

For information on the settings that you can restore, see **Settings That Are Backed Up or Restored on page 9-63**.
Procedure

1. Go to Administration > System Maintenance > Configure BackUp / Restore.

2. Next to Restore Configuration Settings, click Select File and locate the backup file to use for the restore.

3. Click Restore.

   A confirmation dialog box appears.

4. Click OK to continue with the restore.

   **Note**

   If you click Cancel, the restore is canceled.

   All services restart. It can take up to two minutes to restart services after applying imported settings and rules.

Power Off / Restart

The **Power Off / Restart** screen provides options to power off or restart the Deep Discovery Web Inspector appliance and its associated services.

Restarting Deep Discovery Web Inspector

**Procedure**

1. Go to Administration > System Maintenance > Power Off/R restart.

2. Click Restart.

3. Click Proceed.

4. At the confirmation dialog box, choose the appropriate action.
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart</td>
<td>Click to restart the appliance.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to cancel the restart operation.</td>
</tr>
</tbody>
</table>

**Powering Off Deep Discovery Web Inspector**

**Procedure**

1. Go to **Administration > System Maintenance > Power Off/Restart**.
2. Click **Power off**.
3. Click **Proceed**.
4. At the confirmation dialog box, choose the appropriate action.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Off</td>
<td>Click to power off the appliance.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to cancel the power off operation.</td>
</tr>
</tbody>
</table>

**Accounts / Contacts**

Deep Discovery Web Inspector uses role-based administration to grant and control access to the management console where they can perform administrative tasks.

To use role-based administration, you create custom accounts and assign a specific role to each account. A role defines the level of access to the management console.

By creating custom accounts and assigning specific management console privileges to the accounts, you can present account users with only the tools and permissions necessary to perform specific tasks.
Additionally, as part of contacts administration, you can configure a list of recipients in the contact list. The contact list is used by default when sending alert notifications and reports.

**Managing Accounts**

Deep Discovery Web Inspector has a default administrator account (admin) that has full administrative access.

The default administrator account can perform all tasks, including adding new administrator accounts.

Accounts assigned the administrative role can create additional accounts and assign these accounts the **Administrator** role or the **Operator** role. Administrators can delegate tasks to different administrators and operators to reduce bottlenecks in Deep Discovery Web Inspector administration.

Administrator accounts can additionally edit or delete existing accounts.

**Account Role Classifications**

<table>
<thead>
<tr>
<th>ROLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Users have complete administrative access to the features and settings contained in the menu items.</td>
</tr>
<tr>
<td></td>
<td>• Dashboard: Full access</td>
</tr>
<tr>
<td></td>
<td>• Detections: Full access</td>
</tr>
<tr>
<td></td>
<td>• Policy: Full access</td>
</tr>
<tr>
<td></td>
<td>• Alerts / Reports: Full access</td>
</tr>
<tr>
<td></td>
<td>• Administration: Full access</td>
</tr>
</tbody>
</table>
## Role Description

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dashboard</strong>: Full access</td>
</tr>
<tr>
<td></td>
<td>• <strong>Detections</strong>: Full access</td>
</tr>
<tr>
<td></td>
<td>• <strong>Policy</strong>: No access</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts / Reports</strong>: Read-only</td>
</tr>
<tr>
<td></td>
<td>• <strong>Administration</strong>: No access</td>
</tr>
</tbody>
</table>

### Adding Local User Accounts

You can add local user accounts to provide role-based access to the Deep Discovery Web Inspector management console.

#### Procedure

1. Go to **Administration > Accounts / Contacts > Accounts**.
2. Click **Add**.
   - The **Add Account** screen appears.
3. Toggle the **Status** of this account.
4. Specify the account user name.
5. Enter the password and confirm it.
6. Select a **Role** for this account.
   - The role determines the level of access this account has. Valid options are **Administrator** and **Operator**.

   *Account Role Classifications on page 9-68*
7. Click **Save**.

   The new account is added to the **Accounts** list.

---

**Editing Accounts**

You can edit an account's settings, including the account name and password. You can also change the account's role if you need to adjust the permissions for that account because of organizational changes.

---

**Procedure**

1. Go to **Administration > Accounts / Contacts > Accounts**.
2. Click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

---

**Deleting Accounts**

Delete accounts to adjust settings for a role revision or other organizational changes.

---

**Note**

You can only delete custom accounts. You cannot delete the default Deep Discovery Web Inspector administrator account.

---

**Procedure**

1. Go to **Administration > Accounts / Contacts > Accounts**.
2. Select the account to remove.
3. Click **Delete**.
4. At the confirmation message, click OK.

Changing Your Password

You can change your password when you are logged on to the management console.

Procedure

1. On the management console banner, click your account name and then click Change password.

   The Change Password screen appears.

2. Specify password settings.
   • Old password
   • New password
   • Confirm password

3. Click Save.

Managing Contacts

You can add or remove recipient email addresses on the contacts page. Contacts added to this list are sent emails if the default option Send to all contacts is selected when configuring alerts and reports.

Procedure

1. Go to Administration > Accounts / Contacts > Contacts.

2. Type the email addresses of recipients who will receive notifications and reports.
   Use a semicolon to separate multiple recipients.

3. Remove any recipients who should no longer receive notifications and reports.
4. Click Save.

Related information

- Configuring Alert Notifications
- Scheduling Reports

License

For information about managing your product license, see:

Licensing and Maintenance on page 10-1

About Deep Discovery Web Inspector

You can use the About screen in Help > About to view the firmware version, API key, and other product details.
Chapter 10

Licensing and Maintenance

Topics include:

- Maintenance Agreement on page 10-2
- Activation Codes on page 10-2
- Product License Description on page 10-2
- Product License Status on page 10-3
- Viewing Your Product License on page 10-4
- Managing Your Product License on page 10-5
Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration 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.

Typically, 90 days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

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

Activation Codes

Use a valid Activation Code to enable your product. A product will not be operable until activation is complete. An Activation Code has 37 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

If you received a Registration Key instead of an Activation Code, use it to register the product at:

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

A Registration Key has 22 characters (including the hyphens) and appears as follows:

xx-xxxx-xxxx-xxxx

After registration, your Activation Code is sent via email.

Product License Description

The following table describes your product license. For information about viewing the product license, see Viewing Your Product License on page 10-4.
The product name is Deep Discovery Web Inspector-<module name>.
The value for <module name> can be either 510 or 1100. For example: Deep Discovery Web Inspector-510

The product version is associated with the Activation Code and product license. Knowing the product version is helpful for troubleshooting issues.

The Activation Code has 37 characters (including the hyphens) and appears as follows:
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
For details, see Activation Codes on page 10-2.

The license type includes full and evaluation licenses. The Maintenance Agreement defines the available license type.

The number of license seats purchased with this product.

The current state of your product license. For information about the product license statuses, see Product License Status on page 10-3.

The date that the license expires.

Your product license status changes from when you first acquire the product to when you must renew the license. Some of these statuses require intervention in order to maintain all product functionality. You can evaluate the product without activating a product license.
### Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activated</td>
<td>Deep Discovery Web Inspector has full product functionality and component updates for the license period. Technical Support is available based on the Maintenance Agreement.</td>
</tr>
<tr>
<td>In Grace Period</td>
<td>Deep Discovery Web Inspector is activated and has full product functionality for a limited time during the grace period.</td>
</tr>
<tr>
<td>Inactivated</td>
<td>Technical support and component updates are not available. All other Deep Discovery Web Inspector functionality is available.</td>
</tr>
<tr>
<td>Expired</td>
<td>The license is no longer valid. After the grace period lapses, product functionality is limited.</td>
</tr>
<tr>
<td></td>
<td>• For evaluation licenses, component updates are not available. Scanning is maintained with outdated components.</td>
</tr>
<tr>
<td></td>
<td>• For full licenses, technical support and component updates are not available. Scanning is maintained with outdated components.</td>
</tr>
</tbody>
</table>

**WARNING!**

Outdated components significantly reduce product detection capabilities.

### Viewing Your Product License

**Procedure**

1. Go to Administration > License.

2. Under License Details, click View details online to display product licensing details.
Managing Your Product License

Procedure

1. Go to Administration > License.

2. Click New Activation Code.
   
   The Activation Code screen displays.

3. Specify the new activation code.

4. Read the Trend Micro license agreement and then click I have read and accept the terms of the Trend Micro License Agreement.

5. Click Save.
   
   The Deep Discovery Web Inspector activates.

6. View your product license.

   See Viewing Your Product License on page 10-4.
Chapter 11

Technical Support

Learn about the following topics:

• Troubleshooting Resources on page 11-2
• Contacting Trend Micro on page 11-3
• Sending Suspicious Content to Trend Micro on page 11-4
• Other Resources on page 11-5
Troubleshooting Resources

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

Using the Support Portal

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

**Procedure**

2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

**Tip**

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


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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia
provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

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

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

## Contacting Trend Micro

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

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone: +1 (817) 569-8900</td>
</tr>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:
  

- Trend Micro product documentation:
  
  http://docs.trendmicro.com
Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

File Reputation Services

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


Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

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

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

Using the Command Line Interface

You can use the Command Line Interface (CLI) to perform tasks, including the following tasks:

- Configure initial settings, such as the device IP address and host name
- Start, stop, and restart services
- View device status and statistics
- Debug and troubleshoot the device

Related information

- Entering the CLI
- Normal and Privileged Commands
- Entering Privileged Mode
- CLI Command Reference
Entering the CLI

To log on to the CLI, either connect directly to the Deep Discovery Web Inspector appliance or connect using SSH.

Procedure

• To make a direct connection, connect a monitor and keyboard to the Deep Discovery Web Inspector appliance.

  The appliance's command line interface is displayed on the monitor. You can log in to the CLI and perform basic tasks.

• If the SSH service is enabled, do the following to connect using SSH:

  a. Verify the computer you are using can ping Deep Discovery Web Inspector’s IP address.
  b. Use an SSH client to connect to Deep Discovery Web Inspector's IP address and TCP port 22.

  Note
  The default IP address / subnet mask is 192.168.252.1 / 255.255.0.0.

• Log in to the CLI with the default credentials.

  • User name: admin
  • Password: ddwi

  Note
  Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.
Normal and Privileged Commands

The Deep Discovery Web Inspector CLI commands are separated into two categories: normal and privileged commands. Normal commands are basic commands to obtain system information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by the `enable` command and password.

Entering Privileged Mode

**WARNING!**
Enter the shell environment only if your support provider instructs you to perform debugging operations.

Procedure

1. Log on to the CLI.
   
   See *Entering the CLI on page A-2.*

2. At the prompt, type `enable` and press ENTER to enter privileged mode.

3. Type the default password, `trend#1`, and then press ENTER.
   
   The prompt changes from > to #.

CLI Command Reference

The following tables explain the CLI commands.
Note
Some CLI commands require privileged mode. For details, see *Entering Privileged Mode on page A-3.*

configure network

**TABLE A-1. configure network**

<table>
<thead>
<tr>
<th>Command family configures network settings for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure network</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
</tbody>
</table>

configure network basic

**TABLE A-2. configure network basic**

<table>
<thead>
<tr>
<th>Configures basic network settings, including host name, IP address, subnet mask, gateway, and DNS.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure network basic</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
***Network Configuration***

Specify value for each item and press ENTER. Settings apply to the management port (eth0) and require a restart.

Host name: ddwi2.example.com
IPv4 address: 10.64.70.151
Subnet mask: 255.255.254.0
IPv4 gateway: 10.64.70.1
Preferred IPv4 DNS: 10.64.1.55
Alternate IPv4 DNS: 10.64.1.54

Confirm changes and restart (Y/N):

---

**configure network bypass**

**TABLE A-3. configure network bypass**

<table>
<thead>
<tr>
<th>Sets the bypass mode for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure network bypass</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To set the network bypass mode for the Deep Discovery Web Inspector appliance to &quot;on&quot;</td>
</tr>
<tr>
<td>configure network bypass on</td>
</tr>
</tbody>
</table>

**configure network dns ipv4**

**TABLE A-4. configure network dns ipv4**

| Configures IPv4 DNS settings for the Deep Discovery Web Inspector appliance. |
Syntax:

```
configure network dns ipv4 <dns1> [dns2]
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

- `<dns1>`: Primary DNS server
- `[dns2]`: Optional secondary DNS server

**Note**

Use a space to separate the primary and optional secondary DNS value.

Examples:

To configure the primary DNS with an IP address of 192.168.10.21:

```
configure network dns ipv4 192.168.10.21
```

To configure the primary and optional secondary DNS with the following values:

- Primary DNS: 192.168.10.21
- Secondary DNS: 192.168.10.22

```
configure network dns ipv4 192.168.10.21 192.168.10.22
```

configure network hostname

**TABLE A-5. configure network hostname**

Configures the host name for the Deep Discovery Web Inspector appliance.

Syntax:

```
configure network hostname <hostname>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

- `<hostname>`: Host name or fully qualified domain name (FQDN) for the Deep Discovery Web Inspector appliance

Examples:
To change the host name of the Deep Discovery Web Inspector appliance to test.example.com:

```bash
configure network hostname test.example.com
```

**configure network interface ipv4**

**TABLE A-6. configure network interface ipv4**

Configures the IPv4 static IP address and network mask for a network interface.

**Syntax:**

```bash
configure network interface ipv4 <interface> <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

- `<interface>`: Network interface name
- `<ip>`: IP address for the interface
- `<mask>`: Network mask for the interface

**Example:**

To configure a network interface with the following values:

- **Interface:** eth0
- **IPv4 address:** 192.168.10.10
- **IPv4 network mask:** 255.255.255.0

```bash
configure network interface ipv4 eth0 192.168.10.10 255.255.255.0
```

**configure network interface mtu**

**TABLE A-7. configure network interface mtu**

Configures the MTU size for a network interface.

**Syntax:**

```bash
configure network interface mtu <interface> <mtu>
```
**View** | Privileged
---|---
**Parameters** | `<interface>`: Network interface name  
<`mtu>`: Network interface MTU size

| **Example:** |
| To configure a network interface MTU with the following values:  
| • Interface: `eth0`  
| • MTU size: 1580 |
| configure network interface mtu eth0 1580 |

**configure network redirect**

**TABLE A-8. configure network redirect**

Command family configures policies to use when redirecting traffic for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
configure network redirect
```

<table>
<thead>
<tr>
<th><strong>View</strong></th>
<th>Privileged</th>
</tr>
</thead>
</table>

**configure network redirect bypass ip**

**TABLE A-9. configure network redirect bypass ip**

Command family configures a redirect bypass policy for the Deep Discovery Web Inspector appliance by specifying an IP address or IP network range.

**Syntax:**

```
configure network redirect bypass ip
```

<table>
<thead>
<tr>
<th><strong>View</strong></th>
<th>Privileged</th>
</tr>
</thead>
</table>
### configure network redirect bypass ip source add

**TABLE A-10. configure network redirect bypass ip source add**

Adds a redirect bypass policy by specifying a source IP address or network ID.

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
<td>configure network redirect bypass ip source add &lt;ip&gt; &lt;mask&gt;</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>&lt;ip&gt;: Source IP address or network ID</td>
</tr>
<tr>
<td></td>
<td>&lt;mask&gt;: Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To add a new redirect bypass policy entry using a source IP address:

```
configure network redirect bypass ip source add 10.10.10.150 255.255.255.255
```

To add a new redirect bypass policy entry using a source network ID:

```
configure network redirect bypass ip source add 10.10.10.0 255.255.255.128
```

### configure network redirect bypass ip source del

**TABLE A-11. configure network redirect bypass ip source del**

Deletes a redirect bypass policy by specifying a source IP address or network ID.

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
<td>configure network redirect bypass ip source del &lt;ip&gt; &lt;mask&gt;</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>&lt;ip&gt;: Source IP address or network ID</td>
</tr>
<tr>
<td></td>
<td>&lt;mask&gt;: Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To delete a redirect bypass policy entry using a source IP address:

```
configure network redirect bypass ip source del 10.10.10.150 255.255.255.255
```
To delete a redirect bypass policy entry using a source IP address:

```bash
configure network redirect bypass ip source del 192.168.1.1 255.255.255.255
```

To delete a redirect bypass policy entry using a source network ID:

```bash
configure network redirect bypass ip source del 192.168.1.0 255.255.255.128
```

configure network redirect bypass ip destination add

**TABLE A-12. configure network redirect bypass ip destination add**

| Adds a redirect bypass policy by specifying a destination IP address or network ID. |
| Syntax: configure network redirect bypass ip destination add <ip> <mask> |

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>
| Parameters | <ip>: Destination IP address or network ID  
<mask>: Network mask |

**Example:**

To add a new redirect bypass policy entry using a destination IP address:

```bash
configure network redirect bypass ip destination add 10.10.20.150 255.255.255.255
```

To add a new redirect bypass policy entry using a destination network ID:

```bash
configure network redirect bypass ip destination add 10.10.20.0 255.255.255.128
```

calculate network redirect bypass ip destination del

**TABLE A-13. configure network redirect bypass ip destination del**

| Deletes a redirect bypass policy by specifying a destination IP address or network ID. |
**Syntax:**

```bash
configure network redirect bypass ip destination del <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><code>&lt;ip&gt;</code>:</td>
<td>Destination IP address or network ID</td>
</tr>
<tr>
<td><code>&lt;mask&gt;</code>:</td>
<td>Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To delete a redirect bypass policy entry using a destination IP address:

```bash
configure network redirect bypass ip destination del 192.168.2.1 255.255.255.255
```

To delete a redirect bypass policy entry using a destination network ID:

```bash
configure network redirect bypass ip destination del 192.168.2.0 255.255.255.128
```

**configure network redirect scan ip**

**TABLE A-14. configure network redirect scan ip**

Command family configures a redirect scan policy for the Deep Discovery Web Inspector appliance by specifying an IP address or IP network range.

**Syntax:**

```bash
configure network redirect scan ip
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

**configure network redirect scan ip source add**

**TABLE A-15. configure network redirect scan ip source add**

Add a redirect scan policy by specifying a source IP address or network ID.

**Syntax:**

```bash
configure network redirect scan ip source add <ip> <mask>
```
### View Privileged

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip&gt;</td>
<td>Source IP address or network ID</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To add a new redirect scan policy entry using a source IP address:

```
configure network redirect scan ip source add 10.10.10.150 255.255.255.255
```

To add a new redirect scan policy entry using a source network ID:

```
configure network redirect scan ip source add 10.10.0.0 255.255.255.128
```

### configure network redirect scan ip source del

**TABLE A-16. configure network redirect scan ip source del**

Deletes a redirect scan policy by specifying a source IP address or network ID.

**Syntax:**

```
configure network redirect scan ip source del <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Privileged</td>
</tr>
<tr>
<td>&lt;ip&gt;</td>
<td>Source IP address or network ID</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To delete a redirect scan policy entry using a source IP address:

```
configure network redirect scan ip source del 192.168.1.1 255.255.255.255
```

To delete a redirect scan policy entry using a source network ID:

```
configure network redirect scan ip source del 192.168.1.0 255.255.255.128
```
configure network redirect scan ip destination add

**TABLE A-17. configure network redirect scan ip destination add**

Adds a redirect scan policy by specifying a destination IP address or network ID.

**Syntax:**
```
configure network redirect scan ip destination add <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>&lt;ip&gt;</td>
<td>Destination IP address or network ID</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Network mask</td>
</tr>
</tbody>
</table>

**Example:**

To add a new redirect scan policy entry using a destination IP address:
```
configure network redirect scan ip destination add 10.10.20.150 255.255.255.255
```

To add a new redirect scan policy entry using a destination network ID:
```
configure network redirect scan ip destination add 10.10.20.0 255.255.255.128
```

configure network redirect scan ip destination del

**TABLE A-18. configure network redirect scan ip destination del**

 Deletes a redirect scan policy by specifying a destination IP address or network ID.

**Syntax:**
```
configure network redirect scan ip destination del <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>&lt;ip&gt;</td>
<td>Destination IP address or network ID</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Network mask</td>
</tr>
</tbody>
</table>

**Example:**
To delete a redirect scan policy entry using a destination IP address:

```bash
configure network redirect scan ip destination del 192.168.2.1 255.255.255.255
```

To delete a redirect scan policy entry using a destination network ID:

```bash
configure network redirect scan ip destination del 192.168.2.0 255.255.255.128
```

### configure network redirect scan mac

**TABLE A-19. configure network redirect scan mac**

<table>
<thead>
<tr>
<th>Command family configures a redirect scan policy for the Deep Discovery Web Inspector appliance by specifying a MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network redirect scan mac</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

### configure network redirect scan mac source add

**TABLE A-20. configure network redirect scan mac source add**

<table>
<thead>
<tr>
<th>Adds a redirect scan policy by specifying a source MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network redirect scan mac source add &lt;mac_addr&gt;</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
</tbody>
</table>

**Example:**

To add a new redirect scan policy entry using a source MAC address:

```bash
configure network redirect scan mac source add 02:00:00:00:00:00
```
configure network redirect scan mac source del

**TABLE A-21. configure network redirect scan mac source del**

<table>
<thead>
<tr>
<th>Deletes a redirect scan policy by specifying a source MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network redirect scan mac source del &lt;mac_addr&gt;</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To delete a redirect scan policy entry using a source MAC address:</td>
</tr>
<tr>
<td><code>configure network redirect scan mac source del 02:00:00:00:00:00</code></td>
</tr>
</tbody>
</table>

configure network redirect scan mac destination add

**TABLE A-22. configure network redirect scan mac destination add**

<table>
<thead>
<tr>
<th>Adds a redirect scan policy by specifying a destination MAC address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network redirect scan mac destination add &lt;mac_addr&gt;</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To add a new redirect scan policy entry using a destination MAC address:</td>
</tr>
<tr>
<td><code>configure network redirect scan mac destination add 06:00:00:00:00:00</code></td>
</tr>
</tbody>
</table>

configure network redirect scan mac destination del

**TABLE A-23. configure network redirect scan mac destination del**

<table>
<thead>
<tr>
<th>Deletes a redirect scan policy by specifying a destination MAC address.</th>
</tr>
</thead>
</table>
### Syntax:

```bash
configure network redirect scan mac destination del <mac_addr>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td><code>&lt;mac_addr&gt;</code>: Destination MAC address</td>
</tr>
</tbody>
</table>

**Example:**

To delete a redirect scan policy entry using a destination MAC address:

 ```bash
configure network redirect scan mac destination del 06:00:00:00:00:00
```

---

### configure network redirect check-fdb

#### TABLE A-24. configure network redirect check-fdb

Command family configures whether to check the MAC forwarding table when redirecting traffic for the Deep Discovery Web Inspector appliance.

**Syntax:**

```bash
configure network redirect check-fdb
```

**View**

| Privileged |

---

### configure network redirect check-fdb enable

#### TABLE A-25. configure network redirect check-fdb enable

Enables checking the MAC forwarding table when redirecting traffic.

**Syntax:**

```bash
configure network redirect check-fdb enable
```

**View**

| Privileged |

**Parameters**

| None |

**Example:**

```bash
```
To enable checking the MAC forwarding table when redirecting traffic:

`configure network redirect check-fdb enable`

**configure network redirect check-fdb disable**

<table>
<thead>
<tr>
<th>TABLE A-26. configure network redirect check-fdb disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables checking the MAC forwarding table when redirecting traffic.</td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network redirect check-fdb disable</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To disable checking the MAC forwarding table when redirecting traffic:</td>
</tr>
<tr>
<td><code>configure network redirect check-fdb disable</code></td>
</tr>
</tbody>
</table>

**configure network route**

<table>
<thead>
<tr>
<th>TABLE A-27. configure network route</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command family configures IP routes for the Deep Discovery Web Inspector appliance.</td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure network route</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

**configure network route add ipv4**

<table>
<thead>
<tr>
<th>TABLE A-28. configure network route add ipv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adds a new IPv4 route entry.</td>
</tr>
</tbody>
</table>
**Syntax:**

configure network route add ipv4 <ip_prefixlen> <via> <dev>

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>&lt;ip_prefixlen&gt;: Destination network ID with format IP Address/Prefixlen</td>
<td></td>
</tr>
<tr>
<td>&lt;via&gt;: IPv4 address of the next hop router</td>
<td></td>
</tr>
<tr>
<td>&lt;dev&gt;: Name of the interface to use for the route</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

To add a new IPv4 route entry:

```
configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1
```

**configure network route default ipv4**

**TABLE A-29. configure network route default ipv4**

Configures the IPv4 default gateway for the Deep Discovery Web Inspector appliance.

**Syntax:**

configure network route default ipv4 <gateway> <device>

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td></td>
</tr>
<tr>
<td>&lt;gateway&gt;: IPv4 address of default gateway</td>
<td></td>
</tr>
<tr>
<td>&lt;device&gt;: Name of the interface to use to reach the IPv4 default gateway</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Configures the default route for the Deep Discovery Web Inspector appliance:

```
configure network route default ipv4 192.168.10.1 eth0
```
configure network route del ipv4

**TABLE A-30. configure network route del ipv4**

<table>
<thead>
<tr>
<th>Deletes an IPv4 route entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure network route del ipv4 &lt;ip_prefixlen&gt; &lt;via&gt; &lt;dev&gt;</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To delete an IPv4 route for the Deep Discovery Web Inspector appliance:</td>
</tr>
<tr>
<td>configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1</td>
</tr>
</tbody>
</table>

configure service

**TABLE A-31. configure service**

<table>
<thead>
<tr>
<th>Command family configures system services for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure service</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

configure service ssh disable

**TABLE A-32. configure service ssh disable**

| Disables the SSH service. |
**Syntax:**

`configure service ssh disable`

**View**

Privileged

**Parameters**

None

**Examples:**

To disable the SSH service:

`configure service ssh disable`

---

**configure service ssh enable**

**TABLE A-33. configure service ssh enable**

Enables the SSH service.

**Syntax:**

`configure service ssh enable`

**View**

Privileged

**Parameters**

None

**Examples:**

To enable the SSH service:

`configure service ssh enable`

---

**configure service ssh port**

**TABLE A-34. configure service ssh port**

Configures the TCP port to use for the SSH service.

**Syntax:**

`configure service ssh port <port>`
Using the Command Line Interface

**configure service ntp enable**

**TABLE A-35. configure service ntp enable**

| Enables the NTP service on the Deep Discovery Web Inspector appliance. |
|---|---|
| **Syntax:** |
| configure service ntp enable |
| **View** | Privileged |
| **Parameters** | None |
| **Examples:** |
| To enable the NTP service on the Deep Discovery Web Inspector appliance: |
| configure service ntp enable |

**configure service ntp disable**

**TABLE A-36. configure service ntp disable**

| Disables the NTP service on the Deep Discovery Web Inspector appliance. |
|---|---|
| **Syntax:** |
| configure service ntp disable |
| **View** | Privileged |
| **Parameters** | None |
Examples:

To disable the NTP service on the Deep Discovery Web Inspector appliance:

```
configure service ntp disable
```

---

**configure service ntp server-address**

**TABLE A-37. configure service ntp server-address**

<table>
<thead>
<tr>
<th>Configures the NTP server address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure service ntp server-address &lt;address&gt;</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>&lt;address&gt;: IP address or FQDN of the NTP server</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To configure the NTP server address as 192.168.10.21:</td>
</tr>
<tr>
<td>configure service ntp server-address 192.168.10.21</td>
</tr>
</tbody>
</table>

---

**configure system**

**TABLE A-38. configure system**

<table>
<thead>
<tr>
<th>Command family configures basic system settings for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure system</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
</tbody>
</table>
**configure system date**

**TABLE A-39. configure system date**

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>&lt;date&gt;</td>
<td>Set the date using the following format: <strong>yyyy-mm-dd</strong></td>
</tr>
<tr>
<td>&lt;time&gt;</td>
<td>Set the time with the following format: <strong>hh:mm:ss</strong></td>
</tr>
</tbody>
</table>

**Example:**

To set the date to August 12, 2017 and the time to 3:40 PM:

```bash
configure system date 2017-08-12 15:40:00
```

**configure system password enable**

**TABLE A-40. configure system password enable**

Changing the password can only be performed in Privileged mode.

<table>
<thead>
<tr>
<th>Syntax:</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure system password enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Examples:**

To change the password by entering Privileged mode:

```bash
configure system password enable
```
enable

**TABLE A-41. enable**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Example:**

To enter privileged mode:

`enable`

exit

**TABLE A-42. exit**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal when exiting a session</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Privileged when exiting privileged mode</td>
</tr>
</tbody>
</table>

**Example:**

To exit privileged mode or to exit the session when not in privileged mode:

`exit`
**help**

**TABLE A-43. help**

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays an overview of the Command Line Interface (CLI) help information.</td>
<td>To display the Command Line Interface (CLI) help information: help</td>
</tr>
</tbody>
</table>

**Syntax:**

```
help
```

**View** | Normal

**Parameters** | None

**Example:**

To display the Command Line Interface (CLI) help information:

```
help
```

**history**

**TABLE A-44. history**

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the current session's command line history.</td>
<td>To specify six commands for the size of the history list: history 6</td>
</tr>
</tbody>
</table>

**Syntax:**

```
history [limit]
```

**View** | Normal

**Parameters** | [limit]: Sets the size of the history list for the current session Specifying "0" retains all commands for the session.

**Example:**

To specify six commands for the size of the history list:

```
history 6
```
**logout**

**TABLE A-45. logout**

<table>
<thead>
<tr>
<th>Logs out of the current Command Line Interface (CLI) session.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax: logout</td>
</tr>
<tr>
<td>View</td>
</tr>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td>Example:</td>
</tr>
</tbody>
</table>

**ping**

**TABLE A-46. ping**

<table>
<thead>
<tr>
<th>Pings a specified host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax: ping [num_echos] [interval] &lt;dest&gt;</td>
</tr>
<tr>
<td>View</td>
</tr>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Examples:</td>
</tr>
</tbody>
</table>
To ping the host remote.host.com:

```
ping remote.host.com
```

### reboot

**TABLE A-47. reboot**

<table>
<thead>
<tr>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboots the Deep Discovery Web Inspector appliance immediately or after a specified delay.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

```
reboot [time]
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>[time]: Optional delay in minutes before rebooting the Deep Discovery Web Inspector appliance</th>
</tr>
</thead>
</table>

**Examples:**

- To reboot the Deep Discovery Web Inspector appliance immediately:
  
  ```
  reboot
  ```

- To reboot the Deep Discovery Web Inspector appliance after 5 minutes:
  
  ```
  reboot 5
  ```

### resolve

**TABLE A-48. resolve**

<table>
<thead>
<tr>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolves an IPv4 address on the network.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

```
resolve <dest>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>&lt;dest&gt;: Remote IP address to resolve</th>
</tr>
</thead>
</table>
Examples:

To resolve the host name from IP address 192.168.10.1:

resolve 192.168.10.1

restart service

**TABLE A-49. restart service**

<table>
<thead>
<tr>
<th>Command family</th>
<th>restart service system services for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
<td>restart service</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
</tbody>
</table>

restart service product

**TABLE A-50. restart service product**

<table>
<thead>
<tr>
<th>Restarts the product service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>restart service product</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To restart the product service:</td>
</tr>
<tr>
<td>restart service product</td>
</tr>
</tbody>
</table>
**restart service ssh**

**TABLE A-51. restart service ssh**

<table>
<thead>
<tr>
<th>Restarts the SSH service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>restart service ssh</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To restart the SSH service:</td>
</tr>
<tr>
<td>restart ssh service</td>
</tr>
</tbody>
</table>

**show kernel**

**TABLE A-52. show kernel**

<table>
<thead>
<tr>
<th>Command family displays information about the currently running OS kernel for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show kernel</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Normal</td>
</tr>
</tbody>
</table>

**show kernel iostat**

**TABLE A-53. show kernel iostat**

<table>
<thead>
<tr>
<th>Displays CPU statistics and I/O statistics for devices and partitions for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show kernel iostat</td>
</tr>
</tbody>
</table>
show kernel messages

**TABLE A-54. show kernel messages**

Displays OS kernel messages for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show kernel messages
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Examples:**

To display the OS kernel messages:

```
show kernel messages
```

show kernel modules

**TABLE A-55. show kernel modules**

Displays the loaded OS kernel modules for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show kernel modules
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>
**Examples:**

To display the loaded OS kernel modules:

```
show kernel modules
```

**show kernel parameters**

**TABLE A-56. show kernel parameters**

| Displays the OS kernel parameters for the Deep Discovery Web Inspector appliance. |
| Syntax: show kernel parameters |
| View | Normal |
| Parameters | None |

**Examples:**

To display the OS kernel parameters:

```
show kernel parameters
```

**show memory**

**TABLE A-57. show memory**

| Command family displays the memory statistics for the Deep Discovery Web Inspector appliance. |
| Syntax: show memory |
| View | Normal |
### show memory statistic

**TABLE A-58. show memory statistic**

<table>
<thead>
<tr>
<th>Displays system memory statistics for the Deep Discovery Web Inspector.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>show memory statistic</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the system memory statistics:</td>
</tr>
<tr>
<td><code>show memory statistic</code></td>
</tr>
</tbody>
</table>

### show memory vm

**TABLE A-59. show memory vm**

<table>
<thead>
<tr>
<th>Displays virtual memory statistics for the Deep Discovery Web Inspector.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>show memory vm</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the virtual memory statistics:</td>
</tr>
<tr>
<td><code>show memory vm</code></td>
</tr>
</tbody>
</table>
show network

<table>
<thead>
<tr>
<th>TABLE A-60. show network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command family displays various Deep Discovery Web Inspector network information.</td>
</tr>
<tr>
<td><strong>Syntax:</strong> show network</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

show network arp

<table>
<thead>
<tr>
<th>TABLE A-61. show network arp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the value returned from the Address Resolution Protocol (ARP) table for the given IP address.</td>
</tr>
<tr>
<td><strong>Syntax:</strong> show network arp &lt;dest&gt;</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong> To display the ARP information for the address 10.2.23.41:</td>
</tr>
<tr>
<td>show network arp 10.2.23.41</td>
</tr>
</tbody>
</table>

show network bypass

<table>
<thead>
<tr>
<th>TABLE A-62. show network bypass</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the current bypass mode for the Deep Discovery Web Inspector appliance.</td>
</tr>
<tr>
<td><strong>Syntax:</strong> show network bypass</td>
</tr>
</tbody>
</table>
show network connections

**TABLE A-63. show network connections**

Displays the current network connections for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show network connections
```

**View** | Normal
---|---
**Parameters** | None

**Examples:**

To display the current network connections of the Deep Discovery Web Inspector appliance:

```
show network connections
```

show network dns

**TABLE A-64. show network dns**

Displays the DNS IPv4 configuration for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show network dns
```

**View** | Normal
**Parameters** | None
--- | ---

**Examples:**

To display the IPv4 DNS configuration:

`show network dns`

### show network hostname

**TABLE A-65. show network hostname**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the host name of the Deep Discovery Web Inspector appliance.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show network hostname</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
<tr>
<td>To display the host name of the Deep Discovery Web Inspector appliance:</td>
<td></td>
</tr>
<tr>
<td><code>show network hostname</code></td>
<td></td>
</tr>
</tbody>
</table>

### show network interface

**TABLE A-66. show network interface**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the network interface status and configuration for the Deep Discovery Web Inspector appliance.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show network interface</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
</tbody>
</table>
To display the network interface status and configuration:

```
show network interface
```

**show network redirect**

**TABLE A-67. show network redirect**

<table>
<thead>
<tr>
<th>Displays the current redirect policy for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show network redirect</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the current redirect policy for the Deep Discovery Web Inspector appliance:</td>
</tr>
<tr>
<td>show network redirect</td>
</tr>
</tbody>
</table>

**show network route**

**TABLE A-68. show network route**

<table>
<thead>
<tr>
<th>Displays the IP address route table for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show network route</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the IP address route table:</td>
</tr>
<tr>
<td>show network route</td>
</tr>
</tbody>
</table>
show network route default ipv4

**TABLE A-69. show network route default ipv4**

| Displays the default IPv4 gateway for the Deep Discovery Web Inspector appliance. |

**Syntax:**

```
show network route default ipv4
```

**View** | Normal
---|---

**Parameters** | None
---|---

**Examples:**

To display system default IPv4 gateway:

```
show network route default ipv4
```

show network route ipv4

**TABLE A-70. show network route ipv4**

| Displays the IPv4 route table for the Deep Discovery Web Inspector appliance. |

**Syntax:**

```
show network route ipv4
```

| View | Normal |
---|---|

**Parameters** | None
---|---|

**Examples:**

To display system IPv4 route table:

```
show network route ipv4
```
show process

**TABLE A-71. show process**

Command family displays information about currently running processes on the Deep Discovery Web Inspector appliance.

The parent command displays the status of the processes that are currently running.

**Syntax:**

```
show process [target]
```

**View**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>target: Optionally specify a process name or ID; wildcards are supported</th>
</tr>
</thead>
</table>

**Examples:**

To display the status of the processes that are currently running:

```
show process
```

**show process ltrace**

**TABLE A-72. show process ltrace**

Traces library calls of running processes.

**Syntax:**

```
show process ltrace [pid]
```

**View**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>pid: The process ID number (pid)</th>
</tr>
</thead>
</table>

**Examples:**

To display the library call of process 1233:

```
show process ltrace 1233
```
show process stack

**TABLE A-73. show process stack**

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prints a stack trace of a running process.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td>show process stack [pid]</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>pid: The process ID number (pid)</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
<tr>
<td>To display the stack trace of process 1233:</td>
<td>show process stack 1233</td>
</tr>
</tbody>
</table>

show process top

**TABLE A-74. show process top**

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays information about the top currently running processes. The processes with the most activity are at the top.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td>show process top</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
<tr>
<td>To display the status of the top processes that are currently running:</td>
<td>show process top</td>
</tr>
</tbody>
</table>
show process trace

**TABLE A-75. show process trace**

<table>
<thead>
<tr>
<th>Traces system calls and signals.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> show process trace [pid]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong> To display the system calls and signals of process 1233: show process trace 1233</td>
</tr>
</tbody>
</table>

show kernel

**TABLE A-76. show product-info**

<table>
<thead>
<tr>
<th>Command family displays information about product settings for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> show product-info</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

show product-info management-port

**TABLE A-77. show product-info management-port**

<table>
<thead>
<tr>
<th>Displays the management port's IP address and subnet mask for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> show product-info management-port</td>
</tr>
</tbody>
</table>
show product-info operation-mode

**TABLE A-78. show product-info operation-mode**

Displays the operation mode for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th>Syntax:</th>
<th>show product-info operation-mode</th>
</tr>
</thead>
</table>

**View** | Normal
---|---
**Parameters** | None

**Examples:**

To display the operation mode:

show product-info operation-mode

---

show product-info service-status

**TABLE A-79. show product-info service-status**

Displays the status of services for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th>Syntax:</th>
<th>show product-info service-status</th>
</tr>
</thead>
</table>

**View** | Normal
---|---
**Parameters** | None
Examples:

To display the status of services:

```
show product-info service-status
```

### show product-info version

#### TABLE A-80. show product-info version

<table>
<thead>
<tr>
<th>Displays the product version for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax:</td>
</tr>
<tr>
<td><code>show product-info version</code></td>
</tr>
<tr>
<td>View</td>
</tr>
<tr>
<td>Parameters</td>
</tr>
</tbody>
</table>

Examples:

To display the product version:

```
show product-info version
```

### show service

#### TABLE A-81. show service

<table>
<thead>
<tr>
<th>Command family displays the status and configuration information for Deep Discovery Web Inspector appliance services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax:</td>
</tr>
<tr>
<td><code>show service</code></td>
</tr>
<tr>
<td>View</td>
</tr>
</tbody>
</table>
**show service ntp**

**TABLE A-82. show service ntp**

<table>
<thead>
<tr>
<th>Displays information about whether the NTP service is enabled and running for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
</table>

**Syntax:**

```
show service ntp
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Examples:**

To display the NTP service status:

```
show service ntp
```

**show service ntp enabled**

**TABLE A-83. show service ntp enabled**

<table>
<thead>
<tr>
<th>Displays information about whether the NTP service is enabled.</th>
</tr>
</thead>
</table>

**Syntax:**

```
show service ntp enabled
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Examples:**

To display whether the NTP service is enabled:

```
show service ntp enabled
```
show service ntp server-address

**TABLE A-84. show service ntp server-address**

<table>
<thead>
<tr>
<th>Displays the IP address for the NTP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> show service ntp server-address</td>
</tr>
<tr>
<td><strong>View</strong> Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong> None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the IP address of the NTP server: show service ntp server-address</td>
</tr>
</tbody>
</table>

show service ssh

**TABLE A-85. show service ssh**

<table>
<thead>
<tr>
<th>Displays information about whether the SSH service is enabled and running and, if enabled, what the listening port is for the service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> show service ssh</td>
</tr>
<tr>
<td><strong>View</strong> Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong> None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the SSH status: show service ssh</td>
</tr>
</tbody>
</table>
show storage statistic

**TABLE A-86. show storage statistic**

<table>
<thead>
<tr>
<th>Displays statistics for file system disk space usage for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show storage statistic [partition]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To display the file system disk space usage for the Deep Discovery Web Inspector appliance:</td>
</tr>
<tr>
<td>show storage statistic</td>
</tr>
</tbody>
</table>

show system

**TABLE A-87. show system**

<table>
<thead>
<tr>
<th>Command family displays system information for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>show system</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
</tbody>
</table>

show system date

**TABLE A-88. show system date**

<table>
<thead>
<tr>
<th>Displays the current date and time for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
</table>
Syntax:
```
show system date
```

View | Normal
---|---
Parameters | None

Examples:
To display the current date and time of the Deep Discovery Web Inspector appliance:
```
show system date
```

**show system timezone**

**TABLE A-89. show system timezone**

<table>
<thead>
<tr>
<th>Displays the timezone settings for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>show system timezone</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To display the timezone settings:</td>
</tr>
<tr>
<td><code>show system timezone</code></td>
</tr>
</tbody>
</table>

**show system timezone city**

**TABLE A-90. show system timezone city**

<table>
<thead>
<tr>
<th>Displays the city configured in the timezone settings for the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>show system timezone city</code></td>
</tr>
</tbody>
</table>
**show system timezone continent**

**TABLE A-91. show system timezone continent**

Displays the continent configured in the timezone settings for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show system timezone continent
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Examples:**

To display the continent configured in the timezone settings for the Deep Discovery Web Inspector appliance:

```
show system timezone continent
```

**show system timezone country**

**TABLE A-92. show system timezone country**

Displays the country configured in the timezone settings for the Deep Discovery Web Inspector appliance.

**Syntax:**

```
show system timezone country
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>
show system uptime

**TABLE A-93. show system uptime**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None</th>
</tr>
</thead>
</table>

**Examples:**

To display how long Deep Discovery Web Inspector has been running:

```
show system uptime
```

show system version

**TABLE A-94. show system version**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None</th>
</tr>
</thead>
</table>

**Examples:**

To display the version number for the Deep Discovery Web Inspector appliance:

```
show system version
```
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None</th>
</tr>
</thead>
</table>

### Examples:

To display the version number of the Deep Discovery Web Inspector appliance:

```shell
classic
table A-95. shutdown
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>[time]: Optional delay in minutes before shutting down the Deep Discovery Web Inspector appliance</th>
</tr>
</thead>
</table>

**shutdown**

**Syntax:**

```shell
classic
table A-95. shutdown
```

```shell
shutdown [time]
```

**View**

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

**Examples:**

To shut down the Deep Discovery Web Inspector appliance immediately:

```shell
classic
table A-95. shutdown
```

```shell
shutdown
```

To shut down the Deep Discovery Web Inspector appliance after a 5 minute delay:

```shell
classic
table A-95. shutdown
```

```shell
shutdown 5
```

### start service

**Syntax:**

```shell
classic
table A-95. shutdown
```

```shell
start service
```

**View**

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None</th>
</tr>
</thead>
</table>

**Examples:**

Command family starts system services for the Deep Discovery Web Inspector appliance.
## start service product

### TABLE A-97. start service product

<table>
<thead>
<tr>
<th>Starts the product service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>start service product</code></td>
</tr>
<tr>
<td><strong>View</strong>:</td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong>:</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To start the product service:</td>
</tr>
<tr>
<td><code>start service product</code></td>
</tr>
</tbody>
</table>

## start service ssh

### TABLE A-98. start service ssh

<table>
<thead>
<tr>
<th>Starts the SSH service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>start service ssh</code></td>
</tr>
<tr>
<td><strong>View</strong>:</td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong>:</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
To start the SSH service:

```
start ssh service
```

**stop process**

**TABLE A-99. stop process**

<table>
<thead>
<tr>
<th>Stops a running process on the Deep Discovery Web Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> stop process [target]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To stop a process with ID 33:</td>
</tr>
<tr>
<td>stop process 33</td>
</tr>
</tbody>
</table>

**stop process core**

**TABLE A-100. stop process core**

<table>
<thead>
<tr>
<th>Stops a running process on the Deep Discovery Web Inspector appliance and generates a core file.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> stop process core [target]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>
To stop a process with ID 33 and generate a core file:

```
stop process core 33
```

### stop service

**TABLE A-101. stop service**

Command family stops system services for the Deep Discovery Web Inspector appliance.

<table>
<thead>
<tr>
<th>Syntax:</th>
<th>stop service</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Privileged</td>
</tr>
</tbody>
</table>

### stop service product

**TABLE A-102. stop service product**

Stops the product service.

<table>
<thead>
<tr>
<th>Syntax:</th>
<th>stop service product</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Privileged</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

**Example:**

To stop the product service:

```
stop service product
```
**stop service ssh**

**TABLE A-103. stop service ssh**

<table>
<thead>
<tr>
<th>Stops the SSH service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>stop service ssh</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To stop the SSH service:</td>
</tr>
<tr>
<td>stop ssh service</td>
</tr>
</tbody>
</table>

**traceroute**

**TABLE A-104. traceroute**

<table>
<thead>
<tr>
<th>Displays the route a packet takes to a specified destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>traceroute [hops] &lt;dest&gt; [-n]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>[hops]: Specifies the maximum number of hops to the destination</td>
</tr>
<tr>
<td>The minimum number of hops to specify is 6. The default is 30</td>
</tr>
<tr>
<td>hops.</td>
</tr>
<tr>
<td>&lt;dest&gt;: Specifies the host name or IP address of the remote</td>
</tr>
<tr>
<td>system to trace</td>
</tr>
<tr>
<td>[-n]: Do not resolve a host name</td>
</tr>
<tr>
<td>Examples:</td>
</tr>
<tr>
<td>To display the route to IP address 172.10.10.1 with a maximum of 30 hops:</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>traceroute 172.10.10.1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>To display the route to IP address 172.10.10.1 with a maximum of 20 hops:</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>traceroute 20 172.10.10.1</td>
</tr>
</tbody>
</table>
Appendix B

SNMP Object Identifiers

Topics include:

• SNMP Query Objects on page B-2
• SNMP Traps on page B-6
• SNMP Registration Objects on page B-12
SNMP Query Objects

**TABLE B-1. productVersion**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.1.1</td>
</tr>
<tr>
<td>Object name</td>
<td>productVersion</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the Deep Discovery Web Inspector version.</td>
</tr>
</tbody>
</table>

**TABLE B-2. productBuild**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>productBuild</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the Deep Discovery Web Inspector build number.</td>
</tr>
</tbody>
</table>

**TABLE B-3. Product hotfix**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.1.3</td>
</tr>
<tr>
<td>Object name</td>
<td>productHotfix</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the Deep Discovery Web Inspector hotfix number.</td>
</tr>
</tbody>
</table>

**TABLE B-4. patternIndex**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.2.1.1</td>
</tr>
<tr>
<td>Object name</td>
<td>patternIndex</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the pattern index.</td>
</tr>
</tbody>
</table>
### TABLE B-5. patternID

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.2.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>patternID</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the pattern ID.</td>
</tr>
</tbody>
</table>

### TABLE B-6. patternName

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.2.1.3</td>
</tr>
<tr>
<td>Object name</td>
<td>patternName</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the pattern name.</td>
</tr>
</tbody>
</table>

### TABLE B-7. patternVersion

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.2.1.4</td>
</tr>
<tr>
<td>Object name</td>
<td>patternVersion</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the pattern version.</td>
</tr>
</tbody>
</table>

### TABLE B-8. virtualAnalyzerQueue

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.3.1</td>
</tr>
<tr>
<td>Object name</td>
<td>virtualAnalyzerQueue</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the Virtual Analyzer queue number.</td>
</tr>
</tbody>
</table>

### TABLE B-9. ifIndex

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.4.1.1</td>
</tr>
</tbody>
</table>
### TABLE B-10. ifIndex

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>ifIndex</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the interface index.</td>
</tr>
</tbody>
</table>

### TABLE B-11. ifDescr

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.4.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>ifDescr</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the interface description.</td>
</tr>
</tbody>
</table>

### TABLE B-12. ifReceiveThroughput

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.4.1.3</td>
</tr>
<tr>
<td>Object name</td>
<td>ifReceiveThroughput</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the interface receiving throughput.</td>
</tr>
</tbody>
</table>

### TABLE B-13. ifTransmitThroughput

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.1.4.1.4</td>
</tr>
<tr>
<td>Object name</td>
<td>ifTransmitThroughput</td>
</tr>
<tr>
<td>Description</td>
<td>Returns the interface transmitting throughput.</td>
</tr>
</tbody>
</table>

### TABLE B-13. hwMonitorNumber

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.1</td>
</tr>
<tr>
<td>Object name</td>
<td>hwMonitorNumber</td>
</tr>
<tr>
<td>Description</td>
<td>Count of number of conceptual rows in hwMonitorTable</td>
</tr>
</tbody>
</table>
### Table B-14. hwMonitorLastChange

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>hwMonitorLastChange</td>
</tr>
<tr>
<td>Description</td>
<td>The value of system time when a conceptual row was added or deleted from this table</td>
</tr>
</tbody>
</table>

### Table B-15. hwMonitorIndex

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.3.1.1</td>
</tr>
<tr>
<td>Object name</td>
<td>hwMonitorIndex</td>
</tr>
<tr>
<td>Description</td>
<td>A unique identifier that does not persist across management restarts</td>
</tr>
</tbody>
</table>

### Table B-16. tmSubsystemType

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.3.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>tmSubsystemType</td>
</tr>
<tr>
<td>Description</td>
<td>Hardware component reporting environmental state</td>
</tr>
</tbody>
</table>

### Table B-17. tmHardwareStatus

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.3.1.3</td>
</tr>
<tr>
<td>Object name</td>
<td>tmHardwareStatus</td>
</tr>
<tr>
<td>Description</td>
<td>Last reported state of this component</td>
</tr>
</tbody>
</table>
TABLE B-18. tmMonitorDescription

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.3.1.4</td>
</tr>
<tr>
<td>Object name</td>
<td>tmMonitorDescription</td>
</tr>
<tr>
<td>Description</td>
<td>Human readable description of this event</td>
</tr>
</tbody>
</table>

TABLE B-19. tmHardwareTime

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.3.1.3.1.5</td>
</tr>
<tr>
<td>Object name</td>
<td>tmHardwareTime</td>
</tr>
<tr>
<td>Description</td>
<td>Value of system time when tmHardwareStatus was obtained</td>
</tr>
</tbody>
</table>

SNMP Traps

TABLE B-20. updateSuccessNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.1</td>
</tr>
<tr>
<td>Object name</td>
<td>updateSuccessNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that a component update or roll back was successful.</td>
</tr>
</tbody>
</table>

TABLE B-21. updateFailedNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.2</td>
</tr>
<tr>
<td>Object name</td>
<td>updateFailedNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that a component update or roll back was unsuccessful.</td>
</tr>
</tbody>
</table>
### Table B-22. cpuUsageNotification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.3</td>
</tr>
<tr>
<td>Object name</td>
<td>cpuUsageNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the CPU usage level has reached the maximum threshold.</td>
</tr>
</tbody>
</table>

### Table B-23. memUsageNotification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.4</td>
</tr>
<tr>
<td>Object name</td>
<td>memUsageNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the memory usage level has reached the maximum threshold.</td>
</tr>
</tbody>
</table>

### Table B-24. diskSpaceNotification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.5</td>
</tr>
<tr>
<td>Object name</td>
<td>diskSpaceNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the available disk space is less than the minimum threshold.</td>
</tr>
</tbody>
</table>

### Table B-25. serviceStoppedNotification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.6</td>
</tr>
<tr>
<td>Object name</td>
<td>serviceStoppedNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that a service has stopped and cannot be restarted.</td>
</tr>
</tbody>
</table>
### Table B-26. atpDetectNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.7</td>
</tr>
<tr>
<td>Object name</td>
<td>atpDetectNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the number of advanced threat detections on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### Table B-27. ransomwareDetectNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.8</td>
</tr>
<tr>
<td>Object name</td>
<td>ransomwareDetectNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the number of ransomware detections on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### Table B-28. cccDetectNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.9</td>
</tr>
<tr>
<td>Object name</td>
<td>cccDetectNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the number of C&amp;C callbacks on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### Table B-29. licenseExpireNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.10</td>
</tr>
<tr>
<td>Object name</td>
<td>licenseExpireNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that the product license is about to expire or has expired.</td>
</tr>
</tbody>
</table>
TABLE B-30. ntpFailedNotification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.0.11</td>
</tr>
<tr>
<td>Object name</td>
<td>ntpFailedNotification</td>
</tr>
<tr>
<td>Description</td>
<td>Notification to indicate that time synchronization with an NTP server is not successful.</td>
</tr>
</tbody>
</table>

TABLE B-31. updateSuccessMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.1</td>
</tr>
<tr>
<td>Object name</td>
<td>updateSuccessMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that a component update or roll back was successful.</td>
</tr>
</tbody>
</table>

TABLE B-32. updateFailedMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.2</td>
</tr>
<tr>
<td>Object name</td>
<td>updateFailedMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that a component update or roll back was unsuccessful.</td>
</tr>
</tbody>
</table>

TABLE B-33. cpuUsageMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.3</td>
</tr>
<tr>
<td>Object name</td>
<td>cpuUsageMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the CPU usage level has reached the maximum threshold.</td>
</tr>
<tr>
<td>TABLE B-34. memUsageMsg</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>ITEM</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.4</td>
</tr>
<tr>
<td>Object name</td>
<td>memUsageMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the memory usage level has reached the maximum threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE B-35. diskSpaceMsg</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITEM</strong></td>
</tr>
<tr>
<td>OID</td>
</tr>
<tr>
<td>Object name</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE B-36. serviceStoppedMsg</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITEM</strong></td>
</tr>
<tr>
<td>OID</td>
</tr>
<tr>
<td>Object name</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE B-37. atpDetectMsg</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITEM</strong></td>
</tr>
<tr>
<td>OID</td>
</tr>
<tr>
<td>Object name</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>
### TABLE B-38. ransomwareDetectMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.8</td>
</tr>
<tr>
<td>Object name</td>
<td>ransomwareDetectMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the number of ransomware detections on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### TABLE B-39. cccDetectMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.9</td>
</tr>
<tr>
<td>Object name</td>
<td>cccDetectMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the number of C&amp;C callbacks on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### TABLE B-40. licenseExpireMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.10</td>
</tr>
<tr>
<td>Object name</td>
<td>licenseExpireMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the product license is about to expire or has expired.</td>
</tr>
</tbody>
</table>

### TABLE B-41. ntpFailedMsg

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.11</td>
</tr>
<tr>
<td>Object name</td>
<td>ntpFailedMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that time synchronization with an NTP server is not successful.</td>
</tr>
</tbody>
</table>
### Table B-42. coinMinersDetectMsg

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.6101.3006.2.1.12</td>
</tr>
<tr>
<td>Object name</td>
<td>coinMinersDetectMsg</td>
</tr>
<tr>
<td>Description</td>
<td>Message to indicate that the number of coin miner detections on hosts in the specified network groups reaches the threshold during the specified time period.</td>
</tr>
</tbody>
</table>

### SNMP Registration Objects

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.2021</td>
<td>UC Davis</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.6101</td>
<td>Trend Micro, Inc.</td>
</tr>
<tr>
<td>.1.3.6.1.6.3.1.1.5.1</td>
<td>SNMPv2-MIB MIB</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.8072</td>
<td>NET-SNMP-AGENT-MIB</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.6101.999</td>
<td>TMCM</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.6101.3001</td>
<td>TMTM</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.6101.3006</td>
<td>Deep Discovery Web Inspector</td>
</tr>
</tbody>
</table>
Index

A
about
Deep Discovery Web Inspector
product information, 9-72
Maintenance Agreement, 10-2
viewing firmware version, API key, 9-72
viewing product information, 9-72
accessing
Command Line Interface, A-2
deployment wizard, 9-2
management console, 3-5
using the CLI to configure
management console, 3-2
access logs
sending to a syslog server, 9-29
access sylogs
benefits, sending to a syslog server, 1-5
accounts, 9-69. See also local user accounts
adding, 9-69
adding for console access, 9-69
adding local user, 9-69
administration, 9-67
editing, 9-70
managing, 9-68
role-based access, 9-67
role classifications, 9-68
using for console access, 9-67
activating
product licenses, 10-5
activating license
during deployment, 3-6
activation code
finding in license description, 10-2
requirements, 2-8
activation codes
for licenses, 10-1
adding
accounts, 9-69
approved/blocked list, 7-19, 7-21
bypass/redirect policy entries, 9-58
domain objects, 7-17, 7-18
HTTPS inspection rules, 7-8, 7-11
local user accounts, 9-69
network objects, 7-16, 7-17
policies, 7-3, 7-6
static routes, 9-15, 9-16
widgets to tabs, 5-16
admin
default account, 9-68
administration, 9-1, 9-10, 9-64, 9-65, 9-70
accounts, adding accounts, 9-69
accounts, adding local user accounts, 9-69
accounts, editing accounts or changing passwords on accounts, 9-70
accounts, managing accounts, 9-68
accounts, role classifications, 9-68
accounts / contacts, overview, 9-67
admin account, 9-70
back up settings, 9-64, 9-65
components, 9-10
components updates, rolling back updates, 9-10
component updates, 9-7
component updates, list of components, 9-7
component updates, scheduling updates, 9-7
component updates, updating components, 9-9
deployment wizard, 9-2
deployment wizard, accessing, 9-2
deployment wizard, configuring forward proxy mode, 9-2
deployment wizard, configuring transparent bridge mode, 9-5
hotfix upgrades, 9-12
integrated products/services, 9-25
integrated products/services, adding a detection syslog server, 9-30
integrated products/services, configuring threat intelligence sharing settings, 9-28
integrated products/services, Control Manager, 1-10
integrated products/services, Control Manager overview, 9-25
integrated products/services, Control Manager tasks, 9-26
integrated products/services, log settings, 9-25, 9-29, 9-30
integrated products/services, registering Control Manager, 9-27
integrated products/services, threat intelligence sharing overview, 9-28
integrated products/services, unregistering Control Manager, 9-28
licenses, activating product licenses, 10-5
licenses, managing product licenses, 10-5
licenses, product license description, 10-2
licenses, product license statuses, 10-3
licenses, viewing product licenses, 10-4
managing contacts, 9-71
product updates, hotfixes and patches overview, 9-11
product upgrades, 9-12
product upgrades, firmware upgrades, 9-12
product upgrades, managing patches, 9-12
reasons to perform backups, 9-62
restore settings, 9-64, 9-65
system maintenance, 9-50, 9-51
system maintenance, backing up or restoring a configuration, 9-62
system maintenance, bypass/redirect policy priorities and precedence, 9-57
system maintenance, configuring bypass/redirect policies, 9-56
system maintenance, configuring bypass policies, 9-61
system maintenance, configuring debug log level, 9-52
system maintenance, configuring redirect policies, 9-59
system maintenance, enabling/disabling bypass mode, 9-56
system maintenance, exporting and downloading debug files, 9-52
system maintenance, exporting debug or error logs, 9-51
system maintenance, network packet capture, 9-54, 9-55
system maintenance, network services diagnostics, 9-53
system maintenance, storage log deletion settings, 9-51, 9-56
system maintenance, storage
maintenance settings, 9-51
system maintenance, testing network
connections, 9-53
system settings, 9-14
system settings, adding static routes, 9-16
system settings, configuring network
settings, 9-14
system settings, configuring proxy
settings, 9-17
system settings, configuring system
time, 9-19
system settings, managing static routes, 9-15
system settings, notification SMTP
server, 9-18
unable to restore settings, 9-64, 9-65
Virtual Analyzer, 9-39
Virtual Analyzer, configuring network
collections for, 9-47
Virtual Analyzer, deleting images, 9-47
Virtual Analyzer, image preparation
overview, 9-43
Virtual Analyzer, image status and
information, 9-41
Virtual Analyzer, importing images, 9-44
Virtual Analyzer, importing images
from HTTP or FTP server, 9-46
Virtual Analyzer, importing images
from local source, 9-44
Virtual Analyzer, modifying instances, 9-47
Virtual Analyzer, network types, 9-49
Virtual Analyzer, overall statuses, 9-41
Virtual Analyzer, suspicious object
scanning overview, 9-40, 9-41
Virtual Analyzer, viewing status, 9-42
administrator accounts
role, 9-68
admin menu
changing passwords, 3-6, 9-71
advanced detection
benefits of, 1-3
advanced filter list
detected by, 6-5
advanced filters
detected by, field in list of, 6-5
advanced persistent threats
attach sequence, 1-5
information about, 1-5
protection against, 1-5
advanced search filters
detections, 6-9
advanced threat detections in specified
network groups
critical alerts, 8-3
parameters for alert, 8-6
Advanced Threat Indicators
widget, 5-4
advanced threats
Advanced Threat Indicators widget, 5-4
Advanced Threat Scan Engine, 1-9
about, 1-9
aggregating
suspicious objects using Control
Manager, 9-25
agreement
maintenance, 10-1
alert rules
configuring alert notifications, 8-5
modifying, 8-5
overview, 8-2
alerts, 8-1
  adding contacts for receiving, 9-71
  configuring alert notifications, 8-5
  contacts for receiving, 9-67
  critical alerts, 8-2, 8-3
  informational and important alerts, 8-2, 8-4
  managing triggered, 8-2
  notification parameters, 8-6
  notification parameters for critical, 8-6
  notification parameters for important and informational alerts, 8-14
overview, 8-2
  viewing, deleting, or exporting triggered, 8-2
  viewing triggered, 8-2
Anti-Botnet
  detected by, 6-5
anti-malware (ATSE)
  detected by, 6-5
anti-malware (SAL)
  detected by, 6-5
anti-malware (SIE)
  detected by, 6-5
appliance
  setting up for deployment, 3-2
approved/blocked list
  adding, 7-21
  managing, 7-19
  viewing, adding, editing, importing, exporting, 7-19
approved list
  URLs, 7-20
APT, 1-5. See also advanced persistent threats
ATSE, 1-9, 9-8
  about, 1-9
attacker, 1-6
B
backup, 9-64, 9-65
backups
  creating to restore configuration or replicate settings across devices, 9-62
bandwidth
  Bandwidth Status widget, 5-10
Bandwidth Status
  widget, 5-10
basic search filters
  detections, 6-8
benefits
  advanced detection, 1-3
  description of, 1-2
  easy-to-use policy management, 1-2
  flexible deployment, 1-2
  HTTP/2 scanning, 1-4
  HTTPS inspection, 1-4
  patient zero protection, 1-4
  real-time visibility, analysis, action, 1-2
  send access syslogs to a syslog server, 1-5
  Virtual Analyzer sandbox analysis, 1-4
blocked list
  URLs, 7-20
blocked URLs
  detected by, 6-5
Bot Pattern, 9-8
browsers
  supported, 2-4, 2-8
  supported for deployment, 2-4
bypass
  policies, configuring, 9-61
bypass/redirect policies
  viewing, adding, editing, importing/exporting, deleting entries, 9-58
bypass mode
  enabling or disabling, 9-56
bypass policies
  configuring, 9-56, 9-61
  managing, 9-58
  priorities and precedence, 9-57

C
C&C, 1-6
C&C Callback Detections Over Time
  widget, 5-5
C&C callbacks
  C&C Callback Detections Over Time
    widget, 5-5
  threat indicator, 6-4
C&C callbacks detected in specified network groups
  critical alerts, 8-3
  parameters for alert, 8-6
cables
  requirements, 2-8
callback, 1-6
capture. See network packet capture
capturing
  network packet captures, 9-55
changing
  passwords, 3-6, 9-71
changing passwords
  on accounts, 9-70
classifications
  account role, 9-69
  detected by, 6-5
CLI, A-1. See also Command Line Interface

coin miners detected in specified network groups
  parameters for alert, 8-6
command-and-control, 1-6
command line interface
  entering the shell environment, A-3
  using to configure management console access, 3-2
Command Line Interface
  accessing, A-2
  using the, A-1
components
  list of updateable, 9-7
  rolling back, 9-10
  updates, 9-10
  updating, 9-9
components updates
  rolling back updates, 9-10
component update or rollback failed
  important alerts, 8-4
  parameters for alert, 8-14
component updates
  administration, 9-7
  list of updateable components, 9-7
  updating components, 9-9
configuration settings
  backup or restore, 9-62
configuring
  debug log levels, 9-52
  forward proxy mode using deployment wizard, 3-8, 9-2
  management console access, 3-2
  network settings, 9-14
  notification SMTP servers, 9-18
  NTP servers, 9-19
  proxy settings, 9-17
system time, 9-19
threat intelligence sharing settings, 9-28
transparent bridge mode using
deployment wizard, 3-11, 9-5
using the management console, 3-5
configuring actions
  policies, 7-6
connections
  Connection Status widget, 5-9
connection status
  Control Manager, 9-26
Connection Status
  widget, 5-9
considerations
  pre-deployment, 2-2
console access
  adding accounts for, 9-69
  using accounts for, 9-67
console navigation, 4-1
contacts
  adding for notifications alerts, and
  reports, 9-71
  administration, 9-67
  for receiving alerts and reports, 9-67
  managing, 9-71
  using for scheduled reports, 8-20
Control Manager
  checking connection status, 9-26
  consideration when used with threat
  intelligence sharing, 9-28
  managing tasks, 9-26
  overview, 1-10, 9-25
  preparing for deployment, 2-9
  registering, 9-27
  support for synchronizing suspicious
  objects, 9-25
  synchronize suspicious objects, 9-26
  unregistering, 9-28
  what functionality is integrated, 1-10
CPU usage
  Hardware Status widget, 5-8
creating
  backups for restoring configuration or
to replicate settings across devices, 9-62
critical alerts
  configuring notifications for, 8-5
  default alert frequency, 8-3
  default criteria, 8-3
  information about, 8-3
  names of, 8-3
  notification parameters for, 8-6
  overview, 8-2
  viewing triggered alerts, 8-2
cryptography
  SSL, 7-9
  TLS, 7-9
CSR
  generating for HTTPS inspection rules,
  7-8, 7-14
custom network
  configuring for Virtual Analyzer
  network connections, 9-47
  Virtual Analyzer network type, 9-49
D
dashboard, 5-1
  adding widgets, 5-16
  dashboard
    tabs, 5-2
  default tabs, 5-3
  default view, 5-3
  list of widgets, 5-15
  managing tabs, 5-13
managing widgets, 5-17, 5-18
overview, 5-2
System Status tab, 5-8
System Status tab, Bandwidth Status
widget, 5-10
System Status tab, Connection Status
widget, 5-9
System Status tab, Hardware Status
widget, 5-8
System Status tab, Traffic Status widget,
5-9
tabs, 5-12
Threat Monitoring tab, 5-3
Threat Monitoring tab, Advanced
Threat Indicators widget, 5-4
Threat Monitoring tab, C&C Callback
Detections Over Time widget, 5-5
Threat Monitoring tab, Ransomware
Detections Over Time widget, 5-6
Threat Monitoring tab, Top Affected
Hosts widget, 5-6
Threat Monitoring tab, Top Detected
URLs widget, 5-7
Threat Monitoring tab, Virtual
Analyzer Sandbox Analysis widget, 5-7
Virtual Analyzer Status tab, Virtual
Analyzer Average Processing Time
widget, 5-11
Virtual Analyzer Status tab, Virtual
Analyzer Queue widget, 5-12
Virtual Analyzer tab, 5-10
Virtual Analyzer tab, Suspicious
Objects from Virtual Analyzer widget,
5-11
widgets, 5-2
manually setting, 9-19
date
debbug files
exporting and downloading, 9-52
debbug log levels
configuring, 9-52
debbug logs
exporting, 9-51
Deep Discovery Malware Pattern, 9-8
Deep Discovery Trusted Certificate
Authorities, 9-8
default
dashboard view, 5-3
widgets displayed in predefined tabs,
5-15
default account
admin, 9-68
default policy
how it works, 7-5
overview, 7-5
what you can and cannot do with, 7-5
delete admin accounts, 9-70
deleting
bypass/redirect policies, 9-58
static routes, 9-15
triggered alerts, 8-2
Virtual Analyzer images, 9-47
deleting, editing, adding
accounts, 9-68
deploying (enabling)
static routes, 9-15
deployment, 3-1
activating the license, 3-6
benefits of flexible, 1-2
browser and system requirements, 2-4
Control Manager, 2-9
deployment mode overview, 2-2
enabling and starting SSH service, 2-5
forward proxy mode, 2-3
initial configuration of forward proxy mode, 3-8
initial configuration of transparent bridge mode, 3-11
items to prepare, 2-9
opening the management console, 3-5
ports used by appliance, 2-6
recommended network environment, 2-4
setting up the appliance, 3-2
setting up the hardware, 3-2
tasks to perform before, 2-2
transparent bridge mode, 2-3
using CLI to configure management console access, 3-2
using the deployment wizard, 3-8
deployment mode
forward proxy, 2-3
transparent bridge, 2-3
deployment modes
ports used for each mode, 9-14
deployment wizard
accessing, 9-2
accessing and configuring deployments using the, 9-2
configuring forward proxy mode, 9-2
configuring transparent bridge mode, 9-5
initial configuration of forward proxy mode, 3-8
initial configuration of transparent bridge mode, 3-11
performing initial deployment, 3-8
detected by advanced filter, 6-5
classifications, 6-5
classifications for detection, 6-4
detection, 6-2
detection details
investigating, 6-11
list of, 6-12
detection logs
sending to a syslog server, 9-29
detections, 6-1
advanced filters, detected by, 6-5
advanced search filters, 6-9
basic search filters, 6-8
detected by classifications, 6-4
investigating details about, 6-11
list of detection details, 6-12
overview about viewing, 6-7
overview about viewing suspicious objects, 6-18
risk levels, 6-2
suspicious domain objects, 6-19
suspicious file objects, 6-21
suspicious IP address objects, 6-18
suspicious URL objects, 6-20
threat indicator classifications, 6-4
threat indicators, 6-4
viewing all, 6-7
viewing file, 6-16
viewing for affected hosts, 6-13
viewing URL, 6-14
Virtual Analyzer risk levels, 6-3
detection syslog servers
adding, 9-30
diagnostics
system maintenance, network services
diagnostics, 9-53
disabling
  bypass mode, 9-56
disk usage
  Hardware Status widget, 5-8
documentation feedback, 11-6
domain objects
  how used in policies, 7-3
  managing, 7-17
  viewing, adding, editing, removing, importing, exporting, 7-17
domains
  suspicious objects found by Virtual Analyzer, 6-19
download and view
  threat intelligence data file, 9-28
Download Center
  downloading firmware, 9-12
  downloading patches and hotfixes, 9-12
  URL, 9-12
downloader, 1-6
downloading
  debug files, 9-52
  network packet captures, 9-55
  patches and hotfixes, 9-12
duplicating
  HTTPS inspection rules, 7-8
  policies, 7-3
E
edit admin account, 9-70
editing
  accounts, 9-70
  approved/blocked list, 7-19
  bypass/redirect policies, 9-58
  domain objects, 7-17, 7-18
  HTTPS inspection rules, 7-8, 7-11
  network objects, 7-16, 7-17
  notifications, 7-22, 7-26
enabling
  bypass mode, 9-56
enabling and starting
  SSH service, 2-5
enabling or disabling
  HTTPS inspection rules, 7-8
  policies, 7-6
enabling Patient Zero Protection
  policies, 7-6
entering
  Command Line Interface, A-2
error logs
  exporting, 9-51
Ethernet cables
  requirements, 2-8
exfiltrate, 1-6
expiration date
  finding in license description, 10-2
exporting
  approved/blocked list, 7-19
  bypass/redirect policies, 9-58
  debug files, 9-52
  domain objects, 7-17
  network objects, 7-16
  triggered alerts, 8-2
export settings, 9-64
F
features
  advanced detection, 1-3
  description of, 1-2
  easy-to-use policy management, 1-2
  flexible deployment, 1-2
  HTTP/2 scanning, 1-4
  HTTPS inspection, 1-4
  patient zero protection, 1-4
real-time visibility, analysis, action, 1-2
send access syslogs to a syslog server, 1-5
Virtual Analyzer sandbox analysis, 1-4
files
  suspicious objects found by Virtual Analyzer, 6-21
  viewing detections, 6-16
file types
  how used in policies, 7-3
  policies, list when creating, 7-3
firmware
  downloading and updating, 9-12
forward proxy
  deployment mode, topology overview, 2-2
  mode overview, 2-3
forward proxy mode
  accessing the deployment wizard to deploy, 9-2
  configuring using deployment wizard, 9-2
  initial configuration using deployment wizard, 3-8
  initial configuration using the deployment wizard, 3-8
  using the deployment wizard to deploy, 9-2
FTP servers
  importing Virtual Analyzer images from, 9-46
G
  generating
    CSR for HTTPS inspection rules, 7-8, 7-14
    on-demand reports, 8-21
getting started, 4-1
  console navigation, 4-1
  getting started tasks, 4-1
  opening the management console, 3-5
tasks, 4-2
H
  hardware
    Hardware Status widget, 5-8
    setting up for deployment, 3-2
  Hardware Status
    widget, 5-8
  high CPU usage
    important alerts, 8-4
    parameters for alert, 8-14
  high memory usage
    important alerts, 8-4
    parameters for alert, 8-14
  hosts
    Top Affected Hosts widget, 5-6
    viewing detections for affected, 6-13
  hotfixes
    managing, 9-12
    product upgrades, 9-12
  hot fixes
    overview, 9-11
  HTTP/2 scanning
    benefits, 1-4
  HTTP inspection rules
    generating an CSR for, 7-14
  HTTP servers
    importing Virtual Analyzer images from, 9-46
  HTTPS inspection
    benefits and features, 1-4
    overview, 7-2, 7-9
  HTTPS inspection rules
managing, 7-8
viewing, 7-10
viewing, adding, editing, duplicating, removing, ordering, creating CSR file for, 7-8

I
image import tool
Virtual Analyzer, using to import from local source, 9-44
image preparation
Virtual Analyzer, overview of, 9-43
image preparation tool
Virtual Analyzer, overview of, 9-43
images
viewing status for Virtual Analyzer, 9-42
Virtual Analyzer, deleting, 9-47
Virtual Analyzer, importing, 9-44
Virtual Analyzer, importing from HTTP or FTP server, 9-46
Virtual Analyzer, importing from local source, 9-44
Virtual Analyzer, names of, 9-41
Virtual Analyzer scanning using, 9-40
important alerts
configuring notifications for, 8-5
default alert frequency, 8-4
default criteria, 8-4
information about, 8-4
names of, 8-4
notification parameters for, 8-14
overview, 8-2
viewing triggered alerts, 8-2
importing
approved/blocked list, 7-19
bypass/redirect policies, 9-58
domain objects, 7-17

network objects, 7-16
Virtual Analyzer images, 9-44
Virtual Analyzer images from HTTP or FTP server, 9-46
Virtual Analyzer images from local source, 9-44
importing certificates
HTTP inspection rules, 7-11
import settings, 9-65
informational alerts
configuring notifications for, 8-5
default alert frequency, 8-4
default criteria, 8-4
information about, 8-4
names of, 8-4
notification parameters for, 8-14
overview, 8-2
viewing triggered alerts, 8-2
initial deployment
using the deployment wizard, 3-8
inspection
overview of HTTPS, 7-9
inspection rules
viewing HTTPS, 7-10
installation
getting started, 4-1
installing
firmware upgrades, 9-12
patches and hotfixes, 9-12
instances
number deployed for Virtual Analyzer images, 9-41
Virtual Analyzer, modifying, 9-47
integrated products/services
adding a detection syslog server, 9-30
administration of, 9-25
configuring threat intelligence sharing settings, 9-28
Control Manager, managing tasks, 9-26
Control Manager, overview, 1-10
Control Manager overview, 9-25
log settings, configuring a detection syslog server, 9-30
registering Control Manager, 9-27
threat intelligence sharing overview, 9-28
unregistering Control Manager, 9-28
IntelliTrap Exception Pattern, 9-8
IntelliTrap Pattern, 9-8
introduction, 1-1
Deep Discovery Web Inspector, 1-2
new threat landscapes, 1-5
investigating
details about a detection, 6-11
IP addresses
requirements, 2-8
suspicious objects found by Virtual Analyzer, 6-18
L
license
activating during deployment, 3-6
license expiration
critical alerts, 8-3
parameters for alert, 8-6
licenses
activating product, 10-5
activation codes, 10-1
maintaining, 10-1
maintenance agreement, 10-1
managing product, 10-5
product license description, 10-2
product license statuses, 10-3
viewing product, 10-4
license type and seats
finding in license description, 10-2
list
approved/blocked, 7-20
of license statuses, 10-3
of notification message tokens, 7-23
of user notifications, 7-22
local or network folders
importing Virtual Analyzer images from, 9-44
local user accounts
adding for console access, 9-69
logs
configuring log deletion settings for storage maintenance, 9-51
exporting debug or error, 9-51
log settings
configuring for detection syslog server, 9-30
to send access logs to a syslog server, 9-29
to send detection violation logs to a syslog server, 9-29
low free disk space
important alerts, 8-4
parameters for alert, 8-14
M
maintenance
agreement, 10-1
for licensed products, 10-1
maintenance agreement, 9-72
product licenses, 9-72
storage, configuring log deletion settings, 9-51
maintenance agreement, 9-72
Maintenance Agreement
about, 10-2
expiration, 10-2
renewal, 10-2
management
Virtual Analyzer, 9-39
management console
navigation, 4-2
opening the, 3-5
using the CLI to configure, 3-2
management network
configuring for Virtual Analyzer
network connections, 9-47
Virtual Analyzer network type, 9-49
management port, 9-14
managing
accounts, 9-68
approved/blocked list, 7-19
bypass/redirect policies, 9-58
contacts, 9-71
Control Manager tasks, 9-26
dashboard tabs, 5-13
dashboard widgets, 5-17, 5-18
domain objects, 7-17
HTTPS inspection rules, 7-8
network objects, 7-16
notifications, 7-22, 7-26
policies, 7-3
product licenses, 10-5
static routes, 9-15
triggered alerts, 8-2
user-defined settings, 7-15
using the management console, 3-5
memory usage
Hardware Status widget, 5-8
modifying
alert rules, 8-5
policies, 7-3
Virtual Analyzer instances, 9-47

N
navigating
management console, 4-2
network
services diagnostics, system
maintenance, 9-53
network connections
configuring for Virtual Analyzer, 9-47
Network Content Correlation Pattern, 9-8
Network Content Inspection Engine (Linux, User mode, 64-bit), 9-8
Network Content Inspection Pattern, 9-8
network environment
recommended, 2-4
network is down
critical alerts, 8-3
parameters for alert, 8-6
network is up
important alerts, 8-4
parameters for alert, 8-14
network objects
how used in policies, 7-3
managing, 7-16
viewing, adding, editing, importing/exporting, removing, 7-16
network packet capture
system maintenance, 9-54
network packet captures
capturing and downloading, 9-55
network services diagnostics
system maintenance, 9-53
network setting
ports used for each deployment mode, 9-14
network settings configuring, 9-14
network topology
forward proxy mode, 2-3
overview of deployment modes, 2-2
transparent bridge mode, 2-3
network types
Virtual Analyzer, 9-49
Virtual Analyzer, custom network, management network, no access, 9-49
no access Virtual Analyzer network type, 9-49
no network access configuring for Virtual Analyzer network connections, 9-47
notifications
adding contacts for receiving, 9-71
configuring for alert rules, 8-5
configuring SMTP server for, 9-18
editing, 7-26
list of message tokens, 7-23
list of user, 7-22
managing, 7-22
parameters for alert, 8-6
parameters for critical alerts, 8-6
parameters for important and informational alerts, 8-14
viewing and editing, 7-22
NTP servers configuring, 9-19

O
objects
investigating detection details about, 6-11
list of detection details, 6-12
on demand reports, 8-21
on-demand reports, 8-20
opening management console, 3-5
operator accounts role, 9-68
ordering HTTPS inspection rules, 7-8
policies, 7-3
other detected by, 6-5
overall statuses, Virtual Analyzer, 9-41
overview about viewing detections, 6-7
Control Manager, 9-25
Deep Discovery Web Inspector, 1-2
default policy, 7-5
detection risk levels, 6-2
domain objects, 7-18
features and benefits, 1-2
hotfixes and patches, 9-11
how patient zero protection works, 7-4
HTTPS inspection, 7-9
network objects, 7-16
policies, 7-2, 7-3
threat intelligence sharing, 9-28
viewing suspicious objects, 6-18
Virtual Analyzer, image preparation, 9-43

P
packet capture. See network packet capture
parameters
  critical alerts, 8-6
  for alert notifications, 8-6
  for important and informational alerts, 8-14
passwords
  changing, 3-6, 9-71
  changing when editing account settings, 9-70
patches
  managing, 9-12
  overview, 9-11
  product upgrades, 9-12
patient zero. See patient zero protection
patient zero protection
  benefits of, 1-4
  definition, 1-4
  how it works, 7-4
  sandbox analysis, how it works with, 7-4
  Virtual Analyzer, how it works with, 7-4
policies
  adding, 7-6
  adding, viewing, modifying, duplicating, removing, and ordering, 7-3
  benefit of enabling patient zero protection, 1-4
  bypass/redirect, priorities and precedence, 9-57
  configuring bypass, 9-61
  configuring bypass/redirect, 9-56
  configuring redirect, 9-59
  default policy, 7-3, 7-5
  enabling or disabling, 7-3, 7-6
  enabling Patient Zero Protection, 7-6
  how they work, 7-3
  managing, 7-3
  managing bypass/redirect, 9-58
  overview, 7-2
  viewing, 7-5
  what it means to enable patient zero protection, 7-4
  what you can do from the policy menu, 7-2
policy
  overview, 7-2
policy management
  benefits of easy-to-use, 1-2
policy rules. See policies
ports, 2-6
  used by appliance, 2-6
  used for each deployment mode, 9-14
pre-deployment
  browser and system requirements, 2-4
  considerations, 2-2
  Control Manager, 2-9
  deployment mode overview, 2-2
  enabling and starting SSH service, 2-5
  items to prepare, 2-9
  ports used by appliance, 2-6
  recommended network environment, 2-4
  tasks, 2-2
Predictive Machine Learning
  detected by, 6-5
Predictive Machine Learning Pattern, 9-8
Predictive Web Pre-Filter Pattern, 9-9
preparing
  for deployment, Control Manager, 2-9
  for deployment, ports used by appliance, 2-6
preparing for deployment, 2-1
product
license description, 10-2
license statuses, 10-3
product license, 9-72
product updates
  hotfixes and patches overview, 9-11
product upgrades
  managing patches, 9-12
  updating firmware, 9-12
protocols
  Bandwidth Status widget, 5-10
  Connection Status widget, 5-9
  Traffic Status widget, 5-9
proxy setting
  what is affected by, 9-17
proxy settings
  configuring, 9-17
Q
queue
  Virtual Analyzer Queue widget, 5-12
R
ransomware
  Ransomware Detections Over Time widget, 5-6
  threat indicator, 6-4
ransomware detected in specified network groups
  critical alerts, 8-3
  parameters for alert, 8-6
RAT, 1-6
recipients
  for on-demand reports, 8-21
  for scheduled reports, 8-20
  managing, 9-71
recommendations
  network environment, 2-4
resetting
  notifications to default, 7-22
redirect
  policies, configuring, 9-59
redirect policies
  configuring, 9-56, 9-59
  managing, 9-58
  priorities and precedence, 9-57
registering
  Control Manager, 9-27
removing
  domain objects, 7-17
  HTTPS inspection rules, 7-8
  network objects, 7-16
  policies, 7-3
replicate settings
  across devices using backups, 9-62
reports, 8-1
  adding contacts for receiving, 9-71
  contacts for receiving, 9-67
  on demand, 8-21
  on-demand reports, 8-20
  scheduled reports, 8-20
  scheduling, 8-20
  time intervals for scheduled reports, 8-20
required tasks
  you must perform to get started, 4-2
requirements
  deployment, 2-4
  enabling and starting SSH service, 2-5
  pre-deployment, 2-9
  SSH access, 2-4
restore, 9-64, 9-65
restoring configuration
using backups, 9-62
risk levels, 6-2
how assessed, 6-2
overview, 6-2
Virtual Analyzer, 6-3
role-based access
adding accounts for, 9-69
roles
classifications for accounts, 9-69
rollback
components, 9-10
rolling back
hotfixes and patches, 9-12

S
sandbox analysis
benefits of, 1-4
sandbox images
viewing status for Virtual Analyzer, 9-42
Virtual Analyzer, deleting, 9-47
Virtual Analyzer, importing, 9-44
Virtual Analyzer, importing from
HTTP or FTP server, 9-46
Virtual Analyzer, importing from local
source, 9-44
Virtual Analyzer, names of, 9-41
Virtual Analyzer, preparation of, 9-43
Virtual Analyzer scanning using, 9-40
scanning
suspicous objects by Virtual Analyzer,
9-40, 9-41
scheduled reports, 8-20
scheduling, 8-20
schedule updates, 9-10
scheduling
reports, 8-20
Script Analyzer Pattern, 9-9
search filters
detections, advanced, 6-9
detections, basic, 6-8
security patches
overview, 9-11
selecting decryption categories
HTTP inspection rules, 7-11
selecting decryption domain objects
HTTP inspection rules, 7-11
selecting decryption network objects
HTTP inspection rules, 7-11
selecting file types
policies, 7-6
selecting network and domain objects
policies, 7-6
services
affected by proxy settings, 9-17
service stopped/abnormal
critical alerts, 8-3
parameters for alert, 8-6
settings
managing user-defined, 7-15
setting up
hardware for deployment, 3-2
shell environment, A-3
smart protection, 1-10
Web Reputation Services, 1-10
Smart Scan Agent Pattern, 9-9
SMTP
notification server, configuring, 9-18
Spyware/Grayware Pattern, 9-9
SSH
enabling and starting service, 2-5
requirements for access using, 2-4
SSH service
enabling and starting, 2-5
starting
  SSH service, 2-5
static routes
  adding, 9-16
  adding, deploying (enabling), viewing, or deleting, 9-15
  managing, 9-15
statuses
  license, 10-3
  Virtual Analyzer, for each image, 9-41
  Virtual Analyzer, list of overall, 9-41
  Virtual Analyzer, viewing, 9-42
storage logs
  configuring for deletion settings for, 9-51
storage maintenance
  configuring log deletion settings, 9-51
support
  resolve issues faster, 11-4
suspicious
  domain objects, 6-19
suspicious documents
  threat indicator, 6-4
suspicious file
  objects, 6-21
suspicious IP address
  objects, 6-18
suspicious malware
  threat indicator, 6-4
suspicious objects
  Control Manager support for
    synchronizing, 9-25
    domains, 6-19
    file, 6-21
    investigating detection details, 6-11
    IP addresses, 6-18
    list of detection details, 6-12
    overview about viewing, 6-18
    patient zero protection with Virtual Analyzer, 7-4
    Suspicious Objects from Virtual Analyzer widget, 5-11
    synchronize with Control Manager, 9-26
    URLs, 6-20
    Virtual Analyzer scanning of, 9-40, 9-41
  suspicious objects analysis (Virtual Analyzer) detected by, 6-5
  suspicious objects filtering (Virtual Analyzer) detected by, 6-5
  Suspicious Objects from Virtual Analyzer widget, 5-11
  suspicious scripts
    threat indicator, 6-4
  suspicious URL
    objects, 6-20
    threat indicator, 6-4
  synchronize
    suspicious objects using Control Manager, 9-26
syslog server
  sending access logs to a, 9-29
  sending detection violation logs to a, 9-29
syslog servers
  adding detection, 9-30
system maintenance
  administration, 9-50
  backing up or restoring a configuration, 9-62
  bypass/redirect policy priorities and precedence, 9-57
configuring bypass/redirect policies, 9-56
configuring bypass policies, 9-61
configuring debug log levels, 9-52
configuring redirect policies, 9-59
configuring storage log deletion settings, 9-51
enabling/disabling bypass mode, 9-56
exporting and downloading debug files, 9-52
exporting debug or error logs, 9-51
network packet capture, 9-54, 9-55
network services diagnostics, 9-53
testing network connections, 9-53
system requirements
deployment, 2-4
enabling and starting SSH service, 2-5
pre-deployment, 2-9
system settings
adding static routes, 9-16
configuring network settings, 9-14
configuring notification SMTP server, 9-18
configuring proxy settings, 9-17
configuring system time, 9-19
list of what is configured in, 9-14
managing static routes, 9-15
System Status
dashboard tab, 5-8
System Status tab
Bandwidth Status widget, 5-10
Connection Status widget, 5-9
Hardware Status widget, 5-8
Traffic Status widget, 5-9
system time
configuring, 9-19

T

tab
System Status, 5-8
Threat Monitoring, 5-3
Virtual Analyzer, 5-10
tabs, 5-12
adding widgets to, 5-16
settings, 5-13
System Status tab, 5-3
tasks, 5-13
Threat Monitoring tab, 5-3
Virtual Analyzer tab, 5-3
tasks
additional, you must perform to get started, 4-2
getting started, 4-2
pre-deployment, 2-2
tabs, 5-13
testing connections. See network service diagnostics
testing network connections. See network service diagnostics
threat indicators
classifications for detection, 6-4
detection, 6-4
threat intelligence data file
download and view, 9-28
threat intelligence sharing
consideration when used with Control Manager, 9-28
overview, 9-28
threat intelligence sharing settings
configuring, 9-28
threat landscapes
introduction, 1-5
Threat Monitoring
dashboard tab, 5-3

Threat Monitoring tab
  Advanced Threat Indicators widget, 5-4
  C&C Callback Detections Over Time widget, 5-5
  Ransomware Detections Over Time widget, 5-6
  Top Affected Hosts widget, 5-6
  Top Detected URLs widget, 5-7
  Virtual Analyzer Sandbox Analysis widget, 5-7

initial configuration using the deployment wizard, 3-8
using the deployment wizard to deploy, 9-2

triggered alerts
  managing, 8-2
  overview, 8-2
  viewing, 8-2
  viewing, deleting, or exporting, 8-2

true file type
detected by, 6-5

U
unregistering
  Control Manager, 9-28
untrusted server certificate
detected by, 6-5

update/rollback successfully completed
  informational alerts, 8-4
  parameters for alert, 8-14

updateable components
  list of, 9-7

updating
  components, 9-9
  firmware, 9-12

URL filtering
detected by, 6-5

URL Filtering Engine, 9-9

URLs
  suspicious objects found by Virtual Analyzer, 6-20
  Top Detected URLs widget, 5-7
  viewing detections, 6-14

user
  notifications, list of, 7-22

user defined settings
  overview, 7-2

time
  manually setting, 9-19

timezone
  configuring, 9-19

tokens
  notification, list of, 7-23

Top Affected Hosts
  widget, 5-6

Top Detected URLs
  widget, 5-7

Traffic Status
  widget, 5-9

transparent bridge
  deployment mode, topology overview, 2-2
  mode overview, 2-3

transparent bridge mode
  accessing the deployment wizard to deploy, 9-2
  configuring using deployment wizard, 9-5
  initial configuration using deployment wizard, 3-11
user-defined settings
  managing, 7-15
  managing approved/blocked list, 7-15
  managing domain objects, 7-15
  managing network objects, 7-15
  managing notifications, 7-15

user notifications
  list of, 7-22
  list of message tokens, 7-23
  using
    Command Line Interface, A-1

utilization
  Virtual Analyzer images, 9-41

V
  version
    finding in license description, 10-2
  viewing
    all detections, 6-7
    all detections with filters, 6-7
    approved/blocked list, 7-19
    bypass/redirect policies, 9-58
    detections for affected hosts, 6-13
    detections for files, 6-16
    detections for URLs, 6-14
    detection viewing overview, 6-7
    domain objects, 7-17
    HTTPS inspection rules, 7-8, 7-10
    information about CA used to resign, 7-10
    network objects, 7-16
    notifications, 7-22
    policies, 7-3, 7-5
    product information, 9-72
    product licenses, 10-4
    suspicious objects, overview, 6-18
    triggered alerts, 8-2

Virtual Analyzer status, 9-42
violation logs
  sending to a syslog server, 9-29
Virtual Analyzer
  administration, 9-39
  benefit of enabling patient zero protection, 1-4
  benefits of sandbox analysis, 1-4
  configuring network settings for, 9-47
  dashboard tab, 5-10
  deleting images, 9-47
  detections of suspicious objects, 6-18
  image preparation overview, 9-43
  image status and information, 9-41
  importing images, 9-44
  importing images from HTTP or FTP server, 9-46
  importing images from local source, 9-44
  management, 9-39
  modifying instances, 9-47
  network types, 9-49
  overall statuses, 9-41
  patient zero protection during sandbox analysis, 7-4
  risk levels, 6-3
  suspicious domain objects found by, 6-19
  suspicious file objects found by, 6-21
  suspicious IP address objects found by, 6-18
  suspicious object scanning overview, 9-40, 9-41
  suspicious URL objects found by, 6-20
  viewing image information, 9-42
  viewing status, 9-42
Virtual Analyzer Average Processing Time widget, 5-11
Virtual Analyzer Queue widget, 5-12
Virtual Analyzer Sandbox Analysis widget, 5-7
Virtual Analyzer Average Processing Time widget, 5-11
Virtual Analyzer Configuration Pattern, 9-9
Virtual Analyzer Queue widget, 5-12
Virtual Analyzer Sandbox Analysis widget, 5-7
Virtual Analyzer Sensors, 9-9
Virtual Analyzer Status tab
Suspicious Objects from Virtual Analyze widget, 5-11
Virtual Analyzer Average Processing Time widget, 5-11
Virtual Analyzer Queue widget, 5-12
VSAPI, 9-8

W
web reputation, 1-10
web reputation service detected by, 6-5
widgets, 5-15, 5-17, 5-18
adding to tabs, 5-16
Advanced Threat Indicators widget, 5-4
Bandwidth Status widget, 5-10
C&C Callback Detections Over Time widget, 5-5
Connection Status widget, 5-9
displayed by default, 5-15
Hardware Status widget, 5-8
in System Status tab, 5-8
in Threat Monitoring tab, 5-3
in Virtual Analyzer tab, 5-10
list of, 5-15
managing, 5-17, 5-18
Ransomware Detections Over Time, 5-6
Ransomware Detections Over Time widget, 5-6
Suspicious Objects from Virtual Analyzer widget, 5-11
system status
Bandwidth Status, 5-10
Traffic Status, 5-9
System Status tab
Connection Status widget, 5-9
Hardware Status widget, 5-8
tasks you can perform on, 5-17, 5-18
Threat Monitoring tab
Advanced Threat Indicators widget, 5-4
C&C Callback Detections Over Time widget, 5-5
Ransomware Detections Over Time widget, 5-6
Top Affected Hosts widget, 5-6
Top Detected URLs widget, 5-7
Virtual Analyzer Sandbox Analysis widget, 5-7
Top Affected Hosts widget, 5-6
Top Detected URLs widget, 5-7
Traffic Status widget, 5-9
Virtual Analyzer Average Processing Time widget, 5-11
Virtual Analyzer Queue widget, 5-12
Virtual Analyzer Sandbox Analysis widget, 5-7
Virtual Analyzer Status tab
Suspicious Objects from Virtual Analyzer widget, 5-11
Virtual Analyzer Average Processing Time widget, 5-11
Virtual Analyzer Queue widget, 5-12