



# 5.1 TREND MICRO™ Deep Discovery™ Email Inspector Administrator's Guide

Advanced Protection Against Targeted Email Threats



Endpoint Security



Network Security



Protected Cloud



---

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

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

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

Copyright © 2022. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM59194/210115

Release Date: January 2022

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

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

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

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

Evaluate this documentation on the following site:

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

## **Privacy and Personal Data Collection Disclosure**

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

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

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

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

<https://www.trendmicro.com/privacy>

# Table of Contents

## **Preface**

|                            |   |
|----------------------------|---|
| Preface .....              | 1 |
| Documentation .....        | 2 |
| Audience .....             | 3 |
| Document Conventions ..... | 3 |
| About Trend Micro .....    | 4 |

## **Chapter 1: Introduction**

|  |      |
|--|------|
| About Deep Discovery Email Inspector ..... | 1-2  |
| What's New .....                           | 1-2  |
| Features and Benefits .....                | 1-5  |
| A New Threat Landscape .....               | 1-10 |
| A New Solution .....                       | 1-12 |

## **Chapter 2: Getting Started**

|   |     |
|---|-----|
| Getting Started Tasks .....                                 | 2-2 |
| Requirements to Access Deep Discovery Email Inspector ..... | 2-4 |
| Configuring Management Console Access .....                 | 2-5 |
| The Management Console .....                                | 2-7 |
| Logging On Using Local Accounts .....                       | 2-8 |
| Logging On With Single Sign-On .....                        | 2-8 |
| Management Console Navigation .....                         | 2-9 |

## **Chapter 3: Dashboard**

|                          |     |
|--------------------------|-----|
| Dashboard Overview ..... | 3-2 |
| Tabs .....               | 3-2 |
| Predefined Tabs .....    | 3-2 |
| Tab Tasks .....          | 3-3 |

|  |      |
|--|------|
| New Tab Window .....                                 | 3-3  |
| Widgets .....  | 3-4  |
| Adding Widgets to the Dashboard .....                | 3-4  |
| Widget Tasks .....                                   | 3-5  |
| Overview .....                                       | 3-6  |
| Detection Summary Widget .....                       | 3-7  |
| Sender Filtering/Authentication Widget .....         | 3-7  |
| Quarantined Messages Widget .....                    | 3-8  |
| Top Policy Violations Widget .....                   | 3-8  |
| Message Queues Widget .....                          | 3-8  |
| Processed Messages Widget .....                      | 3-8  |
| Threat Monitoring .....                              | 3-9  |
| Attack Sources Widget .....                          | 3-9  |
| High-Risk Messages Widget .....                      | 3-10 |
| Detected Messages Widget .....                       | 3-10 |
| Advanced Threat Indicators .....                     | 3-11 |
| Time-of-Click Protection Widget .....                | 3-11 |
| Top Trends .....                                     | 3-12 |
| Top Attachment Names Widget .....                    | 3-12 |
| Top Attachment Types Widget .....                    | 3-12 |
| Top Affected Recipients Widget .....                 | 3-12 |
| Top Attack Sources Widget .....                      | 3-13 |
| Top Callback Hosts from Virtual Analyzer Widget ...  | 3-14 |
| Top Callback URLs from Virtual Analyzer Widget ....  | 3-14 |
| Top Email Subjects Widget .....                      | 3-15 |
| System Status .....                                  | 3-15 |
| Processing Volume Widget .....                       | 3-15 |
| Hardware Status Widget .....                         | 3-16 |
| Virtual Analyzer .....                               | 3-16 |
| Messages Submitted to Virtual Analyzer Widget .....  | 3-16 |
| Average Virtual Analyzer Processing Time Widget ..   | 3-17 |
| Suspicious Objects from Virtual Analyzer Widget .... | 3-17 |

## **Chapter 4: Detections**

|                                   |     |
|-----------------------------------|-----|
| Detected Risk .....               | 4-2 |
| Threat Type Classifications ..... | 4-5 |

|  |      |
|--|------|
| Exporting Search Results .....                           | 4-6  |
| Detected Messages .....                                  | 4-7  |
| Viewing Detected Messages .....                          | 4-7  |
| Investigating a Detected Message .....                   | 4-12 |
| Viewing Affected Recipients .....                        | 4-15 |
| Viewing Attack Sources .....                             | 4-16 |
| Viewing Senders .....                                    | 4-18 |
| Viewing Email Subjects .....                             | 4-19 |
| Suspicious Objects .....                                 | 4-21 |
| Viewing Suspicious Hosts .....                           | 4-21 |
| Viewing Suspicious URLs .....                            | 4-22 |
| Viewing Suspicious Files .....                           | 4-23 |
| Viewing Synchronized Suspicious Objects .....            | 4-24 |
| Quarantine .....   | 4-26 |
| Sender Filtering/Authentication .....                    | 4-34 |
| Viewing Sender Filtering/Authentication Detections ..... | 4-35 |

## Chapter 5: Policies

|  |      |
|--|------|
| About Policies .....                       | 5-2  |
| General Message Scanning Order .....       | 5-5  |
| Policy Management Guidelines .....         | 5-6  |
| Policy Actions .....                       | 5-8  |
| Policy Matching .....                      | 5-25 |
| Policy Splintering .....                   | 5-28 |
| Policy List .....                          | 5-30 |
| Configuring a Policy .....                 | 5-31 |
| Policy Rules .....                         | 5-36 |
| Content Filtering Rules .....              | 5-37 |
| Configuring a Content Filtering Rule ..... | 5-38 |
| Scanning Conditions for Attachments .....  | 5-41 |
| Adding Keyword Lists or Expressions .....  | 5-42 |
| Data Loss Prevention (DLP) Rules .....     | 5-43 |
| Configuring a DLP Rule .....               | 5-44 |

|   |      |
|---|------|
| Antispam Rules .....                        | 5-45 |
| Configuring an Antispam Rule .....          | 5-46 |
| Threat Protection Rules .....               | 5-49 |
| Configuring a Threat Protection Rule .....  | 5-50 |
| Policy Objects .....                        | 5-53 |
| Notifications .....                         | 5-54 |
| Configuring Recipient Notification .....    | 5-54 |
| Replacement File .....                      | 5-55 |
| Configuring the Replacement File .....      | 5-56 |
| Message Stamps .....                        | 5-56 |
| Configuring a Message Stamp .....           | 5-57 |
| Redirect Pages .....                        | 5-58 |
| Customizing the Redirect Pages .....        | 5-59 |
| Archive Servers .....                       | 5-60 |
| Configuring an Archive Server .....         | 5-61 |
| Data Identifiers .....                      | 5-62 |
| Expressions .....                           | 5-63 |
| Predefined Expressions .....                | 5-63 |
| Viewing Predefined Expressions .....        | 5-63 |
| Customized Expressions .....                | 5-64 |
| Criteria for Customized Expressions .....   | 5-65 |
| Configuring a Customized Expression .....   | 5-66 |
| Importing Expressions .....                 | 5-67 |
| Exporting Expressions .....                 | 5-68 |
| File Attributes .....                       | 5-68 |
| Predefined File Attributes List .....       | 5-69 |
| Configuring File Attributes .....           | 5-69 |
| Importing File Attributes .....             | 5-71 |
| Exporting File Attributes .....             | 5-71 |
| Keyword Lists .....                         | 5-72 |
| Predefined Keyword Lists .....              | 5-72 |
| Customized Keyword Lists .....              | 5-72 |
| Criteria for Customized Keyword Lists ..... | 5-73 |
| Configuring a Keyword List .....            | 5-74 |
| Importing Keyword Lists .....               | 5-75 |
| Exporting Keyword Lists .....               | 5-75 |

|   |      |
|---|------|
| Data Loss Prevention (DLP) Templates .....      | 5-76 |
| Predefined DLP Templates .....                  | 5-77 |
| Customized DLP Templates .....                  | 5-77 |
| Condition Statements and Logical Operators .... | 5-77 |
| Creating a DLP Template .....                   | 5-78 |
| Importing DLP Templates .....                   | 5-80 |
| Exporting DLP Templates .....                   | 5-80 |
| Address Groups .....                            | 5-81 |
| Configuring an Address Group .....              | 5-82 |
| Policy Exceptions .....                         | 5-83 |
| Configuring Message Exceptions .....            | 5-84 |
| Managing Object Exceptions .....                | 5-85 |
| Adding an Object Exception .....                | 5-87 |
| Importing Object Exceptions .....               | 5-88 |
| Configuring URL Keyword Exceptions .....        | 5-89 |
| Graymail Exceptions .....                       | 5-89 |
| Adding a Graymail Exception .....               | 5-90 |
| Importing Graymail Exceptions .....             | 5-90 |
| Configuring Email Encryption Exceptions .....   | 5-91 |

## **Chapter 6: Alerts and Reports**

|                                       |      |
|---------------------------------------|------|
| Alerts .....                          | 6-2  |
| Critical Alerts .....                 | 6-2  |
| Important Alerts .....                | 6-3  |
| Informational Alerts .....            | 6-5  |
| Configuring Alert Notifications ..... | 6-5  |
| Viewing Triggered Alerts .....        | 6-6  |
| Alert Notification Parameters .....   | 6-7  |
| Reports .....                         | 6-27 |
| Scheduling Reports .....              | 6-28 |
| Generating On-Demand Reports .....    | 6-29 |

## **Chapter 7: Logs**

|                                  |     |
|----------------------------------|-----|
| Time-Based Filters and DST ..... | 7-2 |
|----------------------------------|-----|

|  |      |
|--|------|
| Email Message Tracking .....                 | 7-2  |
| Querying Message Tracking Logs .....         | 7-2  |
| MTA Events .....                             | 7-7  |
| Querying MTA Event Logs .....                | 7-7  |
| System Events .....                          | 7-8  |
| Querying System Event Logs .....             | 7-9  |
| Message Queue Logs .....                     | 7-10 |
| Querying Message Queue Logs .....            | 7-11 |
| Rerouting Messages in Message Queues .....   | 7-13 |
| Email Submission Logs .....                  | 7-14 |
| Querying Email Submission Logs .....         | 7-14 |
| Time-of-Click Protection Logs .....          | 7-15 |
| Querying Time-of-Click Protection Logs ..... | 7-15 |
| Applying Advanced Filters .....              | 7-15 |

## **Chapter 8: Administration**

|                                     |      |
|-------------------------------------|------|
| Component Updates .....             | 8-2  |
| Components .....                    | 8-2  |
| Update Source .....                 | 8-4  |
| Configuring the Update Source ..... | 8-4  |
| Updating Components .....           | 8-5  |
| Rolling Back Components .....       | 8-5  |
| Scheduling Component Updates .....  | 8-6  |
| Product Updates .....               | 8-6  |
| System Updates .....                | 8-6  |
| Managing Patches .....              | 8-7  |
| Upgrading Firmware .....            | 8-8  |
| Scanning / Analysis .....           | 8-9  |
| Email Scanning .....                | 8-10 |
| Virtual Analyzer .....              | 8-11 |
| Virtual Analyzer Overview .....     | 8-11 |
| Virtual Analyzer Statuses .....     | 8-12 |

|  |      |
|--|------|
| Overall Status Table .....                           | 8-12 |
| Virtual Analyzer Images .....                        | 8-13 |
| Virtual Analyzer Image Preparation .....             | 8-13 |
| Importing Virtual Analyzer Images .....              | 8-14 |
| Deleting Virtual Analyzer Images .....               | 8-16 |
| Modifying Instances .....                            | 8-17 |
| Configuring Virtual Analyzer Network and Filters ... | 8-17 |
| Configuring an External Virtual Analyzer .....       | 8-28 |
| Email Submissions .....                              | 8-29 |
| Manually Submitting Email Message Samples .....      | 8-30 |
| URL Scanning .....                                   | 8-31 |
| Disabling URL Scanning .....                         | 8-32 |
| File Passwords .....                                 | 8-32 |
| Smart Protection .....                               | 8-36 |
| About Smart Protection Server .....                  | 8-38 |
| Setting Up Smart Protection Server .....             | 8-38 |
| Configuring Smart Protection Settings .....          | 8-39 |
| Smart Feedback .....                                 | 8-40 |
| Enabling Smart Feedback .....                        | 8-41 |
| YARA Rules .....                                     | 8-42 |
| Creating a YARA Rule File .....                      | 8-42 |
| Adding a YARA Rule File .....                        | 8-44 |
| Editing a YARA Rule File .....                       | 8-45 |
| Deleting a YARA Rule File .....                      | 8-45 |
| Exporting a YARA Rule File .....                     | 8-46 |
| Time-of-Click URL Protection .....                   | 8-46 |
| Configuring Time-of-Click Protection Settings .....  | 8-46 |
| Business Email Compromise .....                      | 8-48 |
| Adding a High-Profile User .....                     | 8-48 |
| Adding an Internal Domain .....                      | 8-49 |
| Adding an Approved Sender .....                      | 8-50 |
| Cousin Domains .....                                 | 8-50 |
| Configuring Cousin Domain Settings .....             | 8-51 |
| Sender Filtering/Authentication Settings .....       | 8-52 |
| Sender Filter Order of Evaluation .....              | 8-54 |
| SMTP Error Codes .....                               | 8-56 |
| Configuring Email Reputation Services .....          | 8-56 |

|   |       |
|---|-------|
| Approved Senders List .....   | 8-57  |
| Adding Approved Senders .....   | 8-59  |
| Importing Approved Senders .....  | 8-61  |
| Blocked Senders List .....  | 8-61  |
| Adding Blocked Senders .....  | 8-64  |
| Importing Blocked Senders .....   | 8-65  |
| Configuring DHA Protection Settings .....                                     | 8-66  |
| Configuring Bounce Attack Protection Settings .....                           | 8-68  |
| Configuring SMTP Traffic Throttling Settings .....                            | 8-70  |
| Sender Policy Framework (SPF) .....   | 8-71  |
| Configuring SPF Settings .....  | 8-72  |
| DomainKeys Identified Mail (DKIM) .....                                       | 8-74  |
| Configuring DKIM Authentication Settings .....                                | 8-74  |
| DKIM Signatures .....   | 8-76  |
| Configuring a DKIM Signature .....  | 8-77  |
| Importing DKIM Signatures .....   | 8-79  |
| Domain-based Message Authentication, Reporting &<br>Conformance (DMARC) ..... | 8-79  |
| Configuring DMARC Settings .....  | 8-80  |
| End-User Quarantine .....   | 8-82  |
| Configuring User Quarantine Access Settings .....                             | 8-82  |
| Adding an SMTP Server for EUQ Authentication ....                             | 8-85  |
| EUQ Digest .....  | 8-86  |
| Inline Action Links .....   | 8-87  |
| Configuring EUQ Digest Settings .....   | 8-87  |
| End-User Quarantine Console .....   | 8-88  |
| Accessing the End-User Quarantine Console .....                               | 8-89  |
| Viewing Quarantined Messages .....  | 8-90  |
| Adding Approved Senders .....   | 8-92  |
| Viewing Quarantined Messages for Distribution Lists ....                      | 8-92  |
| Mail Settings .....   | 8-94  |
| Message Delivery .....  | 8-94  |
| Configuring SMTP Connection Settings .....                                    | 8-95  |
| Configuring Message Delivery Settings .....                                   | 8-98  |
| Configuring Limits and Exceptions .....                                       | 8-101 |

|   |       |
|---|-------|
| Configuring the SMTP Greeting Message .....                                 | 8-105 |
| Edge MTA Relay Servers .....  | 8-105 |
| Configuring Edge MTA Relay Servers .....                                    | 8-106 |
| Internal Domains .....  | 8-107 |
| Adding Internal Domains .....   | 8-107 |
| Importing Internal Domains .....  | 8-108 |
| Address Modification .....  | 8-109 |
| Configuring Address Rewriting .....   | 8-109 |
| Configuring Email Domain Rewriting .....                                    | 8-111 |
| Transport Layer Security (TLS) .....  | 8-112 |
| Deploying Deep Discovery Email Inspector in TLS<br>Environments .....       | 8-112 |
| Prerequisites for Using TLS .....   | 8-113 |
| Obtaining a Digital Certificate .....                                       | 8-113 |
| Configuring TLS Settings .....  | 8-113 |
| Incoming Messages .....   | 8-114 |
| Configuring TLS Settings for Incoming<br>Messages .....                     | 8-114 |
| Importing TLS Settings .....  | 8-116 |
| Outgoing Messages .....   | 8-116 |
| DANE for SMTP .....   | 8-117 |
| Configuring TLS Settings for Outgoing Messages<br>.....                     | 8-121 |
| Importing TLS Settings .....  | 8-123 |
| Integrated Products/Services .....  | 8-123 |
| Integrated Trend Micro Products .....                                       | 8-124 |
| Trend Vision One .....  | 8-124 |
| Integrating Deep Discovery Email Inspector with Trend<br>Vision One .....   | 8-125 |
| Unregistering Deep Discovery Email Inspector from<br>Trend Vision One ..... | 8-127 |
| Apex Central .....  | 8-127 |
| Apex Central Features .....   | 8-128 |
| Apex Central Components .....   | 8-129 |
| Registering to Apex Central .....   | 8-129 |
| Unregistering from Apex Central .....                                       | 8-132 |

|   |       |
|---|-------|
| Deep Discovery Director .....   | 8-132 |
| Deep Discovery Director Registration Considerations ....                    | 8-133 |
| Registering to Deep Discovery Director .....                                | 8-134 |
| Unregistering from Deep Discovery Director .....                            | 8-136 |
| Threat Intelligence Sharing .....   | 8-137 |
| Configuring Threat Intelligence Sharing Settings ..                         | 8-137 |
| Auxiliary Products/Services .....   | 8-138 |
| Trend Micro TippingPoint Security Management System (SMS) .....             | 8-139 |
| Configuring Trend Micro TippingPoint Security Management System (SMS) ..... | 8-139 |
| Check Point Open Platform for Security (OPSEC) ...                          | 8-142 |
| Configuring Check Point Open Platform for Security (OPSEC) .....            | 8-143 |
| Preconfiguring a Security Gateway .....                                     | 8-151 |
| Configuring a Secured Connection .....                                      | 8-153 |
| IBM Security Network Protection .....                                       | 8-157 |
| Configuring IBM Security Network Protection .                               | 8-158 |
| Palo Alto Panorama or Firewalls .....                                       | 8-162 |
| Configuring Palo Alto Panorama and Firewalls                                | 8-162 |
| LDAP .....  | 8-165 |
| Configuring an LDAP Server .....  | 8-166 |
| SAML Integration .....  | 8-168 |
| Service Provider Metadata and Certificate .....                             | 8-169 |
| Configuring Identity Provider Settings .....                                | 8-170 |
| Configuring Okta .....  | 8-170 |
| Configuring Active Directory Federation Services ..                         | 8-173 |
| Configuring Endpoints for Single Sign-on through AD FS .....                | 8-177 |
| Log Settings .....  | 8-178 |
| Adding a Syslog Server .....  | 8-179 |
| Editing Syslog Server Profiles .....  | 8-180 |
| SFTP .....  | 8-181 |
| Email Encryption .....  | 8-182 |
| Registering Domains for Email Encryption .....                              | 8-184 |

|   |       |
|---|-------|
| Configure Default Email Identity for Message Signing .... |       |
| 8-186   |       |
| System Settings .....                                     | 8-187 |
| Network Settings .....                                    | 8-187 |
| Configuring Network Settings .....                        | 8-187 |
| Configuring NIC Teaming .....                             | 8-189 |
| Operation Modes .....                                     | 8-190 |
| Monitoring Rules for SPAN/TAP Mode .....                  | 8-192 |
| Adding a Monitoring Rule .....                            | 8-192 |
| Editing a Monitoring Rule .....                           | 8-193 |
| Deleting a Monitoring Rule .....                          | 8-193 |
| Configuring Proxy Settings .....                          | 8-193 |
| Configuring the Notification SMTP Server .....            | 8-194 |
| Configuring System Time .....                             | 8-197 |
| SNMP .....  | 8-197 |
| Configuring Trap Messages .....                           | 8-198 |
| Configuring Manager Requests .....                        | 8-200 |
| Configuring Session Timeout Setting .....                 | 8-202 |
| Certificate Management .....                              | 8-202 |
| SMTP and HTTPS Certificates .....                         | 8-203 |
| Configuring a Certificate Signing Request .....           | 8-204 |
| Configuring a Self-signed Certificate .....               | 8-205 |
| Importing a Certificate .....                             | 8-206 |
| Exporting a Certificate .....                             | 8-207 |
| Assigning a Certificate .....                             | 8-207 |
| Trusted CA Certificates .....                             | 8-207 |
| Importing Certificates .....                              | 8-208 |
| Configuring Connection Security Settings .....            | 8-209 |
| Accounts / Contacts .....                                 | 8-209 |
| Managing Accounts .....                                   | 8-210 |
| Changing Your Password .....                              | 8-215 |
| SAML Groups .....   | 8-215 |
| Configuring SAML Groups .....                             | 8-216 |
| Managing Contacts .....                                   | 8-217 |
| System Maintenance .....                                  | 8-217 |
| Backing Up or Restoring a Configuration .....             | 8-217 |

|   |       |
|---|-------|
| Configuring Storage Maintenance .....                           | 8-224 |
| Powering Off or Restarting Deep Discovery Email Inspector ..... | 8-226 |
| Debug Logs .....  | 8-226 |
| Exporting Debugging Files .....                                 | 8-226 |
| Configuring Log Level .....                                     | 8-227 |
| Testing Network Connections .....                               | 8-227 |
| Licenses .....  | 8-228 |
| Maintenance Agreement .....                                     | 8-229 |
| Activation Codes .....  | 8-230 |
| Product License Status .....                                    | 8-230 |
| Viewing Your Product License .....                              | 8-231 |
| Activating or Renewing Your Product License .....               | 8-232 |
| About Deep Discovery Email Inspector .....                      | 8-233 |

## **Chapter 9: Technical Support**

|   |     |
|---|-----|
| Troubleshooting Resources .....                 | 9-2 |
| Using the Support Portal .....                  | 9-2 |
| Threat Encyclopedia .....                       | 9-2 |
| Contacting Trend Micro .....                    | 9-3 |
| Speeding Up the Support Call .....              | 9-3 |
| Sending Suspicious Content to Trend Micro ..... | 9-4 |
| Email Reputation Services .....                 | 9-4 |
| File Reputation Services .....                  | 9-4 |
| Web Reputation Services .....                   | 9-5 |
| Other Resources .....                           | 9-5 |
| Download Center .....                           | 9-5 |
| Documentation Feedback .....                    | 9-5 |

## **Appendices**

### **Appendix A: Using the Command Line Interface**

|                     |     |
|---------------------|-----|
| Using the CLI ..... | A-2 |
|---------------------|-----|

|   |      |
|---|------|
| Entering the CLI .....                                | A-2  |
| Command Line Interface Commands .....                 | A-3  |
| Entering Privileged Mode .....                        | A-3  |
| CLI Command Reference .....                           | A-3  |
| configure product management-port .....               | A-4  |
| configure product operation-mode .....                | A-4  |
| configure network basic .....                         | A-5  |
| configure network dns .....                           | A-6  |
| configure network hostname .....                      | A-7  |
| configure network interface .....                     | A-8  |
| configure network teaming reinit .....                | A-8  |
| configure network route add .....                     | A-9  |
| configure network route default .....                 | A-9  |
| configure network route del .....                     | A-10 |
| configure network route del default/default ipv6 .... | A-10 |
| configure service nscd disable .....                  | A-11 |
| configure service nscd enable .....                   | A-11 |
| configure service ssh disable .....                   | A-12 |
| configure service ssh enable .....                    | A-12 |
| configure service ssh port .....                      | A-13 |
| configure service ntp .....                           | A-13 |
| configure system date .....                           | A-14 |
| configure system password enable .....                | A-14 |
| configure system timezone .....                       | A-15 |
| enable .....  | A-19 |
| exit .....  | A-19 |
| help .....  | A-20 |
| history .....   | A-20 |
| logout .....  | A-21 |
| ping .....  | A-21 |
| ping6 .....   | A-22 |
| start task postfix drop .....                         | A-22 |
| start task postfix flush .....                        | A-23 |
| start task postfix queue .....                        | A-23 |
| start service nscd .....                              | A-24 |
| start service postfix .....                           | A-24 |
| start service product .....                           | A-25 |

|                              |      |
|------------------------------|------|
| start service ssh .....      | A-25 |
| stop process core .....      | A-25 |
| stop service nscd .....      | A-26 |
| stop service postfix .....   | A-26 |
| stop service product .....   | A-27 |
| stop service ssh .....       | A-27 |
| reboot .....                 | A-28 |
| resolve .....                | A-28 |
| show storage statistic ..... | A-29 |
| show network .....           | A-29 |
| show kernel .....            | A-31 |
| show service .....           | A-32 |
| show memory .....            | A-33 |
| show process .....           | A-33 |
| show product-info .....      | A-34 |
| show system .....            | A-35 |
| shutdown .....               | A-36 |
| traceroute .....             | A-37 |

## **Appendix B: Notification Message Tokens**

|   |     |
|---|-----|
| Recipient Notification Message Tokens ..... | B-2 |
| Alert Notification Message Tokens .....     | B-3 |

## **Appendix C: Connections and Ports**

|                                   |     |
|-----------------------------------|-----|
| Service Addresses and Ports ..... | C-2 |
| Ports Used by the Appliance ..... | C-4 |

## **Appendix D: SNMP Object Identifiers**

|                            |      |
|----------------------------|------|
| SNMP Query Objects .....   | D-2  |
| SNMP Traps .....           | D-17 |
| Registration Objects ..... | D-30 |

## **Appendix E: IPv6 Support in Deep Discovery Email Inspector**

|                                  |     |
|----------------------------------|-----|
| Configuring IPv6 Addresses ..... | E-3 |
|----------------------------------|-----|

|   |     |
|---|-----|
| Configurable IPv6 Addresses .....       | E-3 |
| Management Console IPv6 Addresses ..... | E-3 |
| CLI IPv6 Addresses .....                | E-4 |

## **Appendix F: System Event Logs**

## **Appendix G: Sender Authentication Error Codes**

## **Appendix H: Glossary**

## **Index**

|             |      |
|-------------|------|
| Index ..... | IN-1 |
|-------------|------|



# Preface

## Preface

Topics include:

- *Documentation on page 2*
- *Audience on page 3*
- *Document Conventions on page 3*
- *About Trend Micro on page 4*

## Documentation

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

**TABLE 1. Product Documentation**

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

| DOCUMENT       | DESCRIPTION   |
|----------------|---|
| Support Portal | The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website:<br><a href="https://success.trendmicro.com">https://success.trendmicro.com</a> |

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

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

## Audience

The Deep Discovery Email 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
- Email routing
- SMTP





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

## Document Conventions

The documentation uses the following conventions:

**TABLE 2. Document Conventions**

| CONVENTION  | DESCRIPTION   |
|-------------|---|
| UPPER CASE  | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| <b>Bold</b> | Menus and menu commands, command buttons, tabs, and options                     |

| CONVENTION   | DESCRIPTION   |
|--|---|
| <i>Italics</i>   | References to other documents   |
| Monospace  | Sample command lines, program code, web URLs, file names, and program output  |
| <b>Navigation &gt; Path</b>  | The navigation path to reach a particular screen<br><br>For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface |
|  <b>Note</b>      | Configuration notes   |
|  <b>Tip</b>       | Recommendations or suggestions  |
|  <b>Important</b> | Information regarding required or default configuration settings and product limitations  |
|  <b>WARNING!</b>  | Critical actions and configuration options  |

## About Trend Micro

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

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

provides centralized visibility and investigation to make organizations their most resilient.

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

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



# Chapter 1

## Introduction

This chapter describes the product features, capabilities, and security technology.

Topics include:


- *About Deep Discovery Email Inspector on page 1-2*
- *A New Threat Landscape on page 1-10*
- *A New Solution on page 1-12*

## About Deep Discovery Email Inspector

Deep Discovery Email Inspector stops sophisticated targeted attacks and cyber threats by scanning, simulating, and analyzing suspicious links and attachments in email messages before they can threaten your network. Designed to integrate into your existing email network topology, Deep Discovery Email Inspector can act as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance silently monitoring your network for cyber threats and unwanted spam messages.

### What's New

**TABLE 1-1. New Features in Deep Discovery Email Inspector 5.1**

| FEATURE                      | DESCRIPTION  |
|------------------------------|--|
| Trend Vision One integration | <p>Deep Discovery Email Inspector integrates with Trend Vision One to enable collaborative security analytics in a hybrid environment.</p> <hr/> <div> <b>Important</b></div> <p>Before you can configure integration settings, apply the latest hotfix or patch.</p> <hr/> |
| Certificate management       | <p>You can manage certificates in Deep Discovery Email Inspector to enable secure console access and SMTP communication in Transport Layer Security (TLS) environments.</p>  |
| Email address modification   | <p>Deep Discovery Email Inspector provides the email address modification feature that allows you to:</p> <ul style="list-style-type: none"><li>• Rewrite sender or recipient addresses in message envelops or message headers</li><li>• Rewrite domains in email addresses</li></ul>  |

| FEATURE  | DESCRIPTION   |
|--|---|
| Enhanced TLS communications                          | <p>TLS communications has been enhanced in Deep Discovery Email Inspector to support the following:</p> <ul style="list-style-type: none"><li>• TLS 1.3</li><li>• Secure connections for message transfer based on specified domains and IP addresses</li></ul>   |
| DANE for outbound messages                           | <p>Deep Discovery Email Inspector supports DANE (DNS-based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity.</p>   |
| Enhanced policy settings                             | <p>The policy management feature has been enhanced to provide the following settings:</p> <ul style="list-style-type: none"><li>• Send a blind carbon copy (BCC) of detected messages to specified recipients</li><li>• Change the recipients of detected messages</li><li>• Configure sender-recipient exceptions in policies</li><li>• Configure address groups as policy objects</li><li>• Internal email spoofing prevention</li><li>• Apply message stamps based on policy rules</li></ul> |
| Sender and recipient validation for Inbound messages | <p>Deep Discovery Email Inspector provides the following security settings to enhance inbound message security:</p> <ul style="list-style-type: none"><li>• Reject messages from unknown sender IP addresses or domains</li><li>• Reject messages to unknown recipients</li><li>• Match message header FROM address for sender filtering</li></ul>  |
| Enhanced Time-of-Click protection                    | <p>The Time-of-Click protection feature has been enhanced to include the following:</p> <ul style="list-style-type: none"><li>• Customization of redirect pages for detected URLs</li><li>• Syslog forwarding for detected URLs</li></ul>   |

| FEATURE  | DESCRIPTION   |
|--|---|
| Enhanced Virtual Analyzer                      | <p>The Virtual Analyzer has been enhanced to include the following features:</p> <ul style="list-style-type: none"><li>• Open Document file type for sandbox analysis</li><li>• Windows 10 20H1 image support</li></ul>   |
| Improved detection capability                  | <p>Deep Discovery Email Inspector provides increased protection by improving its detection capabilities. This release supports the following:</p> <ul style="list-style-type: none"><li>• ALG and EGG archive files for scanning</li><li>• Decryption of password-protected ALG and EGG archive files and Open Document files for scanning</li><li>• URL extraction from Open Document files for scanning</li><li>• DLP forensic data display on the Detections screens</li></ul> |
| Enhanced approved and blocked senders lists    | <p>Configuration of the approved and blocked senders lists has been enhanced to include the following:</p> <ul style="list-style-type: none"><li>• Sender list import and export</li><li>• Wildcard support for email domain setting</li></ul>  |
| Enhanced license management                    | <p>The license management feature has been enhanced to support gateway-only license on Deep Discovery Email Inspector for gateway deployment.</p>   |
| New fiber network interface card (NIC) support | <p>Deep Discovery Email Inspector supports additional data ports with 10Gbps fiber NIC installation on hardware models 7200, 7300, and 9200.</p>  |
| Deep Discovery Director 5.3 integration        | <p>Deep Discovery Email Inspector supports integration with Deep Discovery Director 5.3.</p>  |
| Deep Discovery Analyzer 7.0 integration        | <p>Deep Discovery Email Inspector supports integration with Deep Discovery Analyzer 7.0 to enable Linux ELF and shell script file submissions.</p>  |

| FEATURE                         | DESCRIPTION   |
|---------------------------------|---|
| Enhanced virtualized deployment | Deep Discovery Email Inspector supports virtual appliance installation on VMware ESXi 6.7 and 7.0.  |
| Inline migration support        | Deep Discovery Email Inspector provides users with the option of automatically migrating the settings from the following versions to 5.1: <ul style="list-style-type: none"><li>• Deep Discovery Email Inspector 5.0</li><li>• Deep Discovery Email Inspector 3.6</li></ul> |

## Features and Benefits

The following sections describe the Deep Discovery Email Inspector features and benefits.

### Advanced Detection

Deep Discovery Email Inspector advanced detection technology discovers targeted threats in email messages, including spear-phishing and social engineering attacks.

- Reputation and heuristic technologies catch unknown threats and document exploits
- File hash analysis blocks unsafe files and applications
- Detects threats hidden in password-protected files and shortened URLs
- Predictive machine learning technology detects emerging unknown security risks
- Blocks malicious URLs in email messages at the time of mouse clicks

### Visibility, Analysis, and Action

Deep Discovery Email 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.

## Flexible Deployment

Deep Discovery Email Inspector integrates into your existing anti-spam/antivirus network topology by acting as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance monitoring your network for cyber threats.

## Policy Management

Policy management allows administrators to enforce preventative actions on messages based on scanning conditions. You can create policies to perform the following tasks:

- Delete suspicious email messages
- Block and quarantine suspicious email messages
- Allow certain email messages to pass through to the recipient
- Strip suspicious attachments
- Redirect suspicious links to blocking or warning pages
- Tag the email subject with a customized string
- Notify recipients when a policy rule is matched
- Send copies of detected email messages to archive servers

## Custom Threat Simulation Sandbox

The Virtual Analyzer sandbox environment opens files, including password-protected archives and document files, and URLs 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.

## Email Attachment Analysis

Deep Discovery Email Inspector utilizes multiple detection engines and sandbox simulation to investigate file attachments. Supported file types

include a wide range of executable, Microsoft Office, PDF, web content, and compressed files.

## Embedded URL Analysis

Deep Discovery Email Inspector utilizes reputation technology, direct page analysis, and sandbox simulation to investigate URLs embedded in an email message.

## Email Encryption

Email Encryption allows Deep Discovery Email Inspector to perform the following tasks based on policy settings:

- Decrypt messages encrypted using Trend Micro Identity-Based Encryption (IBE) for scanning
- Encrypt messages for secure delivery in MTA mode

Deep Discovery Email Inspector can decrypt and encrypt messages regardless of the email client or platform from which the messages originated.



### Note

When Deep Discovery Email Inspector operates in TAP/BCC mode and receives an encrypted message, Deep Discovery Email Inspector only decrypts and scans the message. Deep Discovery Email Inspector does not encrypt messages in TAP/BCC mode.

---

## Spam Scanning

Spam messages are generally unsolicited messages containing mainly advertising content. Deep Discovery Email Inspector uses the following components to filter email messages for spam:

- Trend Micro Antispam Engine
- Trend Micro spam pattern files

Trend Micro Antispam Engine uses spam signatures and heuristic rules to filter email messages. The Antispam Engine scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. Deep Discovery Email Inspector compares the spam score to the selected spam detection level or user-defined detection threshold. When the spam score exceeds the detection level or threshold, Deep Discovery Email Inspector takes action against the spam message.

For example, spammers often use many exclamation marks or more than one consecutive exclamation mark (!!!!) in their email messages. When Deep Discovery Email Inspector detects a message that uses exclamation marks this way, it increases the spam score for that email message.

The Antispam Engine also includes the Email Malware Threat Scan Engine that performs advanced threat scans on email attachments (including script files and Microsoft Office macroware) to detect malware.

## **Graymail Scanning**

Graymail refers to solicited bulk email messages that are not spam. Deep Discovery Email Inspector detects marketing messages and newsletters, social network notifications, and forum notifications as graymail. Deep Discovery Email Inspector identifies graymail messages in two ways:

- Email Reputation Services scoring the source IP address
- Trend Micro Anti-Spam Engine identifying message content

## **Sender Filtering**

You can configure the following sender filtering settings in Deep Discovery Email Inspector to effectively block senders of spam messages at the IP address or sender email address level:

- Approved and blocked senders lists
- Email Reputation Services (ERS)
- Directory harvest attack (DHA) protection

- Bounce attack protection
- SMTP traffic throttling

## Sender Authentication

Deep Discovery Email Inspector supports the following sender authentication standards to effectively detect and fight against techniques used in email phishing and spoofing:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

In addition, you can configure Deep Discovery Email Inspector to sign outgoing messages using DKIM signatures to prevent spoofing.

## Content Filtering

You can create content filtering rules in Deep Discovery Email Inspector to:

- Block content that you specify as inappropriate from reaching recipients by analyzing message content and attachments
- Detect and remove active content (such as macros) in Microsoft Office and PDF file attachments

## Data Loss Prevention

Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows administrators to:

- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through email messages
- Enforce compliance to established privacy standards

## End-User Quarantine

Deep Discovery Email Inspector includes the End-User Quarantine (EUQ) feature to improve spam management. Messages that are determined to be spam are quarantined and are available for users to review, delete, release, or approve for delivery. You can configure Deep Discovery Email Inspector to automatically send EUQ digest notifications with inline action links. With the web-based EUQ console, users can manage the spam quarantine of their personal accounts and of distribution lists that they belong to and add senders to the Approved Senders list.

## Social Engineering Attack Protection

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages. When Social Engineering Attack Protection is enabled, Deep Discovery Email Inspector scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.

## Password Derivation

Deep Discovery Email Inspector decrypts password-protected archives and document files using a variety of heuristics and customer-supplied keywords.

## 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.

## Spear-Phishing Attacks

Spear-phishing attacks combine phishing attacks and targeted malware. Attackers send spear-phishing messages to a few targeted employees with crafted email messages masquerading as legitimate recipients, possibly a boss or colleague. These spear-phishing messages likely contain a link to a malicious website or a malicious file attachment. A file attachment can exploit vulnerabilities in Microsoft™ Word™, Excel™, and Adobe™ products. The file attachment can also be a compressed archive containing executable files. When a recipient opens the file attachment, malicious software attempts to exploit the system. Often, to complete the ruse, the malicious software launches an innocuous document that appears benign.

Once the malicious software runs, it lies dormant on a system or attempts to communicate back to a command-and-control (C&C) server to receive further instructions.

## 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 Email Inspector prevents spear-phishing attacks and cyber threats, and provides Business Email Compromise (BEC) protection by investigating suspicious links, file attachments, and social engineering attack patterns in email messages before they can threaten your network. Designed to integrate into your existing email network topology, Deep Discovery Email Inspector can act as a mail transfer agent in the mail traffic flow (MTA mode) or as an out-of-band appliance (BCC mode or SPAN/TAP mode) monitoring your network for cyber threats and unwanted spam messages.

Whichever deployment method is chosen, Deep Discovery Email Inspector investigates email messages for suspicious file attachments, embedded links (URLs), spam, content violations, and characteristics. If an email message exhibits malicious behavior, Deep Discovery Email Inspector can block the email message and notify security administrators about the malicious activity.

After Deep Discovery Email Inspector scans an email message for known threats in the Trend Micro Smart Protection Network, it passes suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, Command & Control (C&C) and botnet connections, and other suspicious behaviors or characteristics.

After investigating email messages, Deep Discovery Email Inspector assesses the risk using multi-layered threat analysis. Deep Discovery Email Inspector calculates the risk level based on the highest risk or spam score assigned by the Deep Discovery Email Inspector email scanners, Virtual Analyzer, or Trend Micro Smart Protection Network.

Deep Discovery Email Inspector acts upon email messages according to the assigned risk level or spam score, and policy settings. Configure Deep Discovery Email Inspector to block and quarantine the email message, allow the email message to pass to the recipient, strip suspicious file attachments,

redirect suspicious links to blocking or warning pages, or tag the email message with a string to notify the recipient. While Deep Discovery Email Inspector monitors your network for threats or unwanted spam messages, you can access dashboard widgets and reports for further investigation.

## 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

## **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.

After detecting an unknown or low-prevalence file, the Deep Discovery Email 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.

Deep Discovery Email Inspector can attempt to “Quarantine” the affected file to prevent the threat from continuing to spread across your network.

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

## **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.

## **Social Engineering Attack Protection**

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages. When Social Engineering Attack Protection is enabled, Deep Discovery Email Inspector scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.

## **Trend Vision One**

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

## **Apex Central**

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

Apex Central allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Apex Central allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

## Deep Discovery Director

Trend Micro Deep Discovery Director is a management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication and log aggregation for Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

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

# Chapter 2

## Getting Started

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

Topics include:

- *Getting Started Tasks on page 2-2*
- *Requirements to Access Deep Discovery Email Inspector on page 2-4*
- *Configuring Management Console Access on page 2-5*
- *The Management Console on page 2-7*

## Getting Started Tasks

Getting Started Tasks provides a high-level overview of all procedures required to get Deep Discovery Email Inspector up and running as quickly as possible. Each step links to more detailed instructions later in the document. The getting started process is the same for BCC, SPAN/TAP and MTA modes.

---

### Procedure

1. Configure network settings to access the management console.  
For details, see [Configuring Management Console Access on page 2-5](#).
2. Open the management console.  
For details, see [The Management Console on page 2-7](#).
3. Activate the Deep Discovery Email Inspector product licenses.  
For details, see [Activating or Renewing Your Product License on page 8-232](#).
4. Configure the system time.  
For details, see [Configuring System Time on page 8-197](#).
5. Configure network settings.  
For details, see [Configuring Network Settings on page 8-187](#).
6. Configure the operation mode.  
For details, see [Operation Modes on page 8-190](#).
7. Configure the SMTP server.  
For details, see [Configuring the Notification SMTP Server on page 8-194](#).
8. Configure the mail limits and exceptions.  
For details, see [Configuring Limits and Exceptions on page 8-101](#).
9. Configure Virtual Analyzer network settings.  
For details, see [Configuring Virtual Analyzer Network and Filters on page 8-17](#).

**10. Import Virtual Analyzer images.**

For details, see [Importing Virtual Analyzer Images on page 8-14](#).



**Important**

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

---

**11. Configure the password to open archive files and document files.**

For details, see [Adding File Passwords on page 8-34](#).

**12. Configure email routing for downstream MTAs.**

For details, see [Configuring Message Delivery Settings on page 8-98](#).

**13. Add at least one notification recipient to all critical and important alerts.**

For details, see [Alerts on page 6-2](#).

**14. (Optional) Configure policies.**

For details, see [Configuring a Policy on page 5-31](#).

**15. (Optional) Configure policy exceptions.**

For details, see [Policy Exceptions on page 5-83](#).

**16. (Optional) Register with Apex Central or Deep Discovery Director for central management.**

For details, see [Apex Central on page 8-127](#) or [Deep Discovery Director on page 8-132](#).

**17. Configure upstream MTAs or SPAN/TAP devices.**

- a.** If Deep Discovery Email Inspector is operating in BCC or MTA mode, configure the upstream MTAs to route email traffic to Deep Discovery Email Inspector.

**Note**

Configuring the upstream MTA requires different settings for MTA mode and BCC mode. See the supporting documentation provided by the MTA server manufacturer for instructions about configuring MTA settings.

- In MTA mode, configure the MTA to forward email traffic to Deep Discovery Email Inspector.
- In BCC mode, configure the MTA to copy email traffic to Deep Discovery Email Inspector.

- b.** If Deep Discovery Email Inspector is operating in SPAN/TAP mode, configure the SPAN/TAP device to mirror traffic to Deep Discovery Email Inspector.

**Note**

See the supporting documentation provided by the SPAN/TAP device manufacturer for instructions about configuring settings.

## Requirements to Access Deep Discovery Email Inspector

The following table lists the minimum requirements to access the Command Line Interface and the management console that manage Deep Discovery Email Inspector.

**TABLE 2-1. System Access Requirements**

| APPLICATION | REQUIREMENTS           | DETAILS  |
|-------------|------------------------|--|
| SSH client  | SSH protocol version 2 | Set the Command Line Interface terminal window size to 80 columns and 24 rows. |

| APPLICATION        | REQUIREMENTS        | DETAILS   |
|--------------------|---------------------|---|
| Internet Explorer™ | Version 11          | Use only a supported browser to access the management console.<br><br>Using the data port IP address you set during the initial configuration, specify the following URL:<br><br><code>https://<br/>[Appliance_IP_Address]:443</code> |
| Microsoft Edge™    | Windows 10          |   |
| Mozilla Firefox™   | Version 75 or later |   |
| Google Chrome™     | Version 81 or later |   |

**Note**

- Trend Micro recommends viewing the console using a monitor that supports 1280 x 1024 resolution or greater.
- By default, SSH service is disabled and is not started when enabled. To enable SSH service, see [configure service ssh enable on page A-12](#). To start SSH service, see [start service ssh on page A-25](#).

## Configuring Management Console Access

After completing the installation, the server restarts and loads the Command Line Interface (CLI). Configure Deep Discovery Email Inspector network settings to gain access to the management console.

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

- Host name
- Management IP address and netmask
- Gateway
- DNS

### Procedure

1. Log on to the CLI with the default credentials.

- User name: `admin`
  - Password: `ddei`
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 `#`.
  4. Configure network settings with the following command:  
`configure network basic`
  5. Configure the following network settings and press Enter after typing each setting.



**Note**

IPv6 settings are optional.

---

- Host name
  - IPv4 address
  - Subnet mask
  - IPv4 gateway
  - Preferred IPv4 DNS
  - Alternate IPv4 DNS
  - IPv6 address
  - Prefix length
  - IPv6 gateway
  - Preferred IPv6 DNS
  - Alternate IPv6 DNS
6. Type `Y` to confirm settings and restart.

Deep Discovery Email Inspector implements specified network settings and then restarts all services.

---

The initial configuration is complete and the management console is accessible.

---

**Note**

You can log on to the CLI later to perform additional configuration, troubleshooting, or maintenance tasks. For details about the CLI, see [Using the Command Line Interface on page A-1](#).

---

## The Management Console

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

View the management console using any supported web browser. For information about supported browsers, see [Requirements to Access Deep Discovery Email Inspector on page 2-4](#).

For information about configuring required network settings before accessing the management console, see [Configuring Management Console Access on page 2-5](#).

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

`https://<Appliance IP Address>`

---

**Note**

The default management console IP address / subnet mask is  
`192.168.252.1 / 255.255.0.0`.

---

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

- [Logging On Using Local Accounts on page 2-8](#)

- [Logging On With Single Sign-On on page 2-8](#)

## Logging On Using Local Accounts

---

### Procedure

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

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

- User name: `admin`
- Password: `ddei`

2. Click **Log On**.
3. If this is the first time you log on, change the account password before you can access the management console.



#### Note

For hardware model 7300, download and install Hotfix 1394 to display the correct hardware model information on the management console.

For more information, go to [https://success.trendmicro.com/dcx/s/solution/000290725?language=en\\_US](https://success.trendmicro.com/dcx/s/solution/000290725?language=en_US).

---

## Logging On With Single Sign-On

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

For more information, see [SAML Integration on page 8-168](#).

## Procedure

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

The system automatically navigates to the logon page for your organization.

3. Follow the on-screen instructions and provide your account credentials to access the Deep Discovery Email Inspector management console.

## Management Console Navigation

The management console consists of the following elements:

**TABLE 2-2. Management Console Elements**

| SECTION                | DETAILS   |
|------------------------|---|
| Banner                 | <p>The management console banner contains:</p> <ul style="list-style-type: none"> <li>• Product logo and name: Click to go to the dashboard. For details, see <a href="#">Dashboard Overview on page 3-2</a>.</li> <li>• Name of the user currently logged on: Click and select <b>Change password</b> to change the account password (see <a href="#">Changing Your Password on page 8-215</a>) or select <b>Log off</b> to log out of the management console.</li> <li>• System time: Displays the current system time and time zone.</li> <li>• Appliance IP address: Displays the IP address of the Deep Discovery Email Inspector appliance.</li> <li>• Network traffic: Displays the incoming and outgoing network throughput.</li> </ul> |
| Main Menu Bar          | <p>The main menu bar contains several menu items that allow you to configure product settings. For some menu items, such as <b>Dashboard</b>, clicking the item opens the corresponding screen. For other menu items, submenu items appear when you click or mouseover the menu item. Clicking a submenu item opens the corresponding screen.</p>   |
| Context-sensitive Help | <p>Use <b>Help</b> to find more information about the screen that is currently displayed.</p>   |



# Chapter 3

## Dashboard

Topics include:

- *Dashboard Overview on page 3-2*
- *Tabs on page 3-2*
- *Widgets on page 3-4*

## Dashboard Overview

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

The dashboard consists of the following user interface elements:

| ELEMENT | DESCRIPTION  |
|---------|--|
| Tabs    | Tabs provide a container for widgets.<br>For details, see <a href="#">Tabs on page 3-2</a> .               |
| Widgets | Widgets represent the core dashboard components.<br>For details, see <a href="#">Widgets on page 3-4</a> . |

**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.

---

- Tabs provide a container for widgets. For details, see [Tabs on page 3-2](#).
- Widgets represent the core dashboard components. For details, see [Widgets on page 3-4](#).

**Note**

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

---

## Tabs

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

### Predefined Tabs



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

The predefined tabs include:


- **Overview**
- **Threat Monitoring**
- **Top Trends**
- **System Status**
- **Virtual Analyzer**

Tab Tasks

The following table lists all the tab-related tasks:

| TASK                  | STEPS  |
|-----------------------|--|
| Add a tab             | Click the <b>plus</b> icon (  ) on top of the dashboard. The <b>New Tab</b> window displays.<br><br>For information about this window, see <a href="#">New Tab Window on page 3-3</a> . |
| Edit a tab's settings | Click <b>Tab Settings</b> . A window similar to the <b>New Tab</b> window opens, where you can edit settings.  |
| Move a tab            | Use drag-and-drop to change a tab's position.  |
| Delete a tab          | Click the <b>delete</b> icon (  ) next to the tab title. Deleting a tab also deletes all the widgets in the tab.  |

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:

TABLE 3-1. New Tab Tasks

| TASK  | STEPS                     |
|-------|---------------------------|
| Title | Type the name of the tab. |

| TASK       | STEPS  |
|------------|--|
| Layout     | Choose from the available layouts.   |
| Slide Show | Select to include the tab in the Dashboard slide show.   |
| Duration   | Type the number of seconds to display the tab during the Dashboard slide show.   |
| Auto-fit   | Choose <b>On</b> or <b>Off</b> . This feature works when there is only one widget in a column. Choose <b>On</b> to adjust the height of the single widget to match the highest column. |

## 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.



### Adding Widgets to the Dashboard

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

Do any of the following:

---

#### Procedure

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

- To add the selected widgets, click **Add**.

### Widget Tasks

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

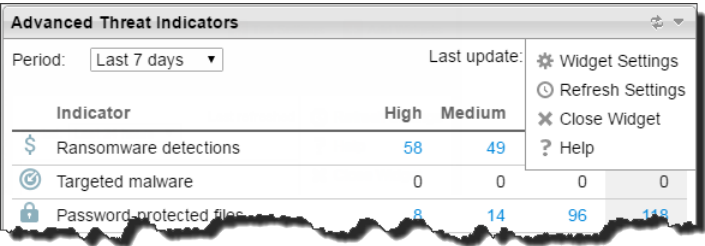
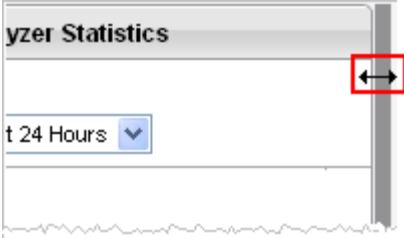
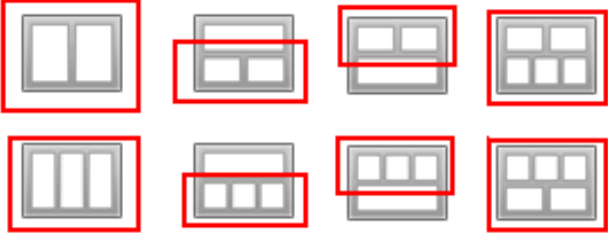


TABLE 3-2. Widget Options Menu

| TASK                              | STEPS   |
|-----------------------------------|---|
| Access widget options             | Click the options icon (⚙️) at the widget's top-right corner to view the menu options.  |
| Edit a widget                     | Click the edit icon (⚙️) to change settings.  |
| Refresh widget data               | Click the refresh icon (🔄) to refresh widget data.<br><br>Click the refresh settings icon (🕒) to set the frequency that the widget refreshes or to automatically refresh widget data.                               |
| Get help                          | Click the question mark icon (❓) to get help. The online help appears explaining how to use the widget.   |
| Delete a widget                   | Click the delete icon (✖️) to close the widget. This action removes the widget from the tab that contains it, but not from any other tabs that contain it or from the widget list in the <b>Add Widgets</b> screen. |
| Move a widget within the same tab | Use drag-and-drop to move the widget to a different location within the tab.  |
| Move a widget to a different tab  | 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.   |

| TASK            | STEPS  |
|-----------------|--|
| Resize a widget | <p>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.</p>  <p>You can resize any widget within a multi-column tab (red squares). These tabs have any of the following layouts.</p>  <p>Change period</p> <p>If available, click the <b>Period</b> drop-down menu to select the time period.</p> |

## Overview

The **Overview** widgets provide detection summary, quarantined and processed messages, top violated policies, and message queue status information.

## Detection Summary Widget

The **Detection Summary** widget displays the numbers of detections for the threat types.

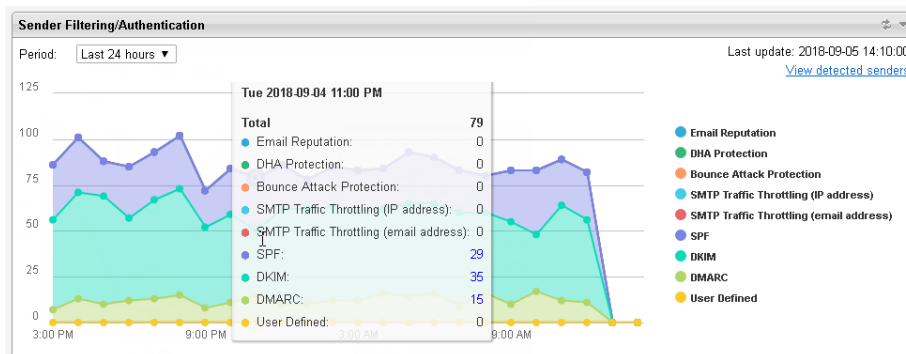
The graph is based on the selected period. The Y-axis represents the detection count. The X-axis represents the period. Mouse-over the points on the graph to view the period and number of detections.

Click a detection category in the legend to hide or show the related data on the graph.

Click **View detected messages** to view all detections.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Sender Filtering/Authentication Widget



The **Sender Filtering/Authentication** widget displays the number of detections based on the sender filtering and authentication settings.

The graph is based on the selected period. The Y-axis represents the detection count. The X-axis represents the period. Mouse-over the points on the graph to view the period and number of detections.

Click a detection category in the legend to hide or show the related data on the graph.

Click **View detected senders** to view the sender filtering/authentication logs.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Quarantined Messages Widget

The **Quarantined Messages** widget displays the quarantine folder size and the total number of quarantined messages. Mouse-over a section on the doughnut chart to view the number of quarantined messages for a quarantine reason.

Click a detection category in the legend to hide or show the related data on the graph.

Click **View quarantined messages** to view all quarantined messages.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Policy Violations Widget

The **Top Policy Violations** widget shows the most common policies and the associated rules that are violated in detected messages based on the selected period. Click a number under **Violations** to view the detected messages for a violated policy.

Click **View detected messages** to view all detected messages.

## Message Queues Widget

The **Message Queues** widget displays the number of messages that just arrived, the number of messages ready for delivery, and the number of messages deferred due to delivery failure. Click a number under **Messages** to view message queue logs.

## Processed Messages Widget

The **Processed Messages** widget displays the number of messages that Deep Discovery Email Inspector processed for each message category or message direction within the selected period. The Y-axis represents the email message count. The X-axis represents the message category or direction.

## Threat Monitoring

View **Threat Monitoring** widgets to understand incoming suspicious messages, attack sources, affected recipients, and which messages were quarantined.

### Attack Sources Widget

The **Attack Sources** widget shows an interactive map representing all source MTAs that routed suspicious email traffic.

An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), Deep Discovery Email Inspector identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

Mouse-over any point on the map to learn about the events that came from the attack source location.

Click any highlighted region on the map to learn more about attacks originating from that region.



#### Note

Attacks in the **No data** group are detected attacks with no location information.

For example, if Deep Discovery Email Inspector is unable to obtain a public IP address from the message routing information, no location information is available.

---

Click **View all attack sources** in the top-right corner to go to the **Attack Sources** screen.

## High-Risk Messages Widget

The **High-Risk Messages** widget shows all incoming malicious messages. High-risk messages have malware communications, malicious contact destinations, malicious behavior patterns, or strings that definitively indicate compromise.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click **View detected messages** to view all detections.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Detected Messages Widget

The **Detected Messages** widget shows all email messages with malicious and suspicious characteristics. Suspicious characteristics include anomalous behavior, false or misleading data, suspicious and malicious behavior patterns, and strings that indicate system compromise but require further investigation.



### Note

A similar widget called Email Messages with Advanced Threats is available in Apex Central, which aggregates data from several Deep Discovery Email Inspector appliances.

---

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of high risk messages and the period.

Click an item in the widget legend to show or hide data related to that metric.

Click **View detected messages** to view all detections.

For general widget tasks, see [Widget Tasks on page 3-5](#).

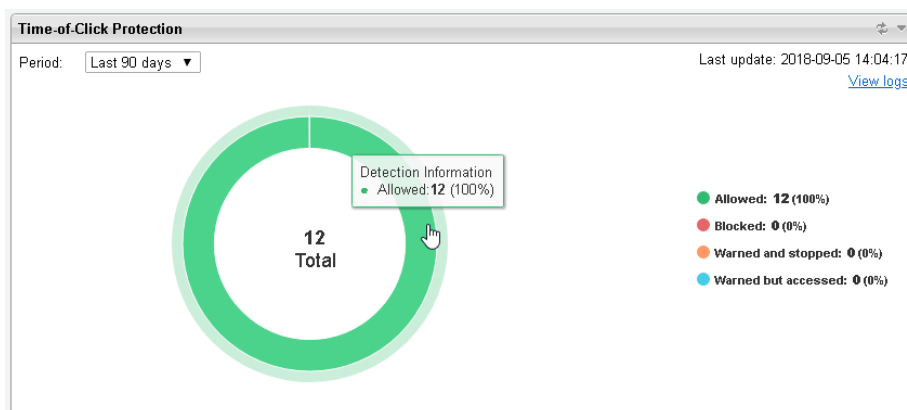
## Advanced Threat Indicators

The **Advanced Threat Indicators** widget shows the type, amount, and risk level of advanced threat indicators detected in all email messages.

The table shows detections based on the selected time period. Click a number under **High**, **Medium**, **Low**, or **Total** to learn more about the detections.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Time-of-Click Protection Widget



The **Time-of-Click Protection** widget displays the total number of detected URLs at the time of user clicks. Mouse-over a section on the doughnut chart to view the number of detected URLs for a detection action.

Click a detection action in the legend to hide or show the related data on the graph.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Trends

View **Top Trends** widgets to understand the top activity in your network, including suspicious message content and callback destinations, to understand the threat characteristics affecting your network.

### Top Attachment Names Widget

The **Top Attachment Names** widget shows the most common file attachments contained in suspicious and high-risk email messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

For general widget tasks, see [Widget Tasks on page 3-5](#).

### Top Attachment Types Widget

The **Top Attachment Types** widget shows the most common attachment file types contained in detected messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

For general widget tasks, see [Widget Tasks on page 3-5](#).

### Top Affected Recipients Widget

The **Top Affected Recipients** widget shows the recipients who received the highest volume of suspicious messages.

**Note**

A similar widget called Top Email Recipients of Advanced Threats is available in Apex Central, which aggregates data from several Deep Discovery Email Inspector appliances.

---

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all recipients** to see all recipients affected by suspicious messages.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Attack Sources Widget

The **Top Attack Sources** widget shows the most active IP addresses attacking your network.

An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), Deep Discovery Email Inspector identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all attack sources** to see all detected attack sources over the selected time period.



### Note

A dash (-) indicates that the location information is not available.

For example, if Deep Discovery Email Inspector is unable to obtain a public IP address from the message routing information, no location information is available.

---

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Callback Hosts from Virtual Analyzer Widget

The **Top Callback Hosts from Virtual Analyzer** widget shows the most common callback hosts contained in suspicious and high-risk email messages. A callback host is the IP address or host name of a C&C server.

When Virtual Analyzer receives an object (file or URL) from the Deep Discovery Email Inspector email scanners, Virtual Analyzer observes whether the object connects to an external network address. A high-risk object attempts to perform a callback to a known C&C server host. Virtual Analyzer reports all connections (URLs, IP addresses, and host names) made by submitted samples, including possible malware callback and other suspicious connections.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all callback hosts** to see all suspicious host objects found during analysis.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Callback URLs from Virtual Analyzer Widget

The **Top Callback URLs from Virtual Analyzer** widget shows the most common callback URLs contained in suspicious and high-risk email messages. A callback URL is the web address of a C&C server.

When Virtual Analyzer receives an object (file or URL) from the Deep Discovery Email Inspector email scanners, Virtual Analyzer observes whether the object connects to an external network address. A high-risk object attempts to perform a callback to a known C&C server host. Virtual Analyzer reports all connections (URLs, IP addresses, and host names) made by submitted samples, including possible malware callback and other suspicious connections.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all callback URLs** to see all suspicious URL objects found during analysis.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Top Email Subjects Widget

The **Top Email Subjects** widget shows the most common email message subjects contained in suspicious and high-risk email messages.

The table shows detections based on the selected time period. Click a number under **Detections** or **High Risk Messages** to learn more about the detections. **Detections** includes all detected email messages, including high-risk messages.

Click **View all email subjects** to see the email subjects in detected messages during the selected time period.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## System Status

View **System Status** widgets to understand overall email message processing volume during different time periods for different risk levels and the current Deep Discovery Email Inspector appliance hardware status. The widgets graphically show how system performance affects message delivery.

## Processing Volume Widget

The **Processing Volume** widget shows all email messages, file attachments, and embedded links that Deep Discovery Email Inspector investigated.

The graph is based on the selected period. The Y-axis represents the total number of processed email messages, attachments, or embedded links. The X-axis represents the period. Mouse-over a point on the graph to view the

number of high risk messages and the period. Click on an item in the legend to toggle it on or off in the graph.

Click an item in the widget legend to show or hide data related to that metric.

Click **View logs** to view the message tracking logs.

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Hardware Status Widget

The **Hardware Status** widget shows the Deep Discovery Email Inspector appliance's current CPU, memory, and disk usage within the last 5 seconds.



### Note

“Disk usage” refers to the amount of data stored on the disk partition.

---

For general widget tasks, see [Widget Tasks on page 3-5](#).

## Virtual Analyzer

View **Virtual Analyzer** widgets to assess Virtual Analyzer performance based on processing time, queue size, and the volume of suspicious objects discovered during analysis.

### Messages Submitted to Virtual Analyzer Widget

The **Messages Submitted to Virtual Analyzer** widget shows the number of email messages that are submitted to Virtual Analyzer for processing during each 5-minute interval.

The graph is based on the selected period. The Y-axis represents the email message count. The X-axis represents the period. Mouse-over a point on the graph to view the number of messages submitted to Virtual Analyzer and the period.

Click **View detected messages in queue** to view email messages currently undergoing analysis.

For general widget tasks, see [Widget Tasks on page 3-5](#).

### 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 number of high risk messages and the period.

Click **Manage Virtual Analyzer** to reallocation instances, to add or remove images, or to make other changes to Virtual Analyzer settings.

For general widget tasks, see [Widget Tasks on page 3-5](#).

### Suspicious Objects from Virtual Analyzer Widget

The **Suspicious Objects from Virtual Analyzer** widget shows the suspicious objects found in Virtual Analyzer. Suspicious objects are objects with the potential to expose systems to danger or loss. Virtual Analyzer detects and analyzes suspicious IP addresses, host names, 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 messages and the period.

Click an item in the widget legend to show or hide data related to that metric.

Click **View suspicious objects** to view suspicious objects affecting your network.

For general widget tasks, see [Widget Tasks on page 3-5](#).



# Chapter 4

## Detections

Topics include:

- *Detected Risk on page 4-2*
- *Threat Type Classifications on page 4-5*
- *Exporting Search Results on page 4-6*
- *Detected Messages on page 4-7*
- *Suspicious Objects on page 4-21*
- *Quarantine on page 4-26*
- *Sender Filtering/Authentication on page 4-34*

## Detected Risk

Detected risk is potential danger exhibited by a suspicious email message.

Deep Discovery Email Inspector assesses email message risk using multi-layered threat analysis. Upon receiving an email message, Deep Discovery Email Inspector email scanners check the email message for known threats in the Trend Micro Smart Protection Network and Trend Micro Advanced Threat Scanning Engine. If the email message has unknown or suspicious characteristics, the email scanners send file attachments and embedded URLs to Virtual Analyzer for further analysis. Virtual Analyzer simulates the suspicious file and URL behavior to identify potential threats. Deep Discovery Email Inspector assigns a risk level to the email message based on the highest risk assigned between the Deep Discovery Email Inspector scanners and Virtual Analyzer.

For details about how Deep Discovery Email Inspector investigates email messages, see [A New Solution on page 1-12](#).

## Email Message Risk Levels

The following table explains the email message risk levels after investigation. View the table to understand why an email message was classified as high, medium, or low risk.

**TABLE 4-1. Email Message Risk Definitions**

| RISK LEVEL | DESCRIPTION  |
|------------|--|
| High       | <p>A high-risk email message contains:</p> <ul style="list-style-type: none"> <li>• Attachments with unknown threats detected as high risk by Virtual Analyzer</li> <li>• Attachments detected as high risk based on YARA rules</li> <li>• Attachments detected as high risk based on suspicious file matching</li> <li>• Attachments detected by Predictive Machine Learning and Email Malware Threat Scan</li> <li>• Business Email Compromise</li> <li>• Links detected as high risk by Virtual Analyzer</li> <li>• Links detected as high risk based on suspicious URL matching</li> </ul> |
| Medium     | <p>A medium-risk email message contains:</p> <ul style="list-style-type: none"> <li>• Known malware</li> <li>• Known phishing threats</li> <li>• Known dangerous links</li> <li>• Attachments detected as medium risk based on YARA rules</li> <li>• Links detected as medium risk based on suspicious URL matching</li> </ul>   |
| Low        | <p>A low-risk email message contains:</p> <ul style="list-style-type: none"> <li>• Known highly suspicious or suspicious links (Aggressive mode)</li> <li>• Links detected as low risk by Virtual Analyzer</li> <li>• Attachments detected as low risk by Virtual Analyzer</li> <li>• Attachments detected as low risk based on YARA rules</li> <li>• Links detected as low risk based on suspicious URL matching</li> <li>• Social engineering attacks</li> <li>• Business Email Compromise (BEC) scams</li> </ul>  |

| RISK LEVEL  | DESCRIPTION  |
|-------------|--|
| No risk     | <p>A no-risk email message:</p> <ul style="list-style-type: none"> <li>• Contains no suspicious attachments or links</li> <li>• Contains known highly suspicious or suspicious links (Standard mode)</li> <li>• Matches policy exception criteria</li> </ul>   |
| Unrated     | <p>An unrated email message falls under any of the following categories:</p> <ul style="list-style-type: none"> <li>• Bypassed scanning: Contains an attachment with a compression layer greater than 20 (the file has been compressed over twenty times)</li> <li>• Unscannable archive: Contains a password-protected archive that could not be extracted and scanned using the password list or heuristically obtained passwords</li> <li>• Unscannable message or attachment: Matches any of the following criteria: <ul style="list-style-type: none"> <li>• Malformed email format</li> <li>• A system timeout occurred when Virtual Analyzer attempted to analyze the message</li> <li>• A system timeout occurred when Virtual Analyzer attempted to analyze some of the attachments or links and no other risks were detected</li> <li>• Virtual Analyzer was unable to analyze all of the attachments or links and no other risks were detected</li> </ul> </li> </ul> |
| Unavailable | <p>Deep Discovery Email Inspector does not assign a risk level to a spam/graymail message or an email message with content violation or DLP incidents.</p>   |

## 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 or low risk.


| RISK LEVEL | DESCRIPTION   |
|------------|---|
| High       | <p>The object exhibited highly suspicious characteristics that are commonly associated with malware.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Malware signatures; known exploit code</li> <li>• Disabling of security software agents</li> <li>• Connection to malicious network destinations</li> <li>• Self-replication; infection of other files</li> <li>• Dropping or downloading of executable files by documents</li> </ul> |
| Low        | The object exhibited mildly suspicious characteristics that are most likely benign.   |
| No Risk    | The object did not exhibit suspicious characteristics.  |

## Threat Type Classifications

The following table explains the threat types detected during scanning or analysis. View the table to understand the malicious activity affecting your network.

**TABLE 4-2. Email Message Threat Types**

| THREAT TYPE      | CLASSIFICATION  |
|------------------|---|
| Targeted malware | Malware made to look like they come from someone a user expects to receive email messages from, possibly a boss or colleague                |
| Malware          | Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems |
| Malicious URL    | A hyperlink embedded in an email message that links to a known malicious web site   |

| THREAT TYPE       | CLASSIFICATION   |
|-------------------|--|
| Suspicious File   | <p>A file that exhibits malicious characteristics</p> <hr/> <p> <b>Important</b><br/>Always handle suspicious files with caution.</p> <hr/> |
| Suspicious URL    | <p>A hyperlink embedded in an email message that links to an unknown malicious website</p>   |
| Phishing          | <p>Email messages that seek to fool users into divulging private information by redirecting users to legitimate-looking web sites</p>  |
| Spam/Graymail     | <p>Unsolicited spam email messages, often of a commercial nature, sent indiscriminately to multiple individuals</p> <p>Graymail refers to solicited bulk email messages that are not spam</p>                                |
| Content violation | <p>Content that you deem inappropriate, such as personal communication or large attachments</p>  |
| DLP incident      | <p>Transmission of email messages containing your organization's digital assets</p>  |

## Exporting Search Results

You can export the search results for detected messages and suspicious objects.

---

### Procedure

- Click **Export All** above the search results.

The search results download as a CSV file.



#### Note

Only the first 50000 entries in the query results are included in the CSV file.

---

## Detected Messages

Detected messages are email messages that contain malicious or suspicious content, embedded links, attachments, or social engineering attack related characteristics. Deep Discovery Email Inspector assigns a risk rating to each email message based on the investigation results.

Query detected messages to:

- Better understand the threats affecting your network and their relative risk
- Find senders and recipients of detected messages
- Understand the email subjects of detected messages
- Research attack sources that route detected messages
- Discover trends and learn about related detected messages
- See how Deep Discovery Email Inspector handled the detected message

## Viewing Detected Messages





Gain intelligence about the context of a spear-phishing attack by investigating a wide array of information facets. Review the email headers to quickly verify the email message origin and how it was routed. Investigate attacks trending on your network by correlating common characteristics (examples: email subjects that appear to be your Human Resource department or fake internal email addresses). Based on the detections, change your policy configuration and warn your users to take preventive measures against similar attacks.


---

### Procedure

1. Go to **Detections > Detected Messages**.
2. Specify the search criteria.  
See [Detected Message Search Filters on page 4-9](#).
3. Press ENTER.  
All email messages matching the search criteria appear.

#### 4. View the results.

| HEADER  | DESCRIPTION  |
|---|--|
|    | Investigate the email message to learn more about potential threats.<br>For details, see <a href="#">Investigating a Detected Message on page 4-12</a> .   |
| Detected  | View the date and time that the suspicious email message was first detected in Deep Discovery Email Inspector.<br><br><div> <b>Note</b><br/>There is a short delay between when Deep Discovery Email Inspector receives an email message and when the email message appears on the <b>Detected Messages</b> screen.</div> |
| Risk Level  | View the level of potential danger exhibited in a suspicious email message.<br>For details, see <a href="#">Detected Risk on page 4-2</a> .  |
| Recipients  | View the detected message recipient email addresses.   |
| Email Header (To)   | View the primary recipient email address in the email header.  |
| Sender  | View the sending email address of the detected message.  |
| Email Header (From)   | View the author email address in the email header.   |
| Email Subject   | View the email subject of the suspicious email message.  |
|  | View the number of email messages with embedded malicious links.   |
|  | View the number of file attachments that are detected by policy rules.   |
| Threat  | View the name and classification of the discovered threat.<br>For details, see <a href="#">Threat Type Classifications on page 4-5</a> .   |

| HEADER | DESCRIPTION  |
|--------|--|
| Action | <p>View the final result after scanning and analyzing the email message. The result is the executed policy action.</p> <hr/> <div>  <b>Note</b><br/> In BCC mode and SPAN/TAP mode, the action is always <b>Monitoring only</b>. </div> <hr/> |


## Detected Message Search Filters

The following table explains the basic search filters for querying suspicious messages. To view the detected messages, go to **Detections > Detected Messages**.



### Note

Search filters do not accept wildcards. Deep Discovery Email Inspector uses fuzzy logic to match search criteria to email message data.

| FILTER      | DESCRIPTION   |
|-------------|---|
| Threat type | <p>Select <b>All</b> or a threat type from the list.</p> <p>For details, see <a href="#">Threat Type Classifications on page 4-5</a>.</p>   |
| Risk level  | <p>Select <b>All</b> or the email message risk level.</p>   |
| Action      | <p>Select <b>All</b> or an action from the list.</p> <p>This is the action that Deep Discovery Email Inspector applies on email messages when a scanning condition is matched in a policy rule.</p> <p>For more information, see <a href="#">Policy Rules on page 5-36</a>.</p> <hr/> <div>  <b>Note</b><br/> In BCC mode and SPAN/TAP mode, the action is always <b>Monitoring only</b>. </div> <hr/> |

| FILTER | DESCRIPTION   |
|--------|---|
| Period | Select a predefined time range or specify a custom range. |

## Applying Advanced Filters

In addition to basic filters, you can apply advanced filters to query suspicious messages.

---

### Procedure

1. Click **Show advanced filters**.
2. Specify the information to filter.

| FILTER              | DESCRIPTION   |
|---------------------|---|
| Sender              | Specify the sender email address.   |
| Email header (To)   | Specify a primary recipient email address in the email header.                    |
| Message ID          | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com |
| Subject             | Specify the email message subject.  |
| Direction           | Specify the message direction.  |
| Rule                | Specify a rule name.  |
| Email header (From) | Specify the author email address in the email header.                             |
| URL                 | Specify a URL.  |

| FILTER          | DESCRIPTION   |
|-----------------|---|
| Source IP       | <p>Specify the MTA IP address nearest to the email sender. The source IP is the IP address of the attack source, compromised MTA, or a botnet with mail relay capabilities.</p> <p>A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection.</p> <hr/> <div data-bbox="525 480 583 529"></div> <p><b>Note</b></p> <p>The <b>Source IP</b> search filter requires an exact-string match. Deep Discovery Email Inspector does not use fuzzy logic to match search results for the source IP address.</p> <hr/> |
| File name       | Specify an attachment file name.  |
| Data identifier | Specify a data identifier name.   |
| YARA rule name  | Specify the name of a YARA rule.  |
| Recipient       | Specify a recipient email address. Only one address is allowed.   |
| Threat name     | <p>Specify the threat name provided by Trend Micro. The dashboard widgets and the <b>Detections</b> tab provide information about threat names.</p> <p>For information about threat discovery capabilities, see <a href="#">Scanning / Analysis on page 8-9</a>.</p>  |

| FILTER                        | DESCRIPTION  |
|-------------------------------|--|
| Sender IP                     | <p>Specify the sender IP address.</p> <p>If you deploy Deep Discovery Email Inspector as an edge MTA in your network, the sender IP address is the public IP address of the external MTA nearest to your network.</p> <p>If you deploy Deep Discovery Email Inspector as a non-edge MTA in your network, the sender IP address is the IP address of the MTA nearest to the edge MTA relay server.</p> <hr/> <div data-bbox="427 524 485 574"></div> <p><b>Note</b> The <b>Sender IP</b> search filter requires an exact-string match. Deep Discovery Email Inspector does not use fuzzy logic to match search results for the sender IP address.</p> <hr/> |
| Policy                        | Specify a policy name.   |
| DLP template                  | Specify a DLP template name.   |
| YARA rule file name           | Specify the name of a YARA rule file.  |
| Password-protected attachment | Select email messages that contain a password-protected file.  |
| Manual email submissions      | <p>Select email messages that are manually submitted to Deep Discovery Email Inspector for analysis by the administrator.</p> <p>For more information, see <a href="#">Email Submissions on page 8-29</a>.</p>   |

### 3. Click **Search**.

## Investigating a Detected Message

### Procedure

#### 1. Search for the email message.

See [Viewing Detected Messages on page 4-7](#).

2. Click the arrow next to the email message in the table.

The table row expands with more information.


3. Discover the email message details.

See [Email Message Details on page 4-13](#).

## Email Message Details

The following table explains the email message details viewable after expanding the search results. The display fields vary depending on the type of detected threats.

| FIELD                        | DESCRIPTION   |
|------------------------------|---|
| View in Threat Connect       | Click <b>View in Threat Connect</b> 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. |
| View Virtual Analyzer Report | Click <b>View Virtual Analyzer Report</b> to view the analysis report in HTML or PDF format.  |
| View Screenshot              | Click <b>View Screenshot</b> to safely display the email message as an image.   |
| Download                     | Select an option from the drop-down list to download the information for further investigation.   |

| FIELD                            | DESCRIPTION   |
|----------------------------------|---|
| Overview                         | <p>View the message ID, recipients, last detection time, sender and source IP addresses, and direction of the email message to understand where the message came from and other tracking information.</p> <hr/> <div>  <b>Note</b> </div> <p>For sender and source IP addresses, <b>Unknown</b> indicates that the detected messages are from an unknown origin (both the location and IP address information is not available), and <b>No data</b> indicates that the location information is not available.</p> <hr/> <p>Get information about the policy rules that the email message violates.</p> |
| Messages                         | View the name of the scanning engine and the category for detected email messages that are considered as spam or graymail.  |
| Attachments                      | Get information about any files attached to the email message, including the file name, password, file type, risk level, SHA-1 and SHA-256 hash values, the scan engine that identified the threat, and the name of detected threats.   |
| YARA Detection                   | Get information about the detected files based on matched YARA rules in the associated YARA rule files.   |
| Links                            | Get information about any embedded suspicious URLs that appeared in the email message, including the URL, site category, risk level, extraction source, the scan engine that identified the threat, and the name of detected threats.   |
| Message Characteristics          | Get information about any social engineering attack related characteristics that were detected in the email message, including the mail server reputation, gaps between transits, inconsistent recipient accounts, and forged sender addresses or unexpected relay servers, etc.  |
| Content Keyword/Expression Match | Get information about the content keywords or expressions that are matched in the email message.  |
| DLP Incident                     | Get information about the data identifiers and DLP templates that are matched in the email message, message location, and forensic data.  |

| FIELD        | DESCRIPTION                            |
|--------------|--|
| Email Header | View the email message header content. |

## Viewing Affected Recipients

Affected recipients are recipients of malicious or suspicious email messages. Gain intelligence about who in your network is targeted by spear-phishing attacks or social engineering attacks and understand the attack behavior in related messages. Learn if your executive is targeted by the attacks and then raise his/her awareness about the attack pattern. Discovering a community of affected recipients belonging to the same department can indicate that the attacker has access to your company address book.

### Procedure

1. Go to **Detections > Recipients**.

2. Specify the search criteria.



- **Recipient** (email address)
- **Period**

3. Press ENTER.

All email messages matching the search criteria appear.

4. View the results.

| HEADER     | DESCRIPTION   |
|------------|---|
| Recipient  | View the detected message recipient email addresses.  |
| Detections | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk  | View the detected messages with malicious characteristics.  |

| HEADER  | DESCRIPTION   |
|---|---|
| Medium Risk   | View the detected messages with characteristics that are most likely malicious.                             |
| Low Risk  | View the detected spam messages or detected messages with content violations or suspicious characteristics. |
| Spam/Graymail   | View the number of detected spam messages or graymail.  |
| Content Violation   | View the number of detected messages with content violations.   |
| DLP Incident  | View the number of detected messages with DLP incidents.  |
|  | View the number of email messages with embedded malicious links.  |
|  | View the number of file attachments that are detected by policy rules.                                      |
| Latest Detection  | View the most recent occurrence of the detected message.  |

---

## Viewing Attack Sources

An attack source is the first MTA with a public IP address that routes a suspicious message. For example, if a suspicious message travels the following route: IP1 (sender) > IP2 (MTA: 225.237.59.52) > IP3 (company mail gateway) > IP4 (recipient), Deep Discovery Email Inspector identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.

Gain intelligence about the prevalence of the attack detections and their relative risk to your network. Learn about the location of the attack, especially whether the attack source is an MTA in your organization or in a region where your organization does not operate.

---

### Procedure

1. Go to **Detections > Attack Sources**.



2. Specify the search criteria.
  - **Attack source** (IP address)
  - **Country**



3. Select the **Period**.

4. Press ENTER.

All email messages matching the search criteria appear.

5. View the results.

| HEADER        | DESCRIPTION  |
|---------------|--|
| Attack Source | View the IP address of the attack source.  |
| Country       | View the country where the attack source is located.<br><br><div>  <b>Note</b><br/>           A dash (-) indicates that the location information is not available.         </div> |
| City          | View the city where the attack source is located.<br><br><div>  <b>Note</b><br/>           A dash (-) indicates that the location information is not available.         </div>    |
| Detections    | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message.  |
| High Risk     | View the detected messages with malicious characteristics.   |
| Medium Risk   | View the detected messages with characteristics that are most likely malicious.  |

| HEADER  | DESCRIPTION   |
|---|---|
| Low Risk  | View the detected spam messages or detected messages with content violations or suspicious characteristics. |
| Spam/Graymail   | View the number of detected spam messages or graymail.  |
| Content Violation   | View the number of detected messages with content violations.   |
| DLP Incident  | View the number of detected messages with DLP incidents.  |
|  | View the number of email messages with embedded malicious links.  |
|  | View the number of file attachments that are detected by policy rules.                                      |
| Latest Detection  | View the most recent occurrence of the detected message.  |

---

## Viewing Senders

Suspicious senders are senders of malicious or suspicious email messages. Find patterns in spoofed sender addresses and learn which social engineering techniques are employed. For example, the sender's email address appears as internal addresses, financial services (PayPal, banks), or other services (Gmail, Taobao, Amazon). Check the sender domain addresses and associated risk level to change policy settings or settings on the anti-spam gateway to block the suspicious sender email addresses at your mail gateway.



---

### Procedure

1. Go to **Detections > Senders**.
2. Specify the search criteria.
  - **Sender** (email address)
  - **Period**
3. Press ENTER.

All email messages matching the search criteria appear.

#### 4. View the results.

| HEADER  | DESCRIPTION   |
|---|---|
| Sender  | View the sending email address of the detected message.   |
| Detections  | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk   | View the detected messages with malicious characteristics.  |
| Medium Risk   | View the detected messages with characteristics that are most likely malicious.   |
| Low Risk  | View the detected spam messages or detected messages with content violations or suspicious characteristics.   |
| Spam/Graymail   | View the number of detected spam messages or graymail.  |
| Content Violation   | View the number of detected messages with content violations.   |
| DLP Incident  | View the number of detected messages with DLP incidents.  |
|  | View the number of email messages with embedded malicious links.  |
|  | View the number of file attachments that are detected by policy rules.  |
| Latest Detection  | View the most recent occurrence of the detected message.  |

## Viewing Email Subjects

Suspicious subjects are the email subjects of malicious or suspicious email messages. Find trends in common keywords or other social engineering techniques. Pretexting is the most common way to engage a victim. Look for email subjects that appear familiar to targeted recipients (examples: holiday party invitation, bank statement, or a common subject used in department newsletters) that can trick your users into opening the email message. If users trust the email subject, there is more chance that they will download a

malicious attachment or follow a phishing link that appears to be a legitimate request for their domain credentials or customer information.

## Procedure

1. Go to **Detections > Subjects**.

2. Specify the search criteria.


- **Email subject**


- **Period**

3. Press ENTER.

All email messages matching the search criteria appear.

4. View the results.

| HEADER  | DESCRIPTION   |
|---|---|
| Email Subject   | View the email subject of the suspicious email message.   |
| Detections  | View the email messages with malicious or suspicious characteristics. Signature-based detection involves searching for known patterns of data within executable code or behavior analysis. Click the number to see more information about the suspicious message. |
| High Risk   | View the detected messages with malicious characteristics.  |
| Medium Risk   | View the detected messages with characteristics that are most likely malicious.   |
| Low Risk  | View the detected spam messages or detected messages with content violations or suspicious characteristics.   |
| Spam/Graymail   | View the number of detected spam messages or graymail.  |
| Content Violation   | View the number of detected messages with content violations.   |
| DLP Incident  | View the number of detected messages with DLP incidents.  |
|  | View the number of email messages with embedded malicious links.  |

| HEADER  | DESCRIPTION  |
|---|--|
|  | View the number of file attachments that are detected by policy rules. |
| Latest Detection  | View the most recent occurrence of the detected message.               |

## Suspicious Objects

Suspicious objects are objects with 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 hosts, URLs, files, and synchronized suspicious objects
- Learn whether email messages contain embedded links or callback addresses
- Find infected endpoints in your network
- Proactively contain or block infections

## Viewing Suspicious Hosts

A suspicious host is an IP address or host name with the potential to expose systems to danger or loss. View suspicious hosts to understand your risk, find related messages, and assess the relative prevalence of the suspicious host.

### Procedure

1. Go to **Detections > Suspicious Objects > Hosts**.
2. Specify the search criteria.
  - **Host** (IP address or host name)

- **Period**

3. Press ENTER.

All suspicious objects matching the search criteria appear.

4. View the results.

| HEADER                    | DESCRIPTION   |
|---------------------------|---|
| Host                      | View the IP address or host name used by the suspicious object.   |
| Port                      | View the port number used by the suspicious object.   |
| Risk Level                | View the level of potential danger in a sample after Virtual Analyzer executes the file or opens the URL. |
| Related Messages          | View the messages containing the same suspicious object.  |
| Latest Message Recipients | View the most recent recipients of the email message containing suspicious objects.                       |
| Latest Detection          | View the date and time Virtual Analyzer last found the suspicious object in a submitted object.           |

---

## Viewing Suspicious URLs

A suspicious URL is a web address with the potential to expose systems to danger or loss . View suspicious URLs to understand your risk, find related messages, and see the most recent occurrences.

---

### Procedure

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

2. Specify the search criteria.

- **URL**

- **Period**

3. Press ENTER.

All suspicious objects matching the search criteria appear.

#### 4. View the results.

| HEADER                    | DESCRIPTION   |
|---------------------------|---|
| URL                       | View the web address of the suspicious object.  |
| Risk Level                | View the level of potential danger in a sample after Virtual Analyzer executes the file or opens the URL. |
| Related Messages          | View the messages containing the same suspicious object.  |
| Latest Message Recipients | View the most recent recipients of the email message containing suspicious objects.                       |
| Latest Detection          | View the date and time Virtual Analyzer last found the suspicious object in a submitted object.           |

## Viewing Suspicious Files

A suspicious file is the associated SHA-1 hash value with the potential to expose systems to danger or loss. View suspicious files to understand your risk, find related messages, and assess the relative prevalence of the suspicious file.

### Procedure

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

2. Specify the search criteria.

- **File SHA-1**

- **Period**

3. Press ENTER.

All suspicious objects matching the search criteria appear.

4. View the results.

| HEADER     | DESCRIPTION  |
|------------|--|
| File SHA-1 | View the 160-bit hash value that uniquely identifies a file. |

| HEADER                    | DESCRIPTION   |
|---------------------------|---|
| Related Messages          | View the messages containing the same suspicious object.  |
| Latest Message Recipients | View the most recent recipients of the email message containing suspicious objects.             |
| Latest Detection          | View the date and time Virtual Analyzer last found the suspicious object in a submitted object. |

---

## Viewing Synchronized Suspicious Objects

Deep Discovery Email Inspector can synchronize suspicious objects with an external source (for example, Trend Vision One, Apex Central, Deep Discovery Director, or Deep Discovery Analyzer). View synchronized suspicious objects to understand your risk, find related messages, and assess the relative prevalence of the suspicious object.

---



### Note

- If Deep Discovery Email Inspector is registered to both Apex Central and Deep Discovery Director 3.0 (or later), Deep Discovery Email Inspector synchronizes suspicious objects from Deep Discovery Director and overwrites existing suspicious objects from Apex Central.
  - If you register Deep Discovery Email Inspector to Trend Vision One, Deep Discovery Director 3.0 (or later), and Trend Micro Apex Central, Deep Discovery Email Inspector synchronizes suspicious objects and exception lists with the integrated products in the following priority: Trend Vision One, Deep Discovery Director, Apex Central.
- 

## Procedure

1. Go to **Detections > Suspicious Objects > Synchronized Suspicious Objects**.
2. Specify the search criteria.

- **Suspicious Object** (IP address, host name, URL, file SHA-1, or file SHA-256)
- **Period** (time range to filter based on the last synchronized time)

3. Press ENTER.

All suspicious objects matching the search criteria appear.

4. View the results.

| HEADER            | DESCRIPTION  |
|-------------------|--|
| Suspicious Object | View the IP address, host name, URL, file SHA-1, or file SHA-256 associated with the synchronized suspicious object.   |
| Type              | View the suspicious object type (Domain, File, IP, or URL).  |
| Risk Level        | View the level of potential danger in a sample after Virtual Analyzer executes the file or opens the URL.  |
| Source            | View the source of the synchronized suspicious object.<br>The source can be one of the following: <ul style="list-style-type: none"> <li>• Trend Vision One</li> <li>• Apex Central</li> <li>• Deep Discovery Analyzer</li> <li>• Deep Discovery Director</li> </ul> |
| User-Defined      | View whether the synchronized suspicious object is user-defined or not.  |
| Expiration        | View the date and time the object is not considered suspicious.  |
| Last Synchronized | View the date and time the entry was last synchronized with the source.  |

## Quarantine

Deep Discovery Email Inspector quarantines suspicious email messages that meet certain policy criteria. View details about an email message before deciding whether to delete the email message, release it to the intended recipients, or resume processing.

Before deciding which action to perform, query the email messages that Deep Discovery Email Inspector quarantined.

Perform any of the following actions:





- Search for quarantined messages based on a variety of criteria
- Learn more about malicious file attachments and URLs
- Release quarantined messages
- Delete quarantined messages
- Resume processing of messages that are quarantined due to spam detection, content violation, or DLP incidents
- Unlock password-protected files in messages to perform a threat scan

## Viewing Quarantined Messages

---

### Procedure

1. Go to **Detections > Quarantine**.
2. Specify the search criteria.  
*See [Quarantine Search Filters on page 4-28](#).*
3. Press ENTER.  
All email messages matching the search criteria appear.
4. View the results.

| HEADER  | DESCRIPTION   |
|---|---|
|    | <p>Investigate the email message to learn more about potential threats.</p> <p>For details, see <a href="#">Investigating a Quarantined Email Message on page 4-31</a>.</p>   |
| Detected  | <p>View the date and time that the suspicious email message was first detected and quarantined in Deep Discovery Email Inspector.</p> <hr/> <div>  <p><b>Note</b></p> <p>There is a short delay between when Deep Discovery Email Inspector receives an email message and when the email message appears on the <b>Quarantine</b> screen.</p> </div> <hr/> |
| Risk Level  | View the level of potential danger exhibited in a suspicious email message.   |
| Recipients  | View the detected message recipient email addresses.  |
| Email Header (To)   | View the primary recipient email address in the email header.   |
| Sender  | View the sending email address of the detected message.   |
| Email Header (From)   | View the author email address in the email header.  |
| Email Subject   | View the email subject of the suspicious email message.   |
|  | View the number of email messages with embedded malicious links.  |
|  | View the number of file attachments that are detected by policy rules.  |
| Threat  | View the name and classification of the discovered threat.  |
| Quarantine Reason   | <p>View the reason why an email message is quarantined.</p> <p>For more information, see <a href="#">Quarantine Reasons on page 4-31</a>.</p>   |

## Quarantine Search Filters

The following table explains the basic search filters for querying the quarantined email messages. To apply advanced filters, see [Applying Advanced Filters on page 4-10](#).

To view the quarantine, go to **Detections > Quarantine**.

**Note**

Search filters do not accept wildcards. Deep Discovery Email Inspector uses fuzzy logic to match search criteria to email message data.

---

| FILTER            | DESCRIPTION   |
|-------------------|---|
| Threat type       | Select <b>All</b> or a threat type from the list.<br>For details, see <a href="#">Threat Type Classifications on page 4-5</a> . |
| Risk level        | Select <b>All</b> or the email message risk level.  |
| Quarantine reason | Select <b>All</b> or a quarantine reason.   |
| Period            | Select a predefined time range or specify a custom range.   |

## Applying Advanced Filters

In addition to basic filters, you can apply advanced filters to query suspicious messages.

---

### Procedure

1. Click **Show advanced filters**.
2. Specify the information to filter.

| FILTER | DESCRIPTION                       |
|--------|-----------------------------------|
| Sender | Specify the sender email address. |

| FILTER              | DESCRIPTION  |
|---------------------|--|
| Email header (To)   | Specify a primary recipient email address in the email header.   |
| Message ID          | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com  |
| Subject             | Specify the email message subject.   |
| Direction           | Specify the message direction.   |
| Rule                | Specify a rule name.   |
| Email header (From) | Specify the author email address in the email header.  |
| URL                 | Specify a URL.   |
| Source IP           | <p>Specify the MTA IP address nearest to the email sender. The source IP is the IP address of the attack source, compromised MTA, or a botnet with mail relay capabilities.</p> <p>A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection.</p> <hr/> <div data-bbox="525 927 583 976"></div> <div data-bbox="596 924 1147 1052"> <p><b>Note</b></p> <p>The <b>Source IP</b> search filter requires an exact-string match. Deep Discovery Email Inspector does not use fuzzy logic to match search results for the source IP address.</p> </div> <hr/> |
| File name           | Specify an attachment file name.   |
| Data identifier     | Specify a data identifier name.  |
| YARA rule name      | Specify the name of a YARA rule.   |
| Recipient           | Specify a recipient email address. Only one address is allowed.  |

| FILTER                        | DESCRIPTION   |
|-------------------------------|---|
| Threat name                   | <p>Specify the threat name provided by Trend Micro. The dashboard widgets and the <b>Detections</b> tab provide information about threat names.</p> <p>For information about threat discovery capabilities, see <a href="#">Scanning / Analysis on page 8-9</a>.</p>  |
| Sender IP                     | <p>Specify the sender IP address.</p> <p>If you deploy Deep Discovery Email Inspector as an edge MTA in your network, the sender IP address is the public IP address of the external MTA nearest to your network.</p> <p>If you deploy Deep Discovery Email Inspector as a non-edge MTA in your network, the sender IP address is the IP address of the MTA nearest to the edge MTA relay server.</p> <hr/> <div data-bbox="427 699 485 748"></div> <p><b>Note</b></p> <p>The <b>Sender IP</b> search filter requires an exact-string match. Deep Discovery Email Inspector does not use fuzzy logic to match search results for the sender IP address.</p> <hr/> |
| Policy                        | Specify a policy name.  |
| DLP template                  | Specify a DLP template name.  |
| YARA rule file name           | Specify the name of a YARA rule file.   |
| Password-protected attachment | Select email messages that contain a password-protected file.   |
| Manual email submissions      | <p>Select email messages that are manually submitted to Deep Discovery Email Inspector for analysis by the administrator.</p> <p>For more information, see <a href="#">Email Submissions on page 8-29</a>.</p>  |

### 3. Click **Search**.

## Quarantine Reasons

The following table describes the quarantine reasons that display on the **Quarantine** screen.

| QUARANTINE REASON         | DESCRIPTION   |
|---------------------------|---|
| Content violation         | Messages with content that matches a content filtering rule.  |
| DLP incident              | Messages with one or more data loss prevention (DLP) policy violations.   |
| Malformed                 | Messages that cannot be opened for processing.  |
| Spam detection            | Messages that are detected as spam/graymail.  |
| Threat detection          | Messages that are detected to contain malware.  |
| Unscannable               | Messages that are not scannable.  |
| Unsuccessful encryption   | Messages that cannot be encrypted.  |
| Unsuccessful decryption   | Messages that cannot be decrypted.  |
| Virtual Analyzer error    | Messages that are not analyzed because of an unexpected error in Virtual Analyzer (for example, processing time-out). |
| Virtual Analyzer time-out | Messages that are not analyzed because of processing time-out in Virtual Analyzer.                                    |

## Investigating a Quarantined Email Message

### Procedure

1. Search for the email message.  
See [Viewing Quarantined Messages on page 4-26](#).
2. Click the arrow next to the email message in the table.  
The table row expands with more information.

3. Discover the email message details.

See [Quarantined Message Details on page 4-32](#).

4. Take action upon the quarantined message.

- Leave the message in the quarantine.






**Note**

Quarantined messages purge based on the settings configured on the **Storage Maintenance** screen.

For details, see [Configuring Storage Maintenance on page 8-224](#).

---

- Click  **Delete** to purge the email message from the quarantine.
  - Click  **Release** to deliver the email message.
  - Click  **Resume Process** to set Deep Discovery Email Inspector to continue message scanning from the last scan checkpoint.
- 



**Note**

Deep Discovery Email Inspector can only continue processing of messages that were quarantined due to spam detection, content violation, or DLP incidents.

---

- Click




**Unlock and Reprocess** to open password-protected files in unscannable messages using the specified password and the entire on the **File Passwords** screen, and perform threat scans on messages.

---

## Quarantined Message Details

The following table explains the email message details viewable after expanding the search results. The display fields vary depending on the type of detected threats.

| FIELD                        | DESCRIPTION   |
|------------------------------|---|
| View in Threat Connect       | Click <b>View in Threat Connect</b> 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.   |
| View Virtual Analyzer Report | Click <b>View Virtual Analyzer Report</b> to view the analysis report in HTML or PDF format.  |
| View Screenshot              | Click <b>View Screenshot</b> to safely display the email message as an image.   |
| Download                     | Select an option from the drop-down list to download the information for further investigation.   |
| Overview                     | <p>View the message ID, recipients, last detection time, sender and source IP addresses, and direction of the email message to understand where the message came from and other tracking information.</p> <hr/> <div>  <b>Note</b><br/>           For sender and source IP addresses, <b>Unknown</b> indicates that the detected messages are from an unknown origin (both the location and IP address information is not available), and <b>No data</b> indicates that the location information is not available.         </div> <hr/> <p>Get information about the policy rules that the email message violates.</p> |
| Messages                     | View the name of the scanning engine and the category for detected email messages that are considered as spam or graymail.  |
| Attachments                  | Get information about any files attached to the email message, including the file name, password, file type, risk level, SHA-1 and SHA-256 hash values, the scan engine that identified the threat, and the name of detected threats.   |
| YARA Detection               | Get information about the detected files based on matched YARA rules in the associated YARA rule files.   |

| FIELD                            | DESCRIPTION  |
|----------------------------------|--|
| Links                            | Get information about any embedded suspicious URLs that appeared in the email message, including the URL, site category, risk level, extraction source, the scan engine that identified the threat, and the name of detected threats.  |
| Message Characteristics          | Get information about any social engineering attack related characteristics that were detected in the email message, including the mail server reputation, gaps between transits, inconsistent recipient accounts, and forged sender addresses or unexpected relay servers, etc. |
| Content Keyword/Expression Match | Get information about the content keywords or expressions that are matched in the email message.   |
| DLP Incident                     | Get information about the data identifiers and DLP templates that are matched in the email message, message location, and forensic data.   |
| Email Header                     | View the email message header content.   |

## Sender Filtering/Authentication


You can view the list of blocked sender IP addresses and email addresses based on the following settings:

- Email Reputation
- DHA protection
- Bounce attack protection
- SMTP traffic throttling (IP address)
- SMTP traffic throttling (Email address)
- SPF
- DKIM
- DMARC
- User defined

## Viewing Sender Filtering/Authentication Detections

You can view the list of sender IP addresses and email address that Deep Discovery Email Inspector blocks on the **Sender Filtering/Authentication** screen under **Detections**.

### Procedure

1. Go to **Detections > Sender Filtering/Authentication**.
2. Specify one or more search criteria.
  - Select an option from the **Rule** drop-down list.
  - Sender email address or IP address and press ENTER or click the search icon (  ).
  - Select a period from the drop-down list.

All blocked sender email addresses or IP addresses matching the search criteria appear.

3. View the results.

| HEADER        | DESCRIPTION   |
|---------------|---|
| Detected      | View the date and time that Deep Discovery Email Inspector blocks messages from the sender based on a sender filtering/authentication rule. |
| IP Address    | View the sender IP address resolved domain IP address for the sender that Deep Discovery Email Inspector blocks.                            |
| Email Address | View the sender email address that Deep Discovery Email Inspector blocks.   |
| Recipients    | View the detected message recipient email addresses.  |
| Rule          | View the name of the sender filtering/authentication rule that is matched.  |
| Action        | View whether Deep Discovery Email Inspector blocks the sender address temporarily or permanently.   |

| HEADER | DESCRIPTION  |
|--------|--|
| Result | View the sender authentication result based on SPF, DKIM, or DMARC verification. |



**Tip**

You can click **Export** to save the query result to a comma-separated value file.

---

# Chapter 5

## Policies

Topics include:


- *About Policies on page 5-2*
- *Policy List on page 5-30*
- *Policy Rules on page 5-36*
- *Policy Objects on page 5-53*
- *Policy Exceptions on page 5-83*

## About Policies

A policy is a set of rules that Deep Discovery Email Inspector uses to evaluate email messages. Use policies to determine the actions applied to detected threats and unwanted contents in email messages.

You can configure policies in Deep Discovery Email Inspector to scan messages based on the message direction (inbound, outbound, or inbound or outbound).

The following table describes the required components for a policy.

| COMPONENT    | DESCRIPTION  |
|--------------|--|
| Policy rules | <p data-bbox="521 261 1069 313">You can create the following types of rules to enforce your organization's antivirus and other security goals:</p> <ul data-bbox="548 329 1170 618" style="list-style-type: none"><li data-bbox="548 329 1170 435">• Content filtering rules: Evaluates message contents to prevent undesirable content from being delivered to recipients and remove active content (such as macros) from Microsoft Office or PDF file attachments</li><li data-bbox="548 451 1170 503">• DLP rules: Prevents the transmission of digital assets through email messages</li><li data-bbox="548 519 1170 548">• Antispam rules: Scans messages for spam or graymail</li><li data-bbox="548 565 1170 618">• Threat protection rules: Scans messages for viruses and other malware such as spyware and worms</li></ul> <p data-bbox="521 634 1177 712">By default, Deep Discovery Email Inspector comes with a Default Policy that includes default rule settings to help protect your network from viruses and related Internet threats.</p> <hr data-bbox="521 748 1184 751"/> <div data-bbox="528 764 585 813"></div> <div data-bbox="599 764 650 784"><b>Note</b></div> <ul data-bbox="628 808 1180 1047" style="list-style-type: none"><li data-bbox="628 808 1180 898">• A threat protection rule does not protect against spam. For best protection against spam, configure an antispam rule and activate Sender Filtering.</li><li data-bbox="628 922 1180 1047">• To use the content filtering, data loss prevent (DLP), and antispam features, activate the license for Gateway Module. For more information, see <a href="#">Licenses on page 8-228</a>.</li></ul> |

| COMPONENT         | DESCRIPTION  |
|-------------------|--|
| Policy objects    | <p>You can configure the following types of objects to customize traffic handling behavior in policies:</p> <ul style="list-style-type: none"> <li>• Notifications</li> <li>• Message tags</li> <li>• Redirect pages</li> <li>• Data identifiers</li> <li>• DLP templates</li> <li>• Archive servers</li> </ul>  |
| Policy exceptions | <p>Policy exceptions reduce false positives. Configure exceptions to set the limits and actions for email encryption, or classify certain email messages as safe. Specify the safe senders, recipients, and X-header content, add files, URLs, IP addresses and domains, add URL keywords, or specify senders to bypass graymail scanning. Safe email messages are discarded (BCC and SPAN/TAP mode) or delivered to the recipient (MTA mode) without further investigation.</p> |

Follow the procedure to create policies in Deep Discovery Email Inspector:

1. (For content filtering and DLP rules) Create data identifiers.

For more information, see [Data Identifiers on page 5-62](#).

2. Create policy rules and notification templates.

For more information, see [Policy Rules on page 5-36](#) and [Configuring Recipient Notification on page 5-54](#).

3. Create policies to apply on target senders and recipients.

For more information, see [Configuring a Policy on page 5-31](#) and [Address Groups on page 5-81](#).

4. Specify trusted senders/recipients or objects for policy exceptions.

For more information, see [Policy Exceptions on page 5-83](#).

## General Message Scanning Order

When Deep Discovery Email Inspector receives an email message, Deep Discovery Email Inspector applies the scan settings on messages in the following order:

- Approved Senders list
- SMTP traffic throttling
- Sender filtering (Email Reputation Services (ERS), Directory Harvest Attack (DHA), and Bounce Attack)
- Domain-based message authentication (SPF, DKIM, and DMARC)
- Message-level exceptions
- Policy rules:
  - Content filtering rules
  - Data loss prevention (DLP) rules
  - Antispam protection rules
  - Advanced threat protection rules

**Note**

When you configure the Approved Senders and Blocked Senders lists for sender filtering/authentication, Deep Discovery Email Inspector applies settings to check the senders in the following order:

- For SMTP traffic throttling:
    - Approved Senders list (IP address)
    - Blocked Senders list (user-defined IP address)
    - SMTP traffic throttling (IP address)
    - Approved Senders list (email address)
    - Blocked Senders list (user-defined email address)
    - SMTP traffic throttling (email address)
  - For sender filtering (ERS, DHA, and Bounce Attack) and domain-based message authentication (SPF, DKIM, and DMARC):
    - Approved Senders list (IP address and email address)
    - Blocked Senders list (user-defined IP address and email address)
    - Sender filtering (ERS, DHA, Bounce Attack)
    - Domain-based message authentication (SPF, DKIM, and DMARC)
- 

## Policy Management Guidelines

Consider the following when configuring policies in Deep Discovery Email Inspector:

- Before you create a policy, create content filtering, data loss prevention (DLP), antispam, and threat protection rules.
- Activate the **Gateway Module** license to enable content filtering and antispam rules. Activate the **Threat Protection** license to enable threat protection rules. If the license for **Gateway Module** is not activated, Deep Discovery Email Inspector disables content filtering and antispam rules.

For more information, see [Licenses on page 8-228](#).

- If the domain of a sender address is in the internal domain list, Deep Discovery Email Inspector considers messages from the sender as outbound messages. Deep Discovery Email Inspector applies policies based on the message direction.
- When you configure multiple rules in a policy, Deep Discovery Email Inspector applies the rules on messages in the following order:
  - Content filtering rules
  - Data loss prevention (DLP) rules
  - Antispam protection rules
  - Advanced threat protection rules
- In policies, the terminal actions are **Delete message**, **Change recipient**, **Block and quarantine**, and **Deliver directly**. For policies with multiple rules, Deep Discovery Email Inspector applies only one terminal action on detected messages. After applying a terminal action on a message for a matched rule, Deep Discovery Email Inspector does not match the message against subsequent rules in the policy.

For more information, see [Policy Actions on page 5-8](#).

- To quarantine phishing messages, select **Quarantine the original message when attachments cannot be stripped** in a threat protection rule.

For more information, see [Configuring a Threat Protection Rule on page 5-50](#) and [Policy Actions on page 5-8](#).

- A policy must include one threat detection rule. Content filtering, DLP, and antispam rules are optional in a policy.
- If you specify multiple content filtering, data loss prevention (DLP), or antispam rules in a policy, you can set the rule matching priority.
- You can create a policy that applies to all incoming messages to any email addresses in your domain (for example, specify \*@domain.com for recipients).

- You can create a policy that applies to all outgoing messages from any email addresses in your domain (for example, specify \*@domain.com for senders).
- To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you create one policy that applies to inbound or outbound messages for all recipients and senders, and with the lowest priority in the **Policy List**.
- If Active Directory query times out or an email address is invalid for a message, Deep Discovery Email Inspector applies the policy for all recipients and senders to the message.
- If you configure more than one policy to apply to the same message direction for all recipients and senders in the **Policy List**, Deep Discovery Email Inspector applies the policy with the highest priority.


## Policy Actions

The following tables describe the actions Deep Discovery Email Inspector performs for the selected actions in a matched policy rule in each operating mode.

**TABLE 5-1. Actions and operation modes: Content filtering rules**

| ACTION         | OPERATION MODE  |   |   |
|----------------|---|---|---|
|                | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
| Delete message | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> <li>• Does not apply subsequent policy rules in the same policy on the email message</li> <li>• Does not deliver the email message</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> |

| ACTION                | OPERATION MODE  |   |   |
|-----------------------|---|---|---|
|                       | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
| Change recipient      | <ul style="list-style-type: none"> <li>• Delivers the email message to one or more recipients that you specify</li> <li>• Does not apply subsequent policy rules in the same policy on the email message</li> </ul>   | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                     | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                     |
| Block and quarantine  | <ul style="list-style-type: none"> <li>• Stores a copy in the quarantine area</li> <li>• Does not apply subsequent rules in the same policy on the email message until you resume the scanning process on the <b>Detections &gt; Quarantine</b> screen.</li> <li>• You can release a quarantined message using the web console</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                     | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                     |
| Strip all attachments | <ul style="list-style-type: none"> <li>• Replaces suspicious attachments with a text file</li> <li>• If configured, tags the email message subject and inserts the X-</li> </ul>  | <ul style="list-style-type: none"> <li>• Applies subsequent rules in the same policy on the email message.</li> </ul> | <ul style="list-style-type: none"> <li>• Applies subsequent rules in the same policy on the email message.</li> </ul> |

| ACTION       | OPERATION MODE   |  |  |
|--------------|--|--|--|
|              | MTA MODE   | SPAN/TAP MODE  | BCC MODE   |
|              | <p>header before delivery</p> <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message.</li> </ul> <hr/> <div>  <b>Note</b> </div> <p>Attachments and extracted URLs from attachments in detected email messages are not sent to Virtual Analyzer for analysis. Only extracted URLs from the message body and subject are sent to Virtual Analyzer for analysis.</p> <hr/> |  |  |
| Pass and tag | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> </ul>   | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> </ul> | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> </ul> |


| ACTION           | OPERATION MODE  |  |  |
|------------------|---|--|--|
|                  | MTA MODE  | SPAN/TAP MODE  | BCC MODE   |
|                  | <ul style="list-style-type: none"> <li>• If configured, tags the email message subject and inserts the X-header before delivery</li> </ul>  |  |  |
| Deliver directly | <ul style="list-style-type: none"> <li>• Does not apply subsequent policy rules in the same policy on the email message</li> <li>• Delivers the email message to the recipient (using the default SMTP server) or to the specified SMTP server</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                    | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul>                    |
| Encrypt message  | <ul style="list-style-type: none"> <li>• Encrypts messages after applying all other non-terminal actions</li> <li>• Applies subsequent rules in the same policy on the email message</li> </ul>   | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>   | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>   |
| Sanitize file    | <ul style="list-style-type: none"> <li>• Removes active content (such as macros) from Microsoft Office files</li> <li>• Applies subsequent rules</li> </ul>   | <ul style="list-style-type: none"> <li>• Applies subsequent rules in the same policy on the email message</li> </ul> | <ul style="list-style-type: none"> <li>• Applies subsequent rules in the same policy on the email message</li> </ul> |

| ACTION            | OPERATION MODE  |   |  |
|-------------------|---|---|--|
|                   | MTA MODE  | SPAN/TAP MODE   | BCC MODE   |
|                   | <p>in the same policy on the email message</p> <ul style="list-style-type: none"> <li>If configured, tags the email message subject and inserts the X-header before delivery</li> </ul> |   |  |
| BCC               | <ul style="list-style-type: none"> <li>Sends a blind carbon copy (BCC) of the email message to the specified recipient</li> </ul>   | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |
| Send notification | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul>                     | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul> | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |
| Insert stamp      | <ul style="list-style-type: none"> <li>If configured, inserts the selected stamp in to the body of detected email messages</li> </ul>   | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |

**TABLE 5-2. Actions and operation modes: Data loss prevention (DLP) rules**

| ACTION               | OPERATION MODE   |   |   |
|----------------------|--|---|---|
|                      | MTA MODE   | SPAN/TAP MODE   | BCC MODE  |
| Delete message       | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> <li>Does not apply subsequent policy rules in the same policy on the email message</li> <li>Does not deliver the email message</li> </ul>    | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Change recipient     | <ul style="list-style-type: none"> <li>Delivers the email message to one or more recipients that you specify</li> <li>Does not apply subsequent policy rules in the same policy on the email message</li> </ul>                        | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Block and quarantine | <ul style="list-style-type: none"> <li>Stores a copy in the quarantine area</li> <li>Does not apply subsequent rules in the same policy on the email message until you resume the scanning process on the <b>Detections</b></li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |

| ACTION                | OPERATION MODE  |   |   |
|-----------------------|---|---|---|
|                       | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
|                       | <ul style="list-style-type: none"><li>&gt; <b>Quarantine</b> screen.</li><li>• You can release a quarantined message using the web console</li></ul>  |   |   |
| Strip all attachments | <ul style="list-style-type: none"><li>• Replaces suspicious attachments with a text file</li><li>• Applies subsequent rules in the same policy on the email message.</li><li>• If configured, tags the email message subject and inserts the X-header before delivery</li></ul> | <ul style="list-style-type: none"><li>• Applies subsequent rules in the same policy on the email message.</li></ul> | <ul style="list-style-type: none"><li>• Applies subsequent rules in the same policy on the email message.</li></ul> |

| ACTION       | OPERATION MODE  |  |  |
|--------------|---|--|--|
|              | MTA MODE  | SPAN/TAP MODE  | BCC MODE   |
|              |  <b>Note</b><br>Attachments and extracted URLs from attachments in detected email messages are not sent to Virtual Analyzer for analysis. Only extracted URLs from the message body and subject are sent to Virtual Analyzer for analysis. |  |  |
| Pass and tag | <ul style="list-style-type: none"><li>• Applies subsequent rules in the same policy on the email message</li><li>• If configured, tags the email message subject and inserts the X-header before delivery</li></ul>   | <ul style="list-style-type: none"><li>• Applies subsequent rules in the same policy on the email message</li></ul> | <ul style="list-style-type: none"><li>• Applies subsequent rules in the same policy on the email message</li></ul> |

| ACTION            | OPERATION MODE  |   |   |
|-------------------|---|---|---|
|                   | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
| Deliver directly  | <ul style="list-style-type: none"> <li>Does not apply subsequent policy rules in the same policy on the email message</li> <li>Delivers the email message to the recipient (using the default SMTP server) or to the specified SMTP server</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul>   | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Encrypt message   | <ul style="list-style-type: none"> <li>Encrypts messages after applying all other non-terminal actions</li> <li>Applies subsequent rules in the same policy on the email message</li> </ul>   | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>                                |
| BCC               | <ul style="list-style-type: none"> <li>Sends a blind carbon copy (BCC) of the email message to the specified recipient</li> </ul>   | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>                                |
| Send notification | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the</li> </ul>   | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the</li> </ul> | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>                                |

| ACTION       | OPERATION MODE  |  |  |
|--------------|---|--|--|
|              | MTA MODE  | SPAN/TAP MODE  | BCC MODE   |
|              | notification template   | notification template  |  |
| Insert stamp | <ul style="list-style-type: none"> <li>If configured, inserts the selected stamp in to the body of detected email messages</li> </ul> | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |

**TABLE 5-3. Actions and operation modes: Antispam rules**

| ACTION           | OPERATION MODE  |   |   |
|------------------|---|---|---|
|                  | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
| Delete message   | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> <li>Does not apply subsequent policy rules in the same policy on the email message</li> <li>Does not deliver the email message</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Change recipient | <ul style="list-style-type: none"> <li>Delivers the email message to one or more recipients that you specify</li> <li>Does not apply subsequent policy rules in the same policy on the email message</li> </ul>                     | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |

| ACTION               | OPERATION MODE  |  |  |
|----------------------|---|--|--|
|                      | MTA MODE  | SPAN/TAP MODE  | BCC MODE   |
| Block and quarantine | <ul style="list-style-type: none"> <li>Stores a copy in the quarantine area</li> <li>Does not apply subsequent rules in the same policy on the email message until you resume the scanning process on the <b>Detections &gt; Quarantine</b> screen.</li> <li>You can release a quarantined message using the web console</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul>                    | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul>                    |
| Pass and tag         | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> <li>If configured, tags the email message subject and inserts the X-header before delivery</li> </ul>  | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> </ul> | <ul style="list-style-type: none"> <li>Applies subsequent rules in the same policy on the email message</li> </ul> |
| Deliver directly     | <ul style="list-style-type: none"> <li>Does not apply subsequent policy rules in the same policy on the email message</li> <li>Delivers the email message to the</li> </ul>   | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul>                    | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul>                    |

| ACTION            | OPERATION MODE  |   |  |
|-------------------|---|---|--|
|                   | MTA MODE  | SPAN/TAP MODE   | BCC MODE   |
|                   | recipient (using the default SMTP server) or to the specified SMTP server   |   |  |
| BCC               | <ul style="list-style-type: none"> <li>Sends a blind carbon copy (BCC) of the email message to the specified recipient</li> </ul>                                   | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |
| Send notification | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul> | <ul style="list-style-type: none"> <li>Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul> | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |
| Insert stamp      | <ul style="list-style-type: none"> <li>If configured, inserts the selected stamp in to the body of detected email messages</li> </ul>                               | <ul style="list-style-type: none"> <li>Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>Not applicable</li> </ul> |

**TABLE 5-4. Actions and operation modes: Threat protection rules**

| ACTION         | OPERATION MODE  |   |   |
|----------------|---|---|---|
|                | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
| Delete message | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |

| ACTION  | OPERATION MODE  |   |   |
|---|---|---|---|
|   | MTA MODE  | SPAN/TAP MODE   | BCC MODE  |
|   | <ul style="list-style-type: none"> <li>Does not deliver the email message</li> </ul>  |   |   |
| Change recipient  | <ul style="list-style-type: none"> <li>Delivers the email message to one or more recipients that you specify</li> <li>Does not apply subsequent policy rules in the same policy on the email message</li> </ul>   | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Block and quarantine  | <ul style="list-style-type: none"> <li>Stores a copy in the quarantine area</li> <li>Does not deliver the email message</li> </ul>  | <ul style="list-style-type: none"> <li>Stores a copy in the quarantine area</li> </ul>          | <ul style="list-style-type: none"> <li>Stores a copy in the quarantine area</li> </ul>          |
| Strip attachments, redirect links to blocking page, and tag | <ul style="list-style-type: none"> <li>Replaces suspicious attachments with a text file</li> <li>Redirects suspicious links to a blocking page</li> <li>If configured, tags the email message subject and inserts the X-header before delivery</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |
| Strip attachments, redirect links to                        | <ul style="list-style-type: none"> <li>Replaces suspicious</li> </ul>   | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>Deletes the email message from the mail queue</li> </ul> |

| ACTION   | OPERATION MODE   |   |   |
|--|--|---|---|
|  | MTA MODE   | SPAN/TAP MODE   | BCC MODE  |
| warning page, and tag                            | attachments with a text file <ul style="list-style-type: none"> <li>• Redirects suspicious links to a warning page</li> <li>• If configured, tags the email message subject and inserts the X-header before delivery</li> <li>• Delivers the email message to the recipient</li> </ul> |   |   |
| Pass and tag                                     | <ul style="list-style-type: none"> <li>• If configured, tags the email message subject and inserts the X-header before delivery</li> </ul>   | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> |
| Deliver directly                                 | <ul style="list-style-type: none"> <li>• Does not apply subsequent policy rules in the same policy on the email message</li> <li>• Delivers the email message to the recipient using the specified SMTP server</li> </ul>  | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> | <ul style="list-style-type: none"> <li>• Deletes the email message from the mail queue</li> </ul> |
| Quarantine the original message when attachments | <ul style="list-style-type: none"> <li>• If no strip attachment action is specified or no attachment</li> </ul>  | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>                                | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>                                |

| ACTION  | OPERATION MODE  |   |  |
|---|---|---|--|
|   | MTA MODE  | SPAN/TAP MODE   | BCC MODE   |
| cannot be stripped  | exists, sends the message to the quarantine area  |   |  |
| Quarantine a copy of the original message when stripping attachments or redirecting links | <ul style="list-style-type: none"> <li>• If a strip attachment action or a redirect link is specified, stores a copy in the quarantine area</li> </ul>  | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul> |
| Attempt to clean before stripping attachments   | <ul style="list-style-type: none"> <li>• If a strip attachment action is specified, performs the clean attachment action</li> <li>• If the clean attachment action is not successful or no strip attachment action is selected, deletes the attachment</li> </ul> | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul> |
| Send notification   | <ul style="list-style-type: none"> <li>• Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul>   | <ul style="list-style-type: none"> <li>• Sends a notification to all message recipients and contact email addresses specified in the notification template</li> </ul> | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul> |
| BCC   | <ul style="list-style-type: none"> <li>• Sends a blind carbon copy</li> </ul>   | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul>  | <ul style="list-style-type: none"> <li>• Not applicable</li> </ul> |

| ACTION       | OPERATION MODE  |  |  |
|--------------|---|--|--|
|              | MTA MODE  | SPAN/TAP MODE  | BCC MODE   |
|              | (BCC) of the email message to the specified recipient   |  |  |
| Insert stamp | <ul style="list-style-type: none"><li>• If configured, inserts the selected stamp in to the body of detected email messages</li></ul> | <ul style="list-style-type: none"><li>• Not applicable</li></ul> | <ul style="list-style-type: none"><li>• Not applicable</li></ul> |

**Note**

- In policies, the terminal actions are **Delete message**, **Change recipient**, **Block and quarantine**, and **Deliver directly**. For policies with multiple rules, Deep Discovery Email Inspector applies only one terminal action on detected messages. After applying a terminal action on a message for a matched rule, Deep Discovery Email Inspector does not match the message against subsequent rules in the policy.

For example, if a policy contains one content filtering rule, one antisпам protection rule, and one threat protection rule, and Deep Discovery Email Inspector applies the **Delete message** action on a message based on the content filtering rule matched, Deep Discovery Email Inspector does not apply the antisпам and threat protection rules on the message.

- For policies with multiple rules, Deep Discovery Email Inspector applies all non-terminal actions on messages for matched rules before delivery or until a terminal action is applied.

As an example, you configure a policy containing one or more content filtering rules, one or more data loss prevention (DLP) rules, one or more antisпам rules, and one threat protection rule. If Deep Discovery Email Inspector applies the **Strip all attachments** action on a message based on the content filtering rule or DLP rule that is first matched, Deep Discovery Email Inspector will continue to scan the messages until a terminal action or all subsequent rules are applied (except Virtual Analyzer submission for attachments).

If Deep Discovery Email Inspector does not apply a strip attachment action on a message based on one or more preceding rules matched, Deep Discovery Email Inspector will continue to scan the messages until a terminal action or all subsequent rules are applied (including Virtual Analyzer submission for attachments).

- When applying multiple actions on a message, Deep Discovery Email Inspector applies the **Encrypt message** action as the last non-terminal action.
- Deep Discovery Email Inspector performs the BCC action after applying all other terminal or non-terminal actions.

## Policy Matching


Deep Discovery Email Inspector first determines the message direction (inbound or outbound) based on the Internal Domains list to apply policies. For more information, see [Internal Domains on page 8-107](#).

If more than one policy applies to a recipient or sender, Deep Discovery Email Inspector matches the enabled policy with the highest priority and applies the associated actions.

For example, consider the following policies.

**TABLE 5-5. Example policies**

| PRIORITY | POLICY NAME                   | TARGET  | DIRECTION |
|----------|-------------------------------|---|-----------|
| 1        | High_Profile_Recipient        | Recipients: <ul style="list-style-type: none"> <li>ceo@example.com</li> <li>cfo@example.com</li> </ul>  | Inbound   |
| 2        | High_Profile_Recipient_Sender | Sender: jim@partner.com<br>Recipients: <ul style="list-style-type: none"> <li>finance_group (Active Directory)</li> <li>alex@example.com</li> </ul> | Inbound   |
| 3        | Trusted_Partner               | Senders: *@partner.com<br>Sender exception:<br>john_doe@partner.com   | Inbound   |
| 4        | Sales_Team                    | Recipients: <ul style="list-style-type: none"> <li>joe@example.com</li> <li>larry@exmple.com</li> </ul>   | Inbound   |
| 5        | IT_Team                       | Recipients: IT_group (Active Directory)   | Inbound   |
| 6        | Acquired_Domain               | Recipients: *@example.com   | Inbound   |

| PRIORITY | POLICY NAME     | TARGET   | DIRECTION           |
|----------|-----------------|--|---------------------|
| 7        | Outbound policy | <p>Senders: *@example.com</p> <hr/> <div>  <b>Note</b><br/>           The domain "example.com" is in the Internal Domains list.         </div> <hr/> <p>Recipient exception:<br/>jane_doe@partner.com</p> | Outbound            |
| 8        | Default policy  | All recipients and senders   | Inbound or outbound |

The following describes how Deep Discovery Email Inspector matches the policies in a top-down approach based on the message direction and priority settings:

- A message from leo@partner.com to the recipient (joe@example.com) matches the policy *Trusted\_Partner*, because this is an inbound message (the domain "partner.com" is not in the Internal Domains list) and the priority for the *Trusted\_Partner* inbound policy (matching the sender setting: \*@partner.com) is higher than the *Sales\_Team* inbound policy (matching the recipient setting: joe@example.com).
- If a message is sent from jim@partner.com to three recipients (ceo@example.com, alex@example.com, and joe@example.com), Deep Discovery Email Inspector considers the message as an inbound message (the domain "partner.com" is not in the Internal Domains list) and matches the following inbound policies:
  - *High\_Profile\_Recipient*: Matching the inbound message direction and recipient ceo@example.com
  - *High\_Profile\_Recipient\_Sender*: Matching the inbound message direction and recipient alex@example.com

- *Trusted\_Partner*: Matching the inbound message direction and recipient joe@exmple.com
- If a message is sent from joe@yahoo.com to four recipients (larry@example.com, alex@example.com, bill@example.com, and jane@newdomain.com) and only bill@example.com belongs to the IT\_Team Active Directory group, Deep Discovery Email Inspector considers the message as an inbound message (the domain "yahoo.com" is not in the Internal Domains list) and matches the following policies:
  - *Sales\_Team*: Matching the inbound message direction and recipient larry@exmple.com
  - *Acquired\_Domain*: Matching the inbound message direction and recipient alex@example.com
  - *IT\_Team*: Matching the inbound message direction and recipient bill@example.com
  - *Default policy*: Matching the inbound message direction and recipient jane@newdomain.com
- If a message is sent from alex@example.com to two recipients (larry@example.com and jane@newdomain.com ), Deep Discovery Email Inspector considers the message as an outbound message (the domain "example.com" is in the Internal Domains list) and matches the *Outbound policy* that has a higher priority than the *Default policy* (matching outbound message direction, sender, and recipients).
- If a message is sent from john\_doe@partner.com to the recipient henry@example.com, Deep Discovery Email Inspector considers the message as an inbound message but only the *Acquired\_Domain* is matched since the sender address john\_doe@partner.com is on the exception list for the policy *Trusted\_Partner*.
- If a message is sent from ceo@example.com to the recipient jane\_doe@partner.com, Deep Discovery Email Inspector considers the message as an outbound message but only the *Default policy* is matched since the recipient address jane\_doe@partner.com is on the exception list for the policy *Outbound policy*.

**Note**

Message splintering occurs when a message with multiple recipients results in multiple policy and policy rule matches in Deep Discovery Email Inspector.

For more information, see [Policy Splintering on page 5-28](#).

## Policy Splintering

Deep Discovery Email Inspector includes the intelligent message splintering feature to enable multiple independent policy matches for a message with multiple recipients. Message splintering allows Deep Discovery Email Inspector to evaluate each recipient against the policy list in a top-down fashion. When a policy is matched, Deep Discovery Email Inspector splits the message (creating message splinters) into multiple messages for the number of affected recipients.

Deep Discovery Email Inspector creates a message splinter only if a message with multiple recipients matches different policy rules in different policies. If all recipients in a message match the same policy or if recipients match the same policy rule in different policies, Deep Discovery Email Inspector does not create a message splinter.

Consider the following policies.

| POLICY NAME | RULE   |
|-------------|--|
| Policy A    | <ul style="list-style-type: none"><li>• Content filter Rule: Tag messages (keyword match)</li><li>• Spam filter Rule: Delete spam messages</li><li>• Threat protection Rule: Delete messages (all risk levels)</li></ul> |
| Policy B    | <ul style="list-style-type: none"><li>• Content filter Rule: Strip attachments (executable)</li><li>• Spam filter Rule: Tag spam messages</li><li>• Threat protection Rule: Delete messages (all risk levels)</li></ul>  |

| POLICY NAME | RULE  |
|-------------|---|
| Policy C    | <ul style="list-style-type: none"><li>• Content filter Rule: Tag messages (keyword match)</li><li>• Content filter Rule: Strip attachments (executable)</li><li>• Spam filter Rule: Tag spam messages</li><li>• Threat protection Rule: Quarantine messages (all risk levels)</li></ul> |
| Policy D    | <ul style="list-style-type: none"><li>• Content filter Rule: Tag messages (keyword match)</li><li>• Threat protection Rule: Quarantine messages (all risk levels)</li></ul>   |

The following scenarios describe how Deep Discovery Email Inspector creates message splinters based on the policy and rule matching:

- A message is sent from joe@test.com to recipients alex@example.com and linda@example.com. If alex@example.com and linda@example.com match *Policy A*, and the message triggers content filtering rule *Tag messages (keyword match)*, Deep Discovery Email Inspector does not create a message splinter because the same policy rule is applied for the same policy matched.
- A message is sent from joe@test.com to recipients jane@example.com, mark@example.com, and leo@example.com. If jane@example.com and mark@example.com match *Policy B*, and leo@example.com matches *Policy C*, and the message triggers policy rules *Strip attachments (executable)* and *Tag spam messages*, Deep Discovery Email Inspector does not create a message splinter because the same policy rules are applied for the matched policies.
- A message is sent from joe@test.com to recipients jane@example.com and bill@example.com. If jane@example.com matches *Policy B* and bill@example.com matches *Policy D*, and the message triggers policy rules *Tag spam messages* and *Tag messages (keyword match)*, Deep Discovery Email Inspector splits the message into two. Deep Discovery Email Inspector applies policy rule *Tag spam messages* to one message for jane@example.com and applies policy rule *Tag messages (keyword match)* to the other message for bill@example.com.

## Policy List

Deep Discovery Email Inspector evaluates email messages against the rules defined in policies. You can enforce specific policies on individual or a group of senders or recipients. Deep Discovery Email Inspector matches the policies based on the sender and recipient information in messages and the message directions. When more than one policy is matched for a message, Deep Discovery Email Inspector takes the action of the matched policy rule with the highest priority.

The following table describes the information on the **Policy List** screen.




| FIELD                  | DESCRIPTION  |
|------------------------|--|
| Priority               | View the number to indicate the priority level of the policy. The smaller the number, the higher the priority. |
| Policy Name            | View the name of the policy.   |
| Direction              | View the message direction the policy applies to.  |
| Senders and Recipients | View the list of senders and recipients to which the policy is applied.  |
| Rules                  | View the list of rules included in the policy.   |
| Archive Server         | View the name of the server to archive messages.   |
| Last Updated           | View the date and time the policy is updated.  |
| Description            | View a description for the policy.   |
| Status                 | Toggle to enable or disable the policy.  |

The following table explains the basic search filters for querying policies.

**Note**

For the **Sender** and **Recipient** search filters, it is recommended you specify a complete email address or the local part. Based on the filters, Deep Discovery Email Inspector searches for sender and recipient email addresses and Active Directory users and groups in policies.

---

| FILTER     | DESCRIPTION  |
|------------|--|
| Status     | Select <b>All</b> or a status from the list.   |
| Direction  | Select the message direction the policy applies to.  |
| Exceptions | Select an exception setting ( <b>None</b> or <b>Specified</b> ) to filter the policies in the list.  |
| Sender     | Type a complete sender email address and click the search icon (  ).  |
| Recipient  | Type a complete recipient email address and click the search icon (  ). |
| Rule       | Type a rule name and click the search icon (  ).                        |
|            | The screen displays the entries that contain the text.   |

You can perform the following actions on the **Policy List** screen:

- **Add:** Creates a new policy
- **Export:** Downloads the policies in a ZIP file
- **Import:** Imports policies that you exported from a source Deep Discovery Email Inspector appliance. This allows you to replicate the same policy settings across several Deep Discovery Email Inspector appliances.
- **Delete:** Removes the selected policy from the policy list.
- **Copy:** Creates a copy of the selected policy. You can edit the copy to create a customized policy.

## Configuring a Policy

You can configure policies to reduce security and productivity threats to your messaging system.

A policy requires the following configuration:

- **General settings:** Specifies the policy name and the hosts to apply the policy

- Policy rule selection:
  - One threat protection rule
  - (Optional) One or more content filtering, data loss prevention (DLP), or antispy rules

**Note**

- Before configuring a policy, make sure that you have created the required policy components (internal domains, notifications, and policy rules).
- You can specify trusted senders/recipients or objects for policy exceptions.

For more information, see [Policy Exceptions on page 5-83](#).

---

---

**Procedure**

1. Configure the required policy components:

- [Notifications on page 5-54](#)
- [Policy Rules on page 5-36](#)

2. Go to **Policies > Policy Management**.

The **Policy List** screen appears.

3. Do one of the following:

- Click **Add** to create a new policy.
- Click a policy name to edit the settings.

4. Select **Enabled** to activate the policy.

5. Type a policy name.

6. Type a number to indicate the priority in which Deep Discovery Email Inspector performs the scan. Deep Discovery Email Inspector applies the policy rules to messages according to the order you specify.

7. Type a description for the policy.
8. Select the message direction for the policy.
9. Specify the senders and recipients. Do one of the following:
  - Select **All** to apply the policy rules to all senders or recipients
  - Select **Specify senders** or **Specify recipients** and complete the following steps to configure the address list.

**Note**

If the domain of a sender is in the Internal Domains list, Deep Discovery Email Inspector does not apply the inbound policy on messages from the sender.

- a. Select a type and provide the required information
- b. Type the required information.

| TYPE               | DESCRIPTION  |
|--------------------|--|
| Email address      | Type a valid email address.<br>For example, test@test.com.   |
| LDAP user or group | Type a user or group name and press [Enter] to search for matching user accounts or groups.  |
| Address group      | Type an address group name and press [Enter] to search for matching address groups.<br><br>You can configure address groups to apply the same policies to multiple email addresses.<br><br>For more information, see <a href="#">Configuring an Address Group on page 5-82</a> . |

- c. If required, select an address group or an LDAP user or group from the search results.
- d. Click **Add**.

10. (Optional) Under **Exceptions**, you can configure Deep Discovery Email Inspector to bypass policy scanning for messages with the specified sender-recipient address pair. Complete the following steps:

- a. Select **Specify exceptions**.
- a. From the **From (sender)** and **To (recipient)** drop-down lists, select an option and provide the required information.

| TYPE               | DESCRIPTION  |
|--------------------|--|
| Any                | Select this option to include all sender or recipient email addresses.   |
| Email address      | Type a valid email address.<br>For example, test@test.com.   |
| LDAP user or group | Type a user or group name and press [Enter] to search for matching user accounts or groups.  |
| Address group      | Type an address group name and press [Enter] to search for matching address groups.<br><br>You can configure address groups to apply the same policies to multiple email addresses.<br><br>For more information, see <a href="#">Configuring an Address Group on page 5-82</a> . |

- b. If required, select an address group or an LDAP user or group from the search results.
  - c. Click **Add**.
11. (Optional) Select an option from the **Archive Server** drop-down list to archive a copy of the messages that match the policy. The default option (**None**) disables message archiving.

**Note**

- If a message matches multiple policies with different archive server settings, Deep Discovery Email Inspector sends a copy of the message to each archive server.
  - If a message matches multiple policies with the same archive server setting, Deep Discovery Email Inspector only sends a copy of the message to the archive server.
- 

For more information, see [Archive Servers on page 5-60](#).

**12.** Specify the threat protection rule.

- a. Click the **Threat Protection** tab.
- b. Select an option from the **Rule** drop-down list.
- c. Click **Add**.

**Note**

- To view the rule settings, click **View**.
  - For more information about configuring threat protection rules, see [Threat Protection Rules on page 5-49](#).
- 

**13.** (Optional) Specify one or more content filtering rules.

- a. Click the **Content Filtering** tab.
- b. Select an option from the **Rule** drop-down list.
- c. Click **Add**.

**Note**

- To view the rule settings, click **View**.
  - For more information about configuring content filtering rules, see [Content Filtering Rules on page 5-37](#).
-

**14.** (Optional) Specify one or more data loss prevention (DLP) rules.

- a.** Click the **DLP** tab.
- b.** Select an option from the **Rule** drop-down list.
- c.** Click **Add**.



**Note**

- To view the rule settings, click **View**.
  - For more information about configuring DLP rules, see [Data Loss Prevention \(DLP\) Rules on page 5-43](#).
- 

**15.** (Optional) Specify one or more antispam rules.

- a.** Click the **Antispam** tab.
- b.** Select an option from the **Rule** drop-down list.
- c.** Click **Add**.



**Note**

- To view the rule settings, click **View**.
  - For more information about configuring antispam rules, see [Antispam Rules on page 5-45](#).
- 

**16.** Click **Save**.

---

## Policy Rules

You can create the following types of rules to enforce your organization's antivirus and other security goals:

- **Content filtering rules:** Evaluates message contents to prevent undesirable content from being delivered to recipients and remove active content (such as macros) from Microsoft Office or PDF file attachments

- DLP rules: Prevents the transmission of digital assets through email messages
- Antispam rules: Scans messages for spam or graymail
- Threat protection rules: Scans messages for viruses and other malware such as spyware and worms

Optionally, you can copy a predefined policy rule and edit the copy to create a new policy rule.

## Content Filtering Rules

Content filtering rules allow you to evaluate and control the delivery of email message on the basis of the message content and attachments. Deep Discovery Email Inspector uses content filtering rules to monitor inbound and outbound messages to check for messages with potentially malicious attachments or the existence of harassing, offensive, or otherwise objectionable message content.

When Deep Discovery Email Inspector detects a message that matches a scanning condition defined in a content filtering rule, Deep Discovery Email Inspector takes action on the message to prevent undesirable content from being delivered to Microsoft Exchange clients.

You can view the list of content filtering rules on the **Content Filtering Rules** screen. The following table describes the rule information.

| FIELD               | DESCRIPTION   |
|---------------------|---|
| Rule Name           | View the descriptive name for the rule.<br>Click a rule name to edit the rule settings. |
| Action              | View one or more actions to apply when the rule conditions are matched.                 |
| Associated Policies | View the number of policies that include the rule.                                      |
| Last Updated        | View the date and time the entry was last updated.                                      |

## Configuring a Content Filtering Rule

You can create content filtering rules to evaluate inbound and outbound email messages based on the following scanning conditions:

- Attachment file types, file names, file size, or the number of attachments
- Content in email headers, body, or attachments
- Sender authentication results
- Internal domains and permitted sender addresses

---

### Procedure

1. Go to **Policies > Policy Management**.

2. Click the **Content Filtering Rules** tab.

3. Do one of the following:

- Click **Add** to create a new rule.
- Click a rule name to change the settings.

4. Type a rule name.

5. Configure the scanning conditions.

a. Under **Attachment**, specify the criteria for attachments.

For more information, see [Scanning Conditions for Attachments on page 5-41](#).

b. Under **Content**, specify one or more keywords or expressions to match in messages.

For more information, see [Adding Keyword Lists or Expressions on page 5-42](#).

c. Under **Sender Authentication Results**, select one or more sender authentication protocols; then, select one or more authentication results from the drop-down list.

**Note**

- For sender authentication result settings in content filtering rules to take effect, go to **Administration > Sender Filtering/Authentication** and click the tab for the authentication protocol (**SPF**, **DKIM Authentication**, or **DMARC**). Then, enable the authentication protocol and select **Insert X-Header into email messages**.
- Deep Discovery Email Inspector matches an email message if an authentication result for each selected sender authentication protocol is matched.

- d. (Optional) Select **Apply rule if sender address does not match message header (From)** to apply the content filtering rule if the sender address and the address in the message header From field do not match.

**Note**

This option is not applicable when Deep Discovery Email Inspector is operating in BCC mode.

- e. (Optional) To detect messages with an internal domain but do not originate from a permitted sender address, select **Enable internal email spoofing prevention** and specify the domain and IP address matching options.
- **Domain matching:** Select an option to match the message envelop sender or header FROM address against the internal domains list.  
  
If a match is found, Deep Discovery Email Inspector continues to check the message sender or source IP address.
  - **IP address matching:** Select an option to match the message sender IP address, source IP address, or both sender and source IP addresses against the permitted sender address list.

If a match is not found, Deep Discovery Email Inspector considers this message an internal email spoofing attempt and applies the rule action.



**Note**

You can configure the internal domains list on the **Internal Domains** screen and the permitted sender IP addresses on the **Limits and Exceptions** screen.

For more information, see [Internal Domains on page 8-107](#) and [Configuring Limits and Exceptions on page 8-101](#).

---

6. Specify the **Action**.

For more information, see [Policy Actions on page 5-8](#).

7. (Optional) To send a blind carbon copy of detected messages to one or more recipients, type the recipient email addresses in the **BCC** field.



**Note**

You can specify up to 50 email addresses. Wildcard characters are not supported.

---

8. (Optional) From the **Send notification** drop-down list, select a notification message to inform recipients about the applied policy action.



**Important**

Deep Discovery Email Inspector only sends recipient notifications when you select **Send notification** and a notification message.

---

You can configure notification messages on the **Notifications** screen (go to **Policies > Policy Objects > Notifications**).

For more information, see [Configuring Recipient Notification on page 5-54](#).

9. (Optional) From the **Insert stamp** drop-down list, select a stamp that you want to insert in to detected messages.

For more information, see [Configuring a Message Stamp on page 5-57](#).


10. Click **Save**.


After adding a rule, you can:

- Click a rule name to edit the rule settings.
- Select a rule and click **Delete** to remove the selected rule.

## Scanning Conditions for Attachments

In content filtering rules, you can specify the following scanning conditions to filter email messages with attachments. Deep Discovery Email Inspector matches an email message when all conditions are met.

| SETTING   | DESCRIPTION  |
|-----------|--|
| File type | <p>Select this option to filter email messages based on the matching option and file types:</p> <ul style="list-style-type: none"> <li>• Matching option:             <ul style="list-style-type: none"> <li>• <b>Selected attachment types:</b> Deep Discovery Email Inspector takes action on messages with attachments of the selected file types.</li> <li>• <b>Not the selected attachment types:</b> Deep Discovery Email Inspector takes action on messages with attachments that are not of the selected file types.</li> </ul> </li> <li>• File types:             <ul style="list-style-type: none"> <li>• True file types</li> <li>• Custom file extensions</li> <li>• Password-protected archive files</li> </ul> </li> </ul> <hr/> <div>  <b>Note</b><br/>           Do not include wildcards in a custom file extension.         </div> |

| SETTING               | DESCRIPTION   |
|-----------------------|---|
| File name             | <p>Select this option to filter email messages based on file names.</p> <p>Type a file name and press Enter. You can specify more than one file name in the text field.</p> <hr/> <p> <b>Note</b><br/>Do not include wildcards in a file name.</p> |
| Attachment size       | <p>Select this option and configure the following settings to filter email messages based on the attachment size:</p> <ul style="list-style-type: none"> <li>• Select a comparison symbol</li> <li>• Type a number to represent the attachment size</li> <li>• Select a unit (KB or MB)</li> </ul>                                  |
| Number of attachments | <p>Select this option and configure the following settings to filter email messages based on the number of attachments detected:</p> <ul style="list-style-type: none"> <li>• Select a comparison symbol</li> <li>• Type a number to represent the number of attachments</li> </ul>   |

## Adding Keyword Lists or Expressions

You can select one or more keyword lists (containing the keywords) and expressions to match in email messages.



### Note

Before you can add keyword lists or expressions in a content filtering rule, configure the keyword lists or expressions on the **Data Identifiers** screen.

For more information, see [Configuring a Keyword List on page 5-74](#) and [Configuring a Customized Expression on page 5-66](#).

## Procedure

1. Under **Contents**, click **Add**.

The **Add Keyword List & Expression** screen appears.

2. Select a message section.
3. Configure the required settings for the message section you select.
  - For the **Header** message section, do the following:
    - a. Select or specify a message header.
    - b. Select a list view option.
    - c. Select one or more keyword lists or expressions.
    - d. Click **Add**.

**Tip**

- Repeat the procedure to add more content matching entries.
- You can click the trash can icon (🗑️) to remove an entry from the table.

- 
- For the **Body** or **Attachment** message section, do the following:
      - a. Select a list view option.
      - b. Select one or more keyword lists or expressions.
  4. Click **Save**.
- 

## Data Loss Prevention (DLP) Rules

Deep Discovery Email Inspector evaluates a file or data against a set of Data Loss Prevent (DLP) rules in policies. DLP rules determine files or data that requires protection from unauthorized transmission and the action that Deep Discovery Email Inspector performs after detecting a transmission.

You can start to configure DLP rules after you have configured data identifiers and organized them in DLP templates.

**Note**

By default, Deep Discovery Email Inspector applies DLP policies on outgoing email messages based on the recipient and sender settings.

---

## Configuring a DLP Rule

You can create a Data Loss Prevention (DLP) rule to specify actions to apply when Deep Discovery Email Inspector detects an unauthorized transmission of data in email messages.

---

### Procedure

1. Go to **Policies > Policy Management**.
2. Click the **DLP Rules** tab.
3. Do one of the following:
  - Click **Add** to create a new rule.
  - Click a rule name to change the settings.
4. Type a rule name.
5. Select a list view option.
6. Select one or more templates in the **Available Templates** list.  
The selected items display in the **Selected Templates** list.
7. Specify the **Action**.

For more information, see [Policy Actions on page 5-8](#).

8. (Optional) To send a blind carbon copy of detected messages to one or more recipients, type the recipient email addresses in the **BCC** field.

**Note**

You can specify up to 50 email addresses. Wildcard characters are not supported.

---

9. (Optional) From the **Send notification** drop-down list, select a notification message to inform recipients about the applied policy action.

**Important**

Deep Discovery Email Inspector only sends recipient notifications when you select **Send notification** and a notification message.

---

You can configure notification messages on the **Notifications** screen (go to **Policies > Policy Objects > Notifications**).

For more information, see [Configuring Recipient Notification on page 5-54](#).

10. (Optional) From the **Insert stamp** drop-down list, select a stamp that you want to insert in to detected messages.

For more information, see [Configuring a Message Stamp on page 5-57](#).

11. Click **Save**.

After adding a rule, you can:

- Click a rule name to edit the rule settings.
  - Select a rule and click **Delete** to remove the selected rule.
  - Select a rule and click **Copy** to create a copy of the selected rule. You can edit the copied rule to create a customized rule.
- 

## Antispam Rules

Deep Discovery Email Inspector uses antispam rules to scan messages identified as spam or graymail.

For more information, see [Spam Scanning on page 1-7](#) and [Graymail Scanning on page 1-8](#).

**Note**

- To maximize spam protection, configure Deep Discovery Email Inspector to use Email Reputation Services (ERS) technology.

For more information, see [Configuring Email Reputation Services on page 8-56](#).

- You can configure graymail exceptions to bypass graymail scanning for messages from trusted IP addresses.

For more information, see [Graymail Exceptions on page 5-89](#)

---

The following table describes the fields on the **Antispam Rules** screen.

| FIELD               | DESCRIPTION   |
|---------------------|---|
| Rule Name           | View the descriptive name for the rule.<br>Click a rule name to edit the rule settings. |
| Action              | View one or more actions to apply when the rule conditions are matched.                 |
| Associated Policies | View the number of policies that include the rule.                                      |
| Last Updated        | View the date and time the entry was last updated.                                      |

## Configuring an Antispam Rule

You can create an antispam rule to specify actions on the following types of potentially unwanted messages:


- Spam
  - Graymail
- 

### Procedure

1. Go to **Policies > Policy Management**.

2. Click the **Antispam Rules** tab.
3. Do one of the following:
  - Click **Add** to create a new rule.
  - Click a rule name to change the settings.
4. Type a rule name.
5. Select the **Spam**, **Graymail**, or both message types and configure the scanning conditions.

| MESSAGE TYPE | DESCRIPTION   |
|--------------|---|
| Spam         | <p>Enables Deep Discovery Email Inspector to scan messages for spam based on the spam catch rate or detection threshold you specify.</p> <ul style="list-style-type: none"><li>• <b>High:</b> This is the most rigorous level of spam detection. Deep Discovery Email Inspector monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those email messages that Deep Discovery Email Inspector filters as spam when they are actually legitimate email messages.</li><li>• <b>Medium:</b> This is the default and recommended setting. Deep Discovery Email Inspector monitors at a high level of spam detection with a moderate chance of filtering false positives.</li><li>• <b>Low:</b> This is most lenient level of spam detection. Deep Discovery Email Inspector only filters the most obvious and common spam messages, but there is a very low chance that it will filter false positives.</li><li>• <b>Specify a detection threshold:</b> Type a threshold value (between 3.0 and 10.0) that represents how critically Deep Discovery Email Inspector analyzes messages to determine if they are spam.</li></ul> |

| MESSAGE TYPE | DESCRIPTION   |
|--------------|---|
| Graymail     | <p>Enables Deep Discovery Email Inspector to scan messages against the Email Reputation Services (ERS) score to identify graymail messages.</p> <p>Select one or more message categories that Deep Discovery Email Inspector considers as graymail.</p> <hr/> <div>  <b>Note</b> </div> <p>You can add the IP addresses or subnets of trusted senders to the <b>Graymail Exceptions</b> list. Email messages from IP addresses or subnets in the list bypass graymail scanning in Deep Discovery Email Inspector.</p> <p>For more information, see <a href="#">Adding a Graymail Exception on page 5-90</a>.</p> |

6. Specify the **Action**.

For more information, see [Policy Actions on page 5-8](#).

7. (Optional) To send a blind carbon copy of detected messages to one or more recipients, type the recipient email addresses in the **BCC** field.



**Note**

You can specify up to 50 email addresses. Wildcard characters are not supported.

8. (Optional) From the **Send notification** drop-down list, select a notification message to inform recipients about the applied policy action.



**Important**

Deep Discovery Email Inspector only sends recipient notifications when you select **Send notification** and a notification message.

You can configure notification messages on the **Notifications** screen (go to **Policies > Policy Objects > Notifications**).

For more information, see [Configuring Recipient Notification on page 5-54](#).

9. (Optional) From the **Insert stamp** drop-down list, select a stamp that you want to insert in to detected messages.

For more information, see [Configuring a Message Stamp on page 5-57](#).

10. Click **Save**.

After adding a rule, you can:

- Click a rule name to edit the rule settings.
- Select a rule and click **Delete** to remove the selected rule.
- Select a rule and click **Copy** to create a copy of the selected rule. You can edit the copied rule to create a customized rule.

---

## Threat Protection Rules

Deep Discovery Email Inspector uses threat protection rules to provide security controls that ensure protection against threats. You can configure threat protection rules to specify traffic handling behavior and customize notification messages.

Deep Discovery Email Inspector scans messages for virus and other malware using the following scan technology:

- [Virtual Analyzer on page 1-13](#)
- [Advanced Threat Scan Engine on page 1-13](#)
- [Predictive Machine Learning on page 1-14](#)

The following table describes the fields on the **Threat Protection Rules** screen.

| FIELD               | DESCRIPTION   |
|---------------------|---|
| Rule Name           | View the descriptive name for the rule.<br>Click a rule name to edit the rule settings. |
| Action              | View one or more actions to apply when the rule conditions are matched.                 |
| Associated Policies | View the number of policies that include the rule.                                      |
| Last Updated        | View the date and time the entry was last updated.                                      |

## Configuring a Threat Protection Rule

You can create threat protection rules to scan messages for viruses and other malware such as spyware and worms.

---

### Procedure

1. Go to **Policies > Policy Management**.
2. Click the **Threat Protection Rules** tab.
3. Do one of the following:
  - Click **Add** to create a new rule.
  - Click a rule name to change the settings.
4. Type a rule name.
5. Configure the settings for High, Medium, Low risk, and Unrated messages.
  - a. For **Unrated** messages, select a detection reason.
  - b. Specify the **Action**.

For more information, see [Policy Actions on page 5-8](#).
  - c. (Optional) From the **Send notification** drop-down list, select a notification message to inform recipients about the applied policy action.

**Important**

Deep Discovery Email Inspector only sends recipient notifications when you select **Send notification** and a notification message.

You can configure notification messages on the **Notifications** screen (go to **Policies > Policy Objects > Notifications**).

For more information, see [Configuring Recipient Notification on page 5-54](#).

- d. (Optional) For low-risk messages, configure the subject tag and X-header settings.
  - **Subject tag:** Specify the string to insert in the subject of email messages.
  - **X-Header:** Specify the text to add to the X-header.
6. (Optional) Under **Advanced Settings**, select one or more of the following settings:
  - Select **Quarantine the original message when attachments cannot be stripped** to store the detected email message in the quarantine when Deep Discovery Email Inspector is unable to strip the attachments. Deep Discovery Email Inspector does not deliver the email message to the recipients.

**Note**

- This setting only takes effect when Deep Discovery Email Inspector is in MTA mode.
  - When you select this option, Deep Discovery Email Inspector also quarantines detected phishing messages.
- 
- Select **Quarantine a copy of the original message when stripping attachments or redirecting links** to store a copy of the detected email message with the attachment and URL in the quarantine for further investigation.

**Note**

This setting only takes effect when Deep Discovery Email Inspector is in MTA mode.

---

- Select **Attempt to clean before stripping attachments** to have Deep Discovery Email Inspector clean an attachment first when you also select a strip attachment action for the rule. If Deep Discovery Email Inspector is unable to clean the attachment, Deep Discovery Email Inspector then deletes the attachment.

Clear the check box to have Deep Discovery Email Inspector immediately delete attachments that are detected as malicious.

---

**Note**

This setting only takes effect when Deep Discovery Email Inspector is in MTA mode.

---

- Select **Prioritize for Virtual Analyzer submission** to submit detected email messages to Virtual Analyzer with high priority.
  - Select **Deliver directly** to send email messages that match a policy rule and are not deleted or quarantined to the specified SMTP server.
- 

**Note**

If you select this setting, you must specify the SMTP server address and port number.

---

- Select **BCC** and type one or more recipient email addresses in the field to send a blind carbon copy of detected messages to the recipients.
- 

**Note**

You can specify up to 50 email addresses. Wildcard characters are not supported.

---

- (Optional) From the **Insert stamp** drop-down list, select a stamp that you want to insert in to detected messages.

For more information, see [Configuring a Message Stamp on page 5-57](#).

7. Click **Save**.

After adding a rule, you can:

- Click a rule name to edit the rule settings.
- Select a rule and click **Delete** to remove the selected rule.

## Policy Objects

Policy objects simplify policy management by storing configurations that can be shared across all policy rules.

The following table describes the policy objects that you can configure in Deep Discovery Email Inspector.

| POLICY OBJECTS   | DESCRIPTION   |
|------------------|---|
| Notifications    | Create messages to notify a recipient or email administrator that Deep Discovery Email Inspector took action on a message or that the message violated Deep Discovery Email Inspector rule scanning conditions.                                   |
| Replacement file | Specify text (to append to all processes messages) and file name (to replace stripped attachments) to notify a recipient that Deep Discovery Email Inspector took action on a message or that the message violated scanning conditions for rules. |
| Stamps           | Configure up to three stamps to insert into messages based on the message direction.  |
| Redirect pages   | Specify a redirect page blocks or warns users from opening suspicious links.  |
| Archive servers  | Configure up to ten archive servers to store email messages based on policy settings.   |

| POLICY OBJECTS   | DESCRIPTION  |
|------------------|--|
| Data identifiers | Configure data identifiers (expressions, file attributes, or keywords) that you can apply in content filtering and DLP policy rules. |
| DLP templates    | Configure DLP templates to include data identifiers and logical operators for use in DLP policy rules.                               |
| Address groups   | Configure address groups to apply policy rules to several email addresses at a time.   |

## Notifications

You can configure a notification and associate it with a policy rule. When a rule is matched, Deep Discovery Email Inspector sends the notification to notify specified recipients that an email message was processed and may contain suspicious or malicious content.

The following table describes the information on the **Notifications** screen.

| HEADER           | DESCRIPTION  |
|------------------|--|
| Name             | View the name of the notification.                         |
| Message          | View a portion of the notification message.                |
| Associated Rules | View the number of rules associated with the notification. |
| Last Updated     | View the date and time the entry was last updated.         |

## Configuring Recipient Notification

You can create a recipient notification for use in policy rules.

---

### Procedure

1. Go to **Policies > Policy Objects > Notifications**.
2. Do one of the following:
  - Click **Add** to create a new notification.

- Click a name to change the settings.
3. In the **Name** field, type a descriptive name for the notification.
  4. Under **Recipients**, specify the recipients Deep Discovery Email Inspector sends the notification when the associated policy rule is matched.
    - **Original email recipient:** Select this option to send the notification to the intended recipient of a detected email message.
    - **Original email sender:** Select this option to send the notification to the original sender of a detected email message.
    - **Send to all contacts and other notification recipients:** Select this option to send the notification to the email addresses define on the **Contacts** screen and the specified recipients.

For more information, see [Managing Contacts on page 8-217](#).

(Optional) To send the notification to other recipients, type the email addresses in the **Other notification recipients** text box. Use a semicolon (;) to separate entries.

5. Configure the email notification sent to the recipient after Deep Discovery Email Inspector investigates and acts upon an email message.

Use the provided tokens to customize your message. For details, see [Recipient Notification Message Tokens on page B-2](#).

6. Click **Save**.

After adding a notification:

- Click **Copy** to duplicate a selected notification. You can edit the notification settings to create a new notification.
- Select a notification and click **Delete** to remove the entry from the list.

---

## Replacement File

Deep Discovery Email Inspector uses a replacement file to replace a stripped suspicious attachment in detected messages to notify a recipient that the

email message was processed and any suspicious or malicious attachment is removed.

## Configuring the Replacement File

---

### Procedure

1. Go to **Policies > Policy Objects > Replacement File**.
2. Under **Replacement File**, configure the following:
  - **File name**: Specify a file name for the replacement file
  - **Text**: Specify the text to include in the replacement file



#### Tip

You can include tokens from the **Available Tokens** list in the text. Before sending the replacement file, Deep Discovery Email Inspector replaces the tokens with the actual data.

---

3. Click **Save**.
- 


## Message Stamps

A message stamp is inserted in to an email message to notify a recipient that Deep Discovery Email Inspector has processed the message.

You can configure up to three message stamps based on message directions (one each for inbound, outbound, or inbound and outbound message directions). There is no limit to the number of stamps you can create for policy rules.

The following table describes the information on the **Stamps** screen.

| FIELD   | DESCRIPTION                              |
|---------|--|
| Name    | View the descriptive name for the stamp. |
| Content | View the text content of the stamp.      |

| FIELD            | DESCRIPTION   |
|------------------|---|
| Insert At        | View the location in the message body to insert the stamp.  |
| Direction        | View the direction of the messages to which the stamp is applied.<br>If the stamp is used in one or more policy rules, this field displays a dash "-".  |
| Associated Rules | View the number of policy rules in which the stamp is applied.<br>If the stamp is applied based on message direction, this field displays a dash "-".   |
| Last Updated     | View the date and time the entry was last updated.  |
| Status           | <div>Toggle to enable or disable the stamp.</div> <div> <b>Note</b><ul style="list-style-type: none"><li>• When a stamp is enabled for a message direction, Deep Discovery Email Inspector automatically inserts the stamp in to message in the specified message direction.</li><li>• You can only disable a stamp that is not used in a policy rule.</li></ul></div> |

## Configuring a Message Stamp

You can configure up to three message stamps based on message directions (one each for inbound, outbound, or inbound and outbound message directions). There is no limit to the number of stamps you can create for policy rules.

### Procedure

1. Go to **Policies > Policy Objects > Stamps**.
2. Do one of the following:
  - Click **Add** to configure a new stamp.

- Click a stamp name to change the settings.
3. Select a status option to enable or disable the stamp.

**Note**

- When a stamp is enabled for a message direction, Deep Discovery Email Inspector automatically inserts the stamp in to message in the specified message direction.
  - You can only disable a stamp that is not used in a policy rule.
- 

4. Type a descriptive name.
5. Select the message location to insert the stamp.
6. Select an option to apply the stamp based on policy rules or message direction.

**Note**

- If you select **Policy rules**, select the stamp in one or more policy rules to have Deep Discovery Email Inspector insert the stamp in to detected messages.
  - If the stamp is not used in a policy rule, you can change this setting on the **Edit Stamp** screen.
- 

7. Type the stamp content in the text field.

You can format the text content using the formatting settings provided. The **Plain text preview** field displays the read-only, plain text version of the content.

8. Click **Save**.
- 

## Redirect Pages

Deep Discovery Email Inspector uses policy actions to determine if a redirect page blocks or warns users from opening suspicious links. You can

customize the redirect pages with your own logo, message body, and administrator contact information.

## Customizing the Redirect Pages

When using built-in redirect pages, ensure that the message recipients can open the redirect pages. If the redirect pages cannot be opened, check your network configuration or use external redirect pages.

---

### Procedure

1. Go to **Policies > Policy Objects > Redirect Pages**.
2. Select whether to use external or built-in redirect pages.
  - **Use external redirect pages:** Type the page URL of the **Blocking page** to use
  - **Use built-in redirect pages:** Select to show the **Warning page** or **Blocking page**.

Do the following to edit the redirect page:

- Select **Use host name in link. Configure the host name to enable this setting..**



#### Tip

Trend Micro recommends enabling this setting to prevent users from accidentally visiting the malicious website.


- Click **host name** to redirect to the **System Settings** screen where you can view or change the **Host name** setting under **Host Name / Gateway / DNS**.



#### Note

Save any changes before navigating away from the **Policy** screen.


---

- Click the **Replace image** () icon to browse and select an image file.

**Important**

Images cannot be bigger than 500x60 pixels and must be in GIF, JPEG, or PNG format.

---

- Click the **Edit** () icon to open the field for editing.
- Click the **Enable** hyperlink to open the **Administrator Contact Information** fields for editing.

3. Click **Save**.

---

## Archive Servers

You can configure archive servers to store email messages that match a policy. When you enable message archiving for a policy, Deep Discovery Email Inspector automatically sends a copy of matched messages to the specified archive server.

**Note**

- You can configure up to ten archive servers.
  - If a message matches multiple policies with different archive server settings, Deep Discovery Email Inspector sends a copy of the message to each archive server.
  - If a message matches multiple policies with the same archive server setting, Deep Discovery Email Inspector only sends a copy of the message to the archive server.
- 

The following table describes the fields on the **Archive Servers** screen.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Server Name         | View the descriptive name of the archive server.         |
| Email Address       | View the email address of the archive server.            |
| Server Address      | View the IP address or FQDN of the archive server.       |
| Port                | View the archive server port number.                     |
| Associated Policies | View the number of policies that use the archive server. |
| Last Updated        | View the date and time the entry was last updated.       |

## Configuring an Archive Server

You can configure up to ten archive servers to store email messages based on policy settings.

---

### Procedure

1. Go to **Policies > Policy Objects**.
2. Click the **Archive Servers** tab.
3. Do one of the following:
  - Click **Add** to configure a new archive server.
  - Click a server name to change the settings.
4. Type a unique server name (up to 64 characters).
5. Type the email address for the archive server.
6. Configure the SMTP server to send messages for archive. Select one of the following options and configure the required settings:
  - **Specify server address and port:** Select this option to specify SMTP server address and port.

After you have configured the SMTP server settings, you can click **Test Connection** to test the connection to the server.

- **Use MX record lookup:** Select this option to search for the SMTP server based on MX records.

7. Click **Save**.

After adding an archive server, you can:

- Click a server name to edit the settings.
- Select a server and click **Delete** to remove the selected entry.



**Note**

You cannot remove an archive server if it is associated with a policy.

---

## Data Identifiers

Digital assets are files and data that an organization must protect against unauthorized transmission. You can define digital assets using the following data identifiers:



**Note**

You cannot delete a data identifier that a content filtering rule or DLP template is using. Delete the rule or template before deleting the data identifier.

---

- **Expressions:** Data that has a certain structure.

For details, see [Expressions on page 5-63](#).

- **File attributes:** File properties such as file type and file size.

For details, see [File Attributes on page 5-68](#).

- **Keyword lists:** A list of special words or phrases.

For details, see [Keyword Lists on page 5-72](#).

## Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

You can use predefined and customized expressions in content filtering and DLP rules.

For more information, see [Predefined Expressions on page 5-63](#) and [Customized Expressions on page 5-64](#).

### Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at:

<http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

#### Viewing Predefined Expressions

**Note**

Predefined expressions cannot be modified or deleted.

---

### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **Expressions** tab.
3. Click the expression name.

#### 4. View the settings on the screen that appears.

---

### Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:  
<http://www.pcre.org/>
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

You can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Deep Discovery Email Inspector subjects it to a content filtering or DLP policy rule. For details about the different criteria options, see [Criteria for Customized Expressions on page 5-65](#).

## Criteria for Customized Expressions

**TABLE 5-6. Criteria Options for Customized Expressions**

| CRITERIA            | RULE   | EXAMPLE  |
|---------------------|--|--|
| None                | None   | <p>All - Names from US Census Bureau</p> <ul style="list-style-type: none"> <li>Expression: <code>[^\\w]{([A-Z][a-z]{1,12} \\s? \\s? [\\s]\\s([A-Z])\\.\\s)[A-Z][a-z]{1,12})[^\\w]</code></li> </ul>   |
| Specific characters | <p>An expression must include the characters you have specified.</p> <p>In addition, the number of characters in the expression must be within the minimum and maximum limits.</p>   | <p>US - ABA Routing Number</p> <ul style="list-style-type: none"> <li>Expression: <code>[^\\w\\\\\\f\\.-=&amp;";]([0123678]\\d{8})[^\\w-\\]+.;&amp;]</code></li> <li>Specific characters: 0123456789</li> <li>Minimum characters in the expression: 9</li> <li>Maximum characters in the expression: 9</li> </ul>  |
| Suffix              | <p>Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters.</p> <p>In addition, the number of characters in the expression must be within the minimum and maximum limits.</p> | <p>All - Home Address</p> <ul style="list-style-type: none"> <li>Expression: <code>D(\\d+\\s[a-z.]+\\s([a-z]+\\s){0,2} (lane ln street st avenue ave road rd place pl drive dr circle cr court ct boulevard blvd)\\.?[0-9a-z,#\\s\\.]{0,30}[\\s,][a-z]{2}\\s\\d{5}(-\\d{4})?)[^\\d-]</code></li> <li>Suffix characters: 0123456789-</li> <li>Number of suffix characters: 5</li> <li>Minimum characters in the expression: 25</li> <li>Maximum characters in the expression: 80</li> </ul> |

| CRITERIA                    | RULE   | EXAMPLE  |
|-----------------------------|--|--|
| Single- character separator | <p>An expression must have two segments separated by a character.</p> <p>In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.</p> | <p>All - Email Address</p> <ul style="list-style-type: none"> <li>• Expression: [^\w.](\w\.){1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.] {0,10}) [^\w.]</li> <li>• Separator: @</li> <li>• Minimum characters to the left: 3</li> <li>• Maximum characters to the left: 15</li> <li>• Maximum characters to the right: 30</li> </ul> |

### Configuring a Customized Expression

#### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **Expressions** tab.
3. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry to change the settings.
4. Type a name. The name must not exceed 256 characters in length and cannot contain a vertical bar (|).
5. Type a description that does not exceed 512 characters.
6. Type the display data format.
7. Type an example for the display data.
 

For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
8. Choose one of the following criteria and configure additional settings for the chosen criteria (see [Criteria for Customized Expressions on page 5-65](#)):

- None
  - Specific characters
  - Suffix
  - Single-character separator
9. Test the expression against an actual data.
- For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
10. Click **Save** if you are satisfied with the result.

**Note**

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

## Importing Expressions

Use this option if you have a properly-formatted XML file containing the expressions. You can generate the file by exporting the expressions from either the Deep Discovery Email Inspector appliance you are currently accessing or from another Deep Discovery Email Inspector appliance.

### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **Expressions** tab.
3. Click **Import** and then locate the XML file containing the expressions.
4. Click **Open**.

A message appears, informing you that importing expressions overwrites existing customized expressions in Deep Discovery Email Inspector.

5. Click **OK** to start the import process.
- 

## Exporting Expressions

You can use the export feature to back up all or selected expressions in an XML file.

---

### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
  2. Click the **Expressions** tab.
  3. Do one of the following:
    - Select one or more entries and click **Export** to download the XML file containing the selected entries.
    - Click **Export All** to download the XML file containing all entries.
- 

## File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the Deep Discovery Email Inspector administrator can create a policy that blocks the transmission of executable files that are 10 to 40 MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types, see the *Data Protection Lists* document at <http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

### Predefined File Attributes List

Data Loss Prevention comes with a predefined file attributes list. This list cannot be modified or deleted. The list has its own built-in conditions that determine if the template should trigger a policy violation.

### Configuring File Attributes

---

#### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **File Attributes** tab.
3. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry to change the settings.
4. Type a name. The name must not exceed 256 characters in length and cannot contain a vertical bar (|).
5. Type a description that does not exceed 512 characters.
6. Select an option for attachment file type matching:
  - **Selected attachment types:** Deep Discovery Email Inspector takes action on messages with attachments of the selected file types.
  - **Not the selected attachment types:** Deep Discovery Email Inspector takes action on messages with attachments that are not of the selected file types.

**Note**

If an attachment is an archive file containing file types that match any of the selected options, Deep Discovery Email Inspector also takes action on the messages.

---

7. Select your preferred true file types.
  8. If a file type you want to include is not listed, select **Custom file extensions** and then type the file type's extension. Deep Discovery Email Inspector checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:
    - Each extension must start with an asterisk (\*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, \*.pol matches 12345.pol and test.pol.
    - You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (\*) to represent two or more characters. See the following examples:
      - \*.m matches the following files: ABC.dem, ABC.prm, ABC.sdc
      - \*.m\*r matches the following files: ABC.mgdr, ABC.mtp2r, ABC.mdmr
      - \*.fm? matches the following files: ABC.fme, ABC.fm!, ABC.fmp
    - Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: \*.do\* matches abc.doctor\_john.jpg and abc.donor12.pdf.
  9. Type the minimum and maximum file sizes and select the unit size. Both file sizes must be whole numbers larger than zero.
- 

**Note**

To disable file size matching, type "0" in the fields.

---

---

**10. Click **Save**.**

---

**Importing File Attributes**

Use this option if you have a properly-formatted XML file containing the file attributes. You can generate the file by exporting the file attributes from either the Deep Discovery Email Inspector appliance you are currently accessing or from another Deep Discovery Email Inspector appliance.

---

**Procedure**

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **File Attributes** tab.
3. Click **Import** and then locate the XML file containing the file attributes.
4. Click **Open**.

A message appears, informing you that importing file attributes overwrites existing customized file attributes in Deep Discovery Email Inspector.

5. Click **OK** to start the import process.
- 

**Exporting File Attributes**

You can use the export feature to back up all or selected file attributes in an XML file.

---

**Procedure**

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **File Attributes** tab.
3. Do one of the following:
  - Select one or more entries and click **Export** to download the XML file containing the selected entries.

- Click **Export All** to download the XML file containing all entries.
- 

## Keyword Lists

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a content filtering or DLP rule and then configure Deep Discovery Email Inspector to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see [Predefined Keyword Lists on page 5-72](#) and [Customized Keyword Lists on page 5-72](#).

### Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at <http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

### Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- Any keyword
- All keywords
- All keywords within <x> characters
- Combined score for keywords exceeds threshold

For details regarding the criteria rules, see [Criteria for Customized Keyword Lists on page 5-73](#).

Criteria for Customized Keyword Lists

TABLE 5-7. Criteria for a Keyword List

| CRITERIA                           | RULE   |
|------------------------------------|--|
| Any keyword                        | A file must contain at least one keyword in the keyword list.  |
| All keywords                       | A file must contain all the keywords in the keyword list.  |
| All keywords within <x> characters | <p>A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within &lt;x&gt; characters of each other.</p> <p>For example, your 3 keywords are WEB, DISK, and USB, and the number of characters you specified is 20.</p> <p>If Deep Discovery Email Inspector detects all keywords in the order DISK, WEB, and USB, the number of characters from the “D” (in DISK) to the “W” (in WEB), from the “W” to the “U” (in USB), and from the “D” to the “U” must be 20 characters or less.</p> <p>The following data matches the criteria:</p> <p>DISK####WEB#####USB</p> <p>The following data do not match the criteria:</p> <p>DISK####WEB#####USB (23 characters between “D” and “U”)</p> <p>DISK*****WEB****USB (23 characters between “D” and “W”)</p> <p>When deciding on the number of characters, remember that a small number, such as 10, will usually result in a shorter scanning time but will only cover a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but the scanning time might be longer.</p> |

| CRITERIA                                      | RULE  |
|---|---|
| Combined score for keywords exceeds threshold | <p>A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold.</p> <p>Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores.</p> <p>Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.</p> |

### Configuring a Keyword List

---

#### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
2. Click the **Keyword Lists** tab.
3. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry to change the settings.
4. Type a name. The name must not exceed 256 characters in length and cannot contain a vertical bar (|).
5. Type a description that does not exceed 512 characters.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
  - **Any keyword**
  - **All keywords**
  - **All keywords within <x> characters**

- **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:
    - a. Type a keyword that contains 3 bytes to 40 characters and specify whether it is case-sensitive.  
  
For example, you can specify two double-byte characters as a keyword.
    - b. Click **Add**.
  8. To delete keywords, select the keywords and click **Delete**.
  9. Click **Save**.
- 

### Importing Keyword Lists

Use this option if you have a properly-formatted XML file containing the keyword lists. You can generate the file by exporting the keyword lists from either the Deep Discovery Email Inspector appliance you are currently accessing or from another Deep Discovery Email Inspector appliance.

---

#### Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
  2. Click the **Keyword Lists** tab.
  3. Click **Import** and then locate the XML file containing the keyword lists.
  4. Click **Open**.  
  
A message appears, informing you that importing keyword lists overwrites existing customized keyword lists in Deep Discovery Email Inspector.
  5. Click **OK** to start the import process.
- 

### Exporting Keyword Lists

You can use the export feature to back up all or selected keyword lists in an XML file.

---

## Procedure

1. Go to **Policies > Policy Objects > Data Identifiers**.
  2. Click the **Keyword Lists** tab.
  3. Do one of the following:
    - Select one or more entries and click **Export** to download the XML file containing the selected entries.
    - Click **Export All** to download the XML file containing all entries.
- 

## Data Loss Prevention (DLP) Templates

A Data Loss Prevention (DLP) template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to send the file to recipients within a domain. Sending the same file to recipients outside the domain is blocked.

You can create your own templates if you have configured data identifiers.

You can also use predefined templates. For details, see [Customized DLP Templates on page 5-77](#) and [Predefined DLP Templates on page 5-77](#).



### Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

---

## Predefined DLP Templates

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA:** Gramm-Leach-Bliley Act
- **HIPAA:** Health Insurance Portability and Accountability Act
- **PCI-DSS:** Payment Card Industry Data Security Standard
- **SB-1386:** US Senate Bill 1386
- **US PII:** United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at <http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

## Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see [Condition Statements and Logical Operators on page 5-77](#).

## Condition Statements and Logical Operators

Data Loss Prevention evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

**TABLE 5-8. Sample Condition Statements**

| CONDITION STATEMENT  | INTERPRETATION AND EXAMPLE  |
|--|---|
| [Data Identifier 1] <b>And</b> [Data Identifier 2] <b>Except</b> [Data Identifier 3] | <p>A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3].</p> <p>For example:</p> <p>A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].</p> |
| [Data Identifier 1] <b>Or</b> [Data Identifier 2]                                    | <p>A file must satisfy [Data Identifier 1] or [Data Identifier 2].</p> <p>For example:</p> <p>A file must be [an Adobe PDF document] or [a Microsoft Word document].</p>  |
| <b>Except</b> [Data Identifier 1]  | <p>A file must not satisfy [Data Identifier 1].</p> <p>For example:</p> <p>A file must not be [a multimedia file].</p>  |

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

## Creating a DLP Template

### Procedure

1. Go to **Policies > Policy Objects > DLP Templates**.
2. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry to change the settings.
3. Type a name. The name must not exceed 256 characters in length and cannot contain a vertical bar (|).

4. Type a description that does not exceed 512 characters.
5. Under **Condition Statement**, do the following to create a condition statement:
  - a. Select a logical operator.

**Note**

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see [Condition Statements and Logical Operators on page 5-77](#).



---

- b. Select a data identifier type.
  - c. Select a data identifier.

**Tip**

To search for a data identifier, type the full or partial name of the data identifier.

---

- d. For expressions, specify the number of occurrences.
    - e. To add additional conditions, click the add icon ().
    - To remove a condition from the statement, click the delete icon ().
    - f. Click **Add** to add the condition statement to the **Template Definition** table.
6. Under **Template Definition**, select a logical operator for each definition.

**Note**

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see [Condition Statements and Logical Operators on page 5-77](#).

---

7. To delete a definition from the template, click the trash bin icon.
  8. Click **Save**.
- 

### Importing DLP Templates

Use this option if you have a properly-formatted XML file containing the DLP templates. You can generate the file by exporting DLP templates from either the Deep Discovery Email Inspector appliance you are currently accessing or from another Deep Discovery Email Inspector appliance.

---

**Note**

Importing DLP templates overwrites existing customized DLP templates in Deep Discovery Email Inspector.

---

### Procedure

1. Go to **Policies > Policy Objects > DLP Templates**.
  2. Click **Import** and then locate the XML file containing the DLP templates and the associated data identifiers.
  3. Click **Open**.  
A confirmation screen appears.
  4. Click **Import** to start the import process.
- 

### Exporting DLP Templates

You can use the export feature to back up all or selected data loss prevention (DLP) templates in an XML file.

---

## Procedure

1. Go to **Policies > Policy Objects > DLP Templates**.
  2. Do one of the following:
    - Select one or more entries and click **Export** to download the XML file containing the selected DLP templates and the associated data identifiers.
    - Click **Export All** to download the XML file containing all DLP templates and data identifiers (even if a data identifier is not used in a DLP template).
- 

## Address Groups


An address group is a collection of user email addresses in your organization. Instead of creating policies to apply policy rules to each address individually, you can create an address group to apply policy rules to several email addresses at the same time.

Before you configure a policy, create an address group by adding email addresses individually or importing them from a text file.

To use the same address group on multiple Deep Discovery Email Inspector appliances, you can export an address group from the source Deep Discovery Email Inspector appliance and import the text file on a target Deep Discovery Email Inspector appliance.

The following table describes the tasks you can perform on the **Address Groups** screen.

| TASK                 | DESCRIPTION  |
|----------------------|--|
| Add an address group | Click <b>Add</b> to configure an address group.<br><br>For more information, see <a href="#">Configuring an Address Group on page 5-82</a> . |

| TASK                    | DESCRIPTION   |
|-------------------------|---|
| Edit an address group   | Click an address group name to change the settings.<br><br>For more information, see <a href="#">Configuring an Address Group on page 5-82</a> .  |
| Export an address group | Select an address group and click <b>Export</b> to download the selected address group in a text file.<br><br> <b>Note</b><br>You can only export one address group at a time. |
| Delete address groups   | Select one or more address groups and click <b>Delete</b> .   |

The following table describes the information on the **Address Groups** screen.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Name                | View the name of the address group.                      |
| Description         | View the description of the address group.               |
| Address count       | View the number of email addresses in the address group. |
| Associated policies | View the number of policies that use the address group.  |
| Last updated        | View the date and time the address group is updated.     |

## Configuring an Address Group

### Procedure

1. Go to **Policies > Policy Objects**.
2. Click the **Address Groups** tab.
3. Do one of the following:

- Click **Add** to configure a new address group.
  - Click a name to change the settings.
4. Type a name.
  5. Type a description for the address group.
  6. Do one of the following:
    - Add an individual email address:  
Type an email address and click **Add**.

**Note**

You can use the \* wildcard character in email addresses. For example, \*@domain.com.

---

- Import a list of email addresses:

**Note**

Deep Discovery Email Inspector can import email addresses from a text file. Ensure that the text file contains only one email address per line. Optionally, use the \* wildcard character to specify an email address. For example, \*@domain.com.

---

- a. Click **Import**.
  - b. Select a text file containing the list of email addresses.
  - c. Click **OK**.
- The new entries display in the address list.
7. Click **Add** or **Save**.
- 

## Policy Exceptions

Policy exceptions reduce false positives. Configure exceptions to set the limits and actions for email encryption, or classify certain email messages as

safe. Specify the safe senders, recipients, and X-header content, add files, URLs, IP addresses and domains, add URL keywords, or specify senders to bypass graymail scanning. Safe email messages are discarded (BCC and SPAN/TAP mode) or delivered to the recipient (MTA mode) without further investigation.

## Configuring Message Exceptions

Deep Discovery Email Inspector considers messages with any of the specified senders, recipients, or X-headers in the exception list safe and bypasses policy rules on these messages. However, Deep Discovery Email Inspector still applies sender filtering and sender authentication settings on these messages.

---

### Procedure

1. Go to **Policies > Exceptions > Messages**.
2. Specify email message exception criteria.
  - **Senders**
  - **Recipients**
  - **X-header**



#### Note

Deep Discovery Email Inspector ignores case-sensitivity for X-header exceptions.

Deep Discovery Email Inspector supports the use of the wildcard asterisk (\*) character to specify an entire domain. For example, to create a **Senders** exception for the domain abc.com, type the following:

```
*@abc.com
```

---

3. Click **Save**.
-

## Managing Object Exceptions

Perform any of the following tasks to manage object exceptions.

---

### Procedure

- Specify search filters to control the display and to view existing exceptions.

The following table describes the **Source** filter options.

| OPTION                  | DESCRIPTION   |
|-------------------------|---|
| All                     | Displays all object exceptions.   |
| Local                   | Displays object exceptions that are added manually on Deep Discovery Email Inspector. |
| Apex Central            | Displays object exceptions that are synchronized from Apex Central.                   |
| Web service             | Displays object exceptions that are imported through the HTTP web service.            |
| Deep Discovery Director | Displays object exceptions that are synchronized from Deep Discovery Director.        |









#### Note

- If Deep Discovery Email Inspector is registered to Apex Central, Deep Discovery Email Inspector synchronizes object exceptions from Apex Central every 10 minutes.
- If Deep Discovery Email Inspector is registered to both Apex Central and Deep Discovery Director 3.0 (or later), Deep Discovery Email Inspector synchronizes object exceptions from Deep Discovery Director and overwrites existing object exceptions from Apex Central.

- 
- Modify the objects considered safe.

The following table describes the actions on object exceptions.

| ACTION   | DESCRIPTION   |
|--|---|
|  Add          | <p>Add a new object to the exceptions list. Optionally include a note to help you better understand the object exception.</p> <p>For more information, see <a href="#">Adding an Object Exception on page 5-87</a>.</p>   |
|  Import       | <p>Select the CSV file to import.</p> <p>The format for each line is:</p> <pre>&lt;type&gt;,&lt;object&gt;,[source],[notes]</pre> <ul style="list-style-type: none"> <li>• &lt;type&gt; values: IP address, Domain, URL, Files</li> <li>• &lt;object&gt; values: IP address, domain, URL, or SHA-1 hash value</li> <li>• (Optional) [source] value: "local"</li> <li>• (Optional) [notes]: Any additional information in any format</li> </ul> <p>Valid CSV examples:</p> <ul style="list-style-type: none"> <li>• Links,www.example.com,local,customer can view this site</li> <li>• IP address,10.10.10.10,,HR address</li> <li>• Files,3395856CE81F2B7382DEE72602F798B642F14140,local,SHA-1 of CA certificate</li> <li>• Domain,example.com,,Added</li> </ul> <p>For more information, see <a href="#">Importing Object Exceptions on page 5-88</a>.</p> |
|  Delete     | Delete the selected objects.  |
|  Delete All | Delete all objects.   |
|  Export     | Export the selected objects.  |
|  Export All | Export the entire exceptions list to a CSV file.  |

## Adding an Object Exception

Deep Discovery Email Inspector passes email messages containing only safe files, URLs, IP addresses, and domains without further investigation. If an email message contains one safe URL and another unknown URL, Deep Discovery Email Inspector investigates the unknown URL. Virtual Analyzer also ignores safe files and URLs during sandbox analysis.

---

### Procedure

1. Go to **Policies > Exceptions > Objects**.
2. Click **Add**.
3. Specify file, URL, IP address, or domain exception criteria.
  - For files, select **File** for the type and then specify the SHA-1 hash value.

**Note**

Threat Connect correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network to provide relevant and actionable intelligence.
  - For URLs, select **URL** for the type and then specify the web address.

**Note**

Specify a complete URL or use a wildcard (\*) for subdomains.
  - For IP addresses, select **IP address** for the type and then specify the web address.
  - For domains, select **Domain** for the type and then specify the web address.
4. (Optional) Specify a note.
5. (Optional) Click **Add More** to specify multiple file, URL, IP address, or domain exception criteria at the same time.

- a. Specify file, URL, IP address, or domain exception criteria.
  - b. Click **Add to List**. The criterion is added to the object list.
6. Click **Save**.

After adding an object exception:

- Click **Delete** to delete the selected entry.
  - Click **Delete All** to delete all entries in the list.
  - Click **Export** to download the selected entry as a CSV file.
  - Click **Export All** to download list as a CSV file.
- 

## Importing Object Exceptions

You can import exceptions from a properly-formatted CSV file.

---

### Procedure

1. Go to **Policies > Exceptions > Objects**.
2. Click **Import**.
3. Do one of the following:
  - If you are importing exceptions for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), browse and then select the CSV file.
  - If you have imported exceptions previously, save another copy of the CSV file, populate it with new objects, browse and then select the CSV file.

4. Click **Import**.

The imported exceptions display in the list with **Web service** as the source.

---

## Configuring URL Keyword Exceptions

URLs that contain any of the specified keywords are considered one-click URLs and will not be accessed by Deep Discovery Email Inspector.

**Note**

- Detected one-click URLs are scanned by Web Reputation Services. Deep Discovery Email Inspector does not submit these URLs to Virtual Analyzer for analysis.
- You can add URLs to the exception list on the **Objects** tab.

For more information, see [Adding an Object Exception on page 5-87](#)

---

### Procedure

1. Go to **Policies > Exceptions > URL Keywords**.
2. Specify URL keywords.

**Note**

- URL keywords are not case sensitive.
  - Specify one keyword per line.
- 

3. Click **Save**.
- 

## Graymail Exceptions

Graymail refers to solicited bulk email messages that are not spam. Deep Discovery Email Inspector can detect marketing messages and newsletters and social network notifications as graymail based on policy rules.

Email messages from IP addresses or subnets in the Graymail Exceptions list bypass graymail scanning in Deep Discovery Email Inspector.

## Adding a Graymail Exception

Deep Discovery Email Inspector bypasses graymail scanning on email messages from IP addresses and subnets that you add to the Graymail Exceptions list.

---

### Procedure

1. Go to **Policies > Exceptions > Graymail Exceptions**.


2. Click **Add**.

The **Add Graymail Exception** screen appears.

3. Type an IPv4/IPv6 address or subnet.

4. Type a description for the exception.

5. (Optional) To add more entries, click **Add More** and do the following:

To delete an entry from the list, click the icon (  ) in the **Action** column.

6. Click **Save**.

After adding a graymail exception:

- Click **Delete All** to delete all entries in the list.
- Click **Export All** to download list as a CSV file.
- To remove one or more entries, select the entries and click **Delete**.
- To export one or more entries as a CSV file, select the entries and click **Export**.

---

## Importing Graymail Exceptions

You can import graymail exceptions from a properly-formatted CSV file.

---

### Procedure

1. Go to **Policies > Exceptions > Graymail Exceptions**.

2. Click **Import**.

A file selection screen appears.

3. Select a CSV file.

4. Click **Open** to import the CSV file.

After importing graymail exceptions:

- Click **Delete All** to delete all entries in the list.
- Click **Export All** to download list as a CSV file.

---


## Configuring Email Encryption Exceptions



Deep Discovery Email Inspector does not encrypt or decrypt messages that meet the thresholds or conditions you specify on the **Email Encryption Exceptions** screen.

---

### Procedure

1. Go to **Policies > Exceptions > Email Encryption Exceptions**.
2. Under **Scanning Criteria**, configure the limits for encrypted and decrypted messages that Deep Discovery Email Inspector processes.

| FIELD                          | DESCRIPTION  |
|--------------------------------|--|
| Maximum encrypted message size | <p>Specify the maximum size for encrypted messages</p> <hr/> <div> <b>Note</b><br/>This setting applies to both inbound and outbound messages. When a message meets the maximum threshold, Deep Discovery Email Inspector applies the specified actions on the message.</div> <hr/> |

| FIELD   | DESCRIPTION  |
|---|--|
| Maximum decrypted message size                | <p>Specify the maximum size for decrypted messages</p> <hr/> <div>  <b>Note</b> </div> <p>This setting applies to both inbound and outbound messages. When a message meets the maximum threshold, Deep Discovery Email Inspector applies the specified actions on the message.</p> <hr/>      |
| Maximum recipients                            | <p>Specify the maximum number of recipients in messages</p> <hr/> <div>  <b>Note</b> </div> <p>This setting applies to both inbound and outbound messages. When a message meets the maximum threshold, Deep Discovery Email Inspector applies the specified actions on the message.</p> <hr/> |
| Unsuccessful encryption for outbound messages | Select this option to apply the action specified under <b>Actions</b> on outbound messages that Deep Discovery Email Inspector cannot encrypt.   |
| Unsuccessful decryption for outbound messages | Select this option to apply the action specified under <b>Actions</b> on outbound messages that Deep Discovery Email Inspector cannot decrypt.   |

- Under **Actions**, configure the actions to apply on messages that reach the specified thresholds and outbound messages that Deep Discovery Email Inspector cannot encrypt or decrypt.

| FIELD       | DESCRIPTION  |
|-------------|--|
| Action      | Select one of the following actions to apply to messages: <ul style="list-style-type: none"><li>• <b>Delete message:</b> Deletes the email message from the mail queue</li><li>• <b>Block and quarantine:</b> Stores a copy in the quarantine area</li><li>• <b>Pass and tag:</b> If configured, tags the email message subject and inserts the X-header before delivery</li></ul> |
| Subject tag | If you select the <b>Pass and tag</b> action, specify the string to insert in the subject of messages.   |
| X-Header    | If you select the <b>Pass and tag</b> action, specify the text to add to the X-header.   |

---

**4. Click Save.**

---



# Chapter 6

## Alerts and Reports

Topics include:

- *Alerts on page 6-2*
- *Reports on page 6-27*

## Alerts

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

- Critical alerts are triggered by events that require immediate attention
- Important alerts are triggered by events that require observation
- Informational alerts are triggered by events that require limited observation (most likely benign)

The threshold to trigger each alert is configurable.




### Note

For information about available message tokens in alert notifications, see [Alert Notification Message Tokens on page B-3](#).

## Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention. Deep Discovery Email Inspector considers malfunctioning sandboxes, stopped services, unreachable relay MTAs, and license expiration as critical problems.

**TABLE 6-1. Critical Alerts**

| NAME                     | CRITERIA<br>(DEFAULT)   | CHECKING INTERVAL<br>(DEFAULT) |
|--------------------------|---|--------------------------------|
| Virtual Analyzer Stopped | Virtual analyzer is unable to recover<br><hr/>  <b>Note</b><br>This alert is only available when using a local Virtual Analyzer. | Immediate                      |
| Service Stopped          | A service has stopped and cannot be restarted   | Immediate                      |

| NAME                   | CRITERIA<br>(DEFAULT)                       | CHECKING INTERVAL<br>(DEFAULT) |
|------------------------|---|--------------------------------|
| Relay MTAs Unreachable | All relay MTAs for a domain are unreachable | Once every 5 minutes           |
| License Expiration     | License is about to expire or has expired   | Immediate                      |

## Important Alerts

The following table explains the important alerts triggered by events that require observation. Deep Discovery Email Inspector considers traffic surges, suspicious message detections, hardware capacity changes, certain sandbox queue activity, and component update issues as important events.

**TABLE 6-2. Important Alerts**

| NAME                                       | CRITERIA<br>(DEFAULT)   | CHECKING INTERVAL<br>(DEFAULT) |
|--|---|--------------------------------|
| Suspicious Messages Identified             | 1 or more messages detected with threats  | Once every 5 minutes           |
| Watchlisted Recipients at Risk             | 1 or more messages detected with threats sent to watchlist recipients                       | Once every 5 minutes           |
| Quarantined Messages with Detected Threats | At least 10 messages quarantined  | Once every 30 minutes          |
| Long Message Delivery Queue                | At least 500 messages in delivery queue   | Once every 5 minutes           |
| High CPU Usage                             | CPU usage is at least 90%   | Once every 5 minutes           |
| Long Virtual Analyzer Submission Queue     | At least 20 messages in queue for Virtual Analyzer submission with a wait time of 5 minutes | Immediate                      |

| <b>NAME</b>                                       | <b>CRITERIA<br/>(DEFAULT)</b>  | <b>CHECKING INTERVAL<br/>(DEFAULT)</b> |
|---|--|--|
| Long Virtual Analyzer Processing Time             | Average Virtual Analyzer processing time is greater than 15 minutes                    | Once every hour                        |
| Low Free Disk Space                               | Disk space is 5GB or less  | Once every 30 minutes                  |
| Component Update/Rollback Unsuccessful            | An update/rollback was not successful  | Immediate                              |
| Email Messages Timed Out Without Analysis Results | At least 1 email message timed out without analysis results                            | Once every 5 minutes                   |
| Email Message Encryption/Decryption Unsuccessful  | At least 1 message with unsuccessful encryption or decryption                          | Once every 5 minutes                   |
| Low Free Threat Quarantine Disk Space             | Free quarantine disk space left to store messages with detected threats is 10% or less | Once every 30 minutes                  |
| High Memory Usage                                 | Memory usage is at least 90%   | Once every 5 minutes                   |
| Long Message Deferred Queue                       | At least 100 messages in deferred queue  | Once every 5 minutes                   |
| Low Free Spam Quarantine Disk Space               | Free quarantine disk space left to store spam messages is 10% or less                  | Once every 30 minutes                  |
| Account Locked                                    | One or more accounts have been locked  | Immediate                              |
| Unsuccessful DKIM Signing                         | At least 5 messages with unsuccessful DKIM signing                                     | Once every 5 minutes                   |
| Connection Issue                                  | Unable to establish connection to a required resource                                  | Once every 30 minutes                  |

## Informational Alerts

The following table explains the alerts triggered by events that require limited observation. Surges in detection and processing, and completed updates are most likely benign events.

**TABLE 6-3. Informational Alerts**

| NAME                                 | CRITERIA<br>(DEFAULT)                         | CHECKING INTERVAL<br>(DEFAULT) |
|--------------------------------------|---|--------------------------------|
| Threat Detection Surge               | At least 10 messages detected                 | Once every hour                |
| Processing Surge                     | At least 20,000 messages processed            | Once every hour                |
| Component Update/Rollback Successful | An update/rollback was successfully completed | Immediate                      |
| Data Loss Prevention Incident        | At least 10 messages with DLP rule violations | Once every hour                |

## Configuring Alert Notifications

Add at least one notification recipient for all critical and important alerts.



### Note

Configure the SMTP server to send notifications. For details, see [Configuring the Notification SMTP Server on page 8-194](#).

### 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.  
For details, see [Alert Notification Parameters on page 6-7](#).

4. Click **Save**.
  5. Click **Back** to return to the **Alert Rules** screen.
- 

## Viewing Triggered Alerts

---

### Procedure

1. Go to **Alerts / Reports > Alerts > Triggered Alerts**.
2. Specify the search criteria.
  - **Level**
  - **Type**
  - **Rule Name**
  - **Period**
3. View alert details.

| HEADER                  | DESCRIPTION   |
|-------------------------|---|
| Triggered               | The date and time when the alert occurred   |
| Level                   | The importance of the alert: critical, important, or informational                                    |
| Rule                    | The name of the alert rule  |
| Criteria                | The alert rule criteria that triggered the alert  |
| Count                   | The number or duration of triggered alert occurrences. Click a number to display related log entries. |
| Notification Recipients | The most recent alert notification recipients   |
| Notification Subject    | The most recent alert notification subject  |



---

## Managing Alerts

Perform any of the following tasks to manage alerts.

## Procedure

- Specify search filters to control the display and view existing exceptions.
- Export or purge triggered alerts after review.

| OPTION  | DESCRIPTION                              |
|---|--|
| <br>Delete     | Delete the selected alerts.              |
| <br>Export All | Export up to 50000 alerts to a CSV file. |

## Alert Notification Parameters

All triggered alert rules can notify recipients with a custom email message. Some alerts have additional parameters, including message count, checking interval, or risk level.

## Critical Alert Parameters



### Note

For explanations about available message tokens in each alert, see [Alert Notification Message Tokens on page B-3](#).

**TABLE 6-4. Virtual Analyzer Stopped**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.                           |
| Alert level | Displays the alert level in email messages.                                |
| Recipients  | Specify the recipients who will receive the triggered alert email message. |
| Subject     | Specify the subject of the triggered alert email message.                  |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> </ul> |

**TABLE 6-5. Service Stopped**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.   |
| Alert level | Displays the alert level in email messages.  |
| Recipients  | Specify the recipients who will receive the triggered alert email message.   |
| Subject     | Specify the subject of the triggered alert email message.  |
| Message     | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %ServiceName%</li> </ul> |

**TABLE 6-6. Relay MTAs Unreachable**

| PARAMETER   | DESCRIPTION                                      |
|-------------|--|
| Status      | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages.      |

| PARAMETER  | DESCRIPTION  |
|------------|--|
| Recipients | Specify the recipients who will receive the triggered alert email message.   |
| Subject    | Specify the subject of the triggered alert email message.  |
| Message    | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"><li>• %ConsoleURL%</li><li>• %DateTime%</li><li>• %DeviceName%</li><li>• %DeviceIP%</li><li>• %MessageList%</li><li>• %MTAList%</li></ul> |

**TABLE 6-7. License Expiration**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.                           |
| Alert level | Displays the alert level in email messages.                                |
| Recipients  | Specify the recipients who will receive the triggered alert email message. |
| Subject     | Specify the subject of the triggered alert email message.                  |

| PARAMETER | DESCRIPTION  |
|-----------|--|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"><li>• %ConsoleURL%</li><li>• %DateTime%</li><li>• %DaysBeforeExpirationATD%</li><li>• %DaysBeforeExpirationSEG%</li><li>• %DeviceName%</li><li>• %DeviceIP%</li><li>• %ExpirationDateATD%</li><li>• %ExpirationDateSEG%</li><li>• %LicenseStatusATD%</li><li>• %LicenseStatusSEG%</li><li>• %LicenseTypeATD%</li><li>• %LicenseTypeSEG%</li></ul> |

## Important Alert Parameters



### Note

For explanations about available message tokens in each alert, see [Alert Notification Message Tokens on page B-3](#).

**TABLE 6-8. Suspicious Messages Identified**

| PARAMETER      | DESCRIPTION  |
|----------------|--|
| Status         | Select an option to enable or disable the alert.                 |
| Alert level    | Displays the alert level in email messages.                      |
| Email messages | Specify the email message threshold that will trigger the alert. |

| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Risk level      | Select the risk level that will trigger the alert.   |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients      | Specify the recipients who will receive the triggered alert email message.   |
| Subject         | Specify the subject of the triggered alert email message.  |
| Message         | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %MessageList%</li> </ul> |

**TABLE 6-9. Watchlisted Recipients at Risk**

| PARAMETER           | DESCRIPTION  |
|---------------------|--|
| Status              | Select an option to enable or disable the alert.   |
| Alert level         | Displays the alert level in email messages.  |
| Recipient watchlist | Add recipients to the watchlist. The alert triggers when any watchlist recipient receives a suspicious or malicious email message. |
| Email messages      | Specify the email message threshold that will trigger the alert.   |
| Risk level          | Select the risk level that will trigger the alert.   |
| Alert frequency     | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.                                     |
| Recipients          | Specify the recipients who will receive the triggered alert email message.   |
| Subject             | Specify the subject of the triggered alert email message.  |

| PARAMETER | DESCRIPTION  |
|-----------|--|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %MessageList%</li> </ul> |

**TABLE 6-10. Quarantined Messages with Detected Threats**

| PARAMETER            | DESCRIPTION  |
|----------------------|--|
| Status               | Select an option to enable or disable the alert.   |
| Alert level          | Displays the alert level in email messages.  |
| Quarantined messages | Specify the quarantine message threshold that will trigger the alert.  |
| Risk level           | Select the risk level that will trigger the alert.   |
| Alert frequency      | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients           | Specify the recipients who will receive the triggered alert email message.   |
| Subject              | Specify the subject of the triggered alert email message.  |
| Message              | <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %MessageList%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-11. Long Message Delivery Queue**

| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Status          | Select an option to enable or disable the alert.   |
| Alert level     | Displays the alert level in email messages.  |
| Email messages  | Specify the email message threshold that will trigger the alert.   |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients      | Specify the recipients who will receive the triggered alert email message.   |
| Subject         | Specify the subject of the triggered alert email message.  |
| Message         | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeliveryQueue%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %QueueThreshold%</li> </ul> |

**TABLE 6-12. High CPU Usage**

| PARAMETER         | DESCRIPTION  |
|-------------------|--|
| Status            | Select an option to enable or disable the alert.   |
| Alert level       | Displays the alert level in email messages.  |
| Average CPU usage | Specify the threshold for the average CPU usage that will trigger the alert.                   |
| Alert frequency   | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |

| PARAMETER  | DESCRIPTION   |
|------------|---|
| Recipients | Specify the recipients who will receive the triggered alert email message.  |
| Subject    | Specify the subject of the triggered alert email message.   |
| Message    | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %CPUPhreshold%</li> <li>• %CPUUsage%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> </ul> |

**TABLE 6-13. Long Virtual Analyzer Submission Queue**

| PARAMETER         | DESCRIPTION  |
|-------------------|--|
| Status            | Select an option to enable or disable the alert.   |
| Alert level       | Displays the alert level in email messages.  |
| Submissions       | Select email message threshold that will trigger the alert.  |
| Alert frequency   | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.                                       |
| Average wait time | Select the average wait time threshold for samples waiting in the submission queue during the past hour that will trigger the alert. |
| Recipients        | Specify the recipients who will receive the triggered alert email message.   |
| Subject           | Specify the subject of the triggered alert email message.  |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"><li>• %ConsoleURL%</li><li>• %DeviceIP%</li><li>• %DeviceName%</li><li>• %DateTime%</li><li>• %SandboxQueue%</li><li>• %SandboxQueueThreshold%</li></ul> |

**TABLE 6-14. Long Virtual Analyzer Processing Time**

| PARAMETER               | DESCRIPTION  |
|-------------------------|--|
| Status                  | Select an option to enable or disable the alert.   |
| Alert level             | Displays the alert level in email messages.  |
| Average processing time | Select the average time threshold required to process samples in the sandbox queue during the past hour that will trigger the alert. |
| Alert frequency         | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.                                       |
| Recipients              | Specify the recipients who will receive the triggered alert email message.   |
| Subject                 | Specify the subject of the triggered alert email message.  |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %AveSandboxProc%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %SandboxProcThreshold%</li> </ul> |

**TABLE 6-15. Low Free Disk Space**

| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Status          | Select an option to enable or disable the alert.   |
| Alert level     | Displays the alert level in email messages.  |
| Free Disk space | The lowest disk space threshold in GB that triggers the alert.   |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients      | Specify the recipients who will receive the triggered alert email message.   |
| Subject         | Specify the subject of the triggered alert email message.  |
| Message         | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %DiskSpace%</li> </ul> |

**TABLE 6-16. Component Update/Rollback Unsuccessful**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.   |
| Alert level | Displays the alert level in email messages.  |
| Recipients  | Specify the recipients who will receive the triggered alert email message.   |
| Subject     | Specify the subject of the triggered alert email message.  |
| Message     | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %ComponentList%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> </ul> |

**TABLE 6-17. Email Messages Timed Out Without Analysis Results**


| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Status          | Select an option to enable or disable the alert.   |
| Alert level     | Displays the alert level in email messages.  |
| Email messages  | Specify the email message threshold that will trigger the alert.                               |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |
| Recipients      | Specify the recipients who will receive the triggered alert email message.                     |
| Subject         | Specify the subject of the triggered alert email message.                                      |

| PARAMETER | DESCRIPTION  |
|-----------|--|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %MessageList%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-18. Email Message Encryption/Decryption Unsuccessful**


| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Status          | Select an option to enable or disable the alert.   |
| Alert level     | Displays the alert level in email messages.  |
| Email messages  | Specify the email message threshold that will trigger the alert.   |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients      | Specify the recipients who will receive the triggered alert email message.   |
| Subject         | Specify the subject of the triggered alert email message.  |
| Message         | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %MessageList%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-19. Low Free Threat Quarantine Disk Space**

| PARAMETER                         | DESCRIPTION   |
|-----------------------------------|---|
| Status                            | Select an option to enable or disable the alert.  |
| Alert level                       | Displays the alert level in email messages.   |
| Free threat quarantine disk space | <p>The lowest disk space threshold that triggers the alert.</p> <hr/> <div>  <b>Note</b> </div> <p><b>Free threat quarantine disk space</b> refers to the percentage of space remaining on the disk partition to store messages with detected threats.</p> <hr/> |
| Alert frequency                   | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.  |
| Recipients                        | Specify the recipients who will receive the triggered alert email message.  |
| Subject                           | Specify the subject of the triggered alert email message.   |
| Message                           | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %DiskSpace%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul>  |

**TABLE 6-20. High Memory Usage**

| PARAMETER   | DESCRIPTION                                      |
|-------------|--|
| Status      | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages.      |


| PARAMETER            | DESCRIPTION   |
|----------------------|---|
| Average memory usage | <p>Select the threshold for average memory usage that will trigger the alert.</p> <hr/> <div>  <b>Note</b> </div> <p><b>Free disk space</b> refers to the amount of space remaining on the disk partition.</p> <hr/>               |
| Alert frequency      | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.  |
| Recipients           | Specify the recipients who will receive the triggered alert email message.  |
| Subject              | Specify the subject of the triggered alert email message.   |
| Message              | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %MemoryThreshold%</li> <li>• %MemoryUsage%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-21. Long Message Deferred Queue**

| PARAMETER         | DESCRIPTION  |
|-------------------|--|
| Status            | Select an option to enable or disable the alert.   |
| Alert level       | Displays the alert level in email messages.  |
| Deferred messages | Specify the email message threshold that will trigger the alert.                               |
| Alert frequency   | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |

| PARAMETER  | DESCRIPTION  |
|------------|--|
| Recipients | Specify the recipients who will receive the triggered alert email message.   |
| Subject    | Specify the subject of the triggered alert email message.  |
| Message    | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeferredQueue%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %QueueThreshold%</li> </ul> |

**TABLE 6-22. Low Free Spam Quarantine Disk Space**

| PARAMETER                       | DESCRIPTION  |
|---------------------------------|--|
| Status                          | Select an option to enable or disable the alert.   |
| Alert level                     | Displays the alert level in email messages.  |
| Free spam quarantine disk space | <p>The lowest disk space threshold that triggers the alert.</p> <hr/> <div>  <b>Note</b><br/> <b>Free spam quarantine disk space</b> refers to the percentage of space remaining on the disk partition to store spam messages. </div> <hr/> |
| Alert frequency                 | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients                      | Specify the recipients who will receive the triggered alert email message.   |
| Subject                         | Specify the subject of the triggered alert email message.  |

| PARAMETER | DESCRIPTION  |
|-----------|--|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %DiskSpace%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-23. Account Locked**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.   |
| Alert level | Displays the alert level in email messages.  |
| Recipients  | Specify the recipients who will receive the triggered alert email message.   |
| Subject     | Specify the subject of the triggered alert email message.  |
| Message     | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %Account%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %DateTime%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-24. Unsuccessful DKIM Signing**

| PARAMETER   | DESCRIPTION                                      |
|-------------|--|
| Status      | Select an option to enable or disable the alert. |
| Alert level | Displays the alert level in email messages.      |

| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Email messages  | Specify the email message threshold that will trigger the alert.   |
| Alert frequency | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients      | Specify the recipients who will receive the triggered alert email message.   |
| Subject         | Specify the subject of the triggered alert email message.  |
| Message         | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %TotalMessages%</li> <li>• %Interval%</li> <li>• %DateTime%</li> <li>• %DeviceName%</li> <li>• %DeviceIP%</li> <li>• %ConsoleURL%</li> </ul> |

**TABLE 6-25. Connection Issue**

| PARAMETER          | DESCRIPTION  |
|--------------------|--|
| Status             | Select an option to enable or disable the alert.   |
| Alert level        | Displays the alert level in email messages.  |
| Alert frequency    | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |
| Monitored services | Select one or more services to monitor.  |
| Recipients         | Specify the recipients who will receive the triggered alert email message.                     |
| Subject            | Specify the subject of the triggered alert email message.                                      |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"><li>• %ServiceList%</li><li>• %DateTime%</li><li>• %DiagnosisTip%</li><li>• %DeviceName%</li><li>• %DeviceIP%</li><li>• %ConsoleURL%</li></ul> |

## Informational Alert Parameters



### Note

For explanations about available message tokens in each alert, see [Alert Notification Message Tokens on page B-3](#).

**TABLE 6-26. Threat Detection Surge**

| PARAMETER         | DESCRIPTION  |
|-------------------|--|
| Status            | Select an option to enable or disable the alert.   |
| Alert level       | Displays the alert level in email messages.  |
| Detected messages | Select the detections threshold that will trigger the alert.                                   |
| Alert frequency   | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |
| Recipients        | Specify the recipients who will receive the triggered alert email message.                     |
| Subject           | Specify the subject of the triggered alert email message.                                      |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"><li>• %ConsoleURL%</li><li>• %DateTime%</li><li>• %DetectionCount%</li><li>• %DetectionThreshold%</li><li>• %DeviceIP%</li><li>• %DeviceName%</li><li>• %Interval%</li></ul> |

**TABLE 6-27. Processing Surge**

| PARAMETER          | DESCRIPTION  |
|--------------------|--|
| Status             | Select an option to enable or disable the alert.   |
| Alert level        | Displays the alert level in email messages.  |
| Processed messages | The email message threshold that triggers the alert.   |
| Alert frequency    | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria. |
| Recipients         | Specify the recipients who will receive the triggered alert email message.                     |
| Subject            | Specify the subject of the triggered alert email message.                                      |

| PARAMETER | DESCRIPTION   |
|-----------|---|
| Message   | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %Interval%</li> <li>• %ProcessingCount%</li> <li>• %ProcessingThreshold%</li> </ul> |

**TABLE 6-28. Component Update/Rollback Successful**

| PARAMETER   | DESCRIPTION  |
|-------------|--|
| Status      | Select an option to enable or disable the alert.   |
| Alert level | Displays the alert level in email messages.  |
| Recipients  | Specify the recipients who will receive the triggered alert email message.   |
| Subject     | Specify the subject of the triggered alert email message.  |
| Message     | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %ConsoleURL%</li> <li>• %ComponentList%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> </ul> |

**TABLE 6-29. Data Loss Prevention Incident**

| PARAMETER                | DESCRIPTION  |
|--------------------------|--|
| Status                   | Select an option to enable or disable the alert.   |
| Alert level              | Displays the alert level in email messages.  |
| Detected messages        | Select the detections threshold that will trigger the alert.   |
| DLP templates to monitor | Select a list view option and one or more DLP templates to monitor.  |
| Alert frequency          | View the time interval that Deep Discovery Email Inspector checks for the alert rule criteria.   |
| Recipients               | Specify the recipients who will receive the triggered alert email message.   |
| Subject                  | Specify the subject of the triggered alert email message.  |
| Message                  | <p>Specify the body of the triggered alert email message.</p> <p>Use the following tokens to customize your message:</p> <ul style="list-style-type: none"> <li>• %DetectionCount%</li> <li>• %DetectionThreshold%</li> <li>• %Interval%</li> <li>• %MessageList%</li> <li>• %DateTime%</li> <li>• %DeviceIP%</li> <li>• %DeviceName%</li> <li>• %ConsoleURL%</li> </ul> |

## Reports

Deep Discovery Email 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 Email 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.



### Note

Configure the SMTP server to send notifications. For details, see [Configuring the Notification SMTP Server on page 8-194](#).

---

## Procedure

1. Go to **Alerts / Reports > Reports > Schedules**.
2. Enable a scheduled report by selecting the associated interval.
  - **Generate daily report**
  - **Generate weekly report**
  - **Generate monthly report**
3. Specify when to generate the report.



### Note

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.



### Note

Separate multiple recipients with a semicolon.

---

5. Optional: Select the **Include detailed information** check box to include a list containing the high-risk messages, alerts, and suspicious objects found during analysis.
  6. Click **Save**.
- 

## Generating On-Demand Reports

---

### Procedure

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

| OPTION                       | DESCRIPTION   |
|------------------------------|---|
| Period                       | Select the scope and start time for report generation.  |
| Include detailed information | Optional: Select the check box to include a list containing the high-risk messages, alerts, and suspicious objects found during analysis. |
| Recipients                   | Specify the recipients. Separate multiple recipients with a semicolon.  |

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 recipients.
-



# Chapter 7

## Logs

Topics include:

- *Time-Based Filters and DST on page 7-2*
- *Email Message Tracking on page 7-2*
- *MTA Events on page 7-7*
- *System Events on page 7-8*
- *Message Queue Logs on page 7-10*
- *Email Submission Logs on page 7-14*
- *Time-of-Click Protection Logs on page 7-15*

## Time-Based Filters and DST

When querying logs using time-based filters, the query assumes that the selected time range is based on the current Daylight Savings Time (DST) status. For example, if the time shifts from 2 a.m. back to 1 a.m. for DST and you query 0100-0159 after DST, the query matches the logs from the new 0100-0159 after the shift. Even though the local times match, the query results do not show logs matching the pre-DST time.

## Email Message Tracking

Track any email message that passed through Deep Discovery Email Inspector, including blocked and delivered messages. Deep Discovery Email Inspector records message details, including the sender, recipients, and the taken policy action.

Message tracking logs indicate if an email message was received or sent by Deep Discovery Email Inspector. Message tracking logs also provide evidence about Deep Discovery Email Inspector investigating an email message.

## Querying Message Tracking Logs

---

### Procedure

1. Go to **Logs > Message Tracking**.
2. Specify the search criteria.



#### Note

No wildcards are supported. Deep Discovery Email Inspector uses fuzzy logic to match search results.

---

| FILTER | DESCRIPTION   |
|--------|---|
| Period | Select a predefined time range or specify a custom range. |

| FILTER              | DESCRIPTION  |
|---------------------|--|
| Recipients          | Specify a recipient email address. Only one address is allowed.  |
| Email header (To)   | Specify a primary recipient email address in the email header.   |
| Sender              | Specify the sender email address.  |
| Email header (From) | Specify the author email address in the email header.  |
| Subject             | Specify the email message subject.   |
| Direction           | Specify the message direction.   |
| Message ID          | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com  |
| Source IP           | Specify the MTA IP address nearest to the email sender. The source IP is the IP address of the attack source, compromised MTA, or a botnet with mail relay capabilities.<br><br>A compromised MTA is usually a third-party open mail relay used by attackers to send malicious email messages or spam without detection. |
| Risk level          | Select <b>All</b> or the email message risk level.   |
| TLS (Upstream)      | Select a TLS version for inbound SMTP traffic.   |
| TLS (Downstream)    | Select a TLS version for outbound SMTP traffic.  |

| FILTER        | DESCRIPTION  |
|---------------|--|
| Latest status | <p>Select any of the following check boxes:</p> <ul style="list-style-type: none"> <li>• <b>Deleted:</b> Messages that were deleted based on content filtering or threat protection rules, or from the <b>Quarantine</b>.</li> <li>• <b>Delivered/Processing completed:</b> Messages that were delivered. In BCC mode and SPAN/TAP mode, email messages with this status are discarded.</li> <li>• <b>Delivery unsuccessful:</b> Messages that could not be delivered. In BCC mode and SPAN/TAP mode, email messages are never delivered.</li> <li>• <b>Recipient changed:</b> Messages with the recipient changed.</li> <li>• <b>Quarantined:</b> Messages that were quarantined in keeping with your Deep Discovery Email Inspector policies. In BCC mode and SPAN/TAP mode, email messages are never quarantined.</li> <li>• <b>Queued for delivery:</b> Messages that are pending delivery. In BCC mode and SPAN/TAP mode, email messages with this status are queued to be discarded.</li> <li>• <b>Queued for sandbox analysis:</b> Messages that are pending analysis.</li> </ul> |

### 3. Click **Query**.

Logs matching the search criteria appear in the table. The query results include message ID, recipients, sender, subject, risk level, latest status, and received timestamp.



#### Note

You can clear the search criteria by clicking **Clear filters**.

### 4. View the results.

- Click the ► icon next to a row to view detailed information about the email message.

| FIELD              | DESCRIPTION   |
|--------------------|---|
| Message details    | <p>This field displays the following information:</p> <ul style="list-style-type: none"> <li>• <b>Source IP:</b> Displays the MTA IP address nearest to the email message sender.<br/>Example: 123 . 123 . 123 . 123.</li> <li>• <b>Sender IP:</b> Displays the sender IP address</li> <li>• <b>Direction:</b> Displays the SMTP traffic direction</li> <li>• <b>TLS (Upstream):</b> Displays the TLS version for the inbound SMTP traffic</li> <li>• <b>TLS (Downstream):</b> Displays the TLS version for the outbound SMTP traffic</li> </ul>  |
| Processing history | <p>View how Deep Discovery Email Inspector processed the email message. The following are the possible processing actions:</p> <ul style="list-style-type: none"> <li>• <b>Action set to 'pass':</b> <ul style="list-style-type: none"> <li>• The <b>Pass</b> policy action was applied to the email message.</li> <li>• A copy of the email message was released by the user. This only applies if the <b>Strip attachments, redirect links to blocking page, and tag</b> and <b>Strip attachments, redirect links to warning page, and tag</b> policies were applied to the original email message.</li> </ul> </li> <li>• <b>Deleted:</b> The email message was deleted based on content filtering or threat protection rules, or from the <b>Quarantine</b>.</li> <li>• <b>Delivered:</b> The email message was delivered.</li> <li>• <b>Not analyzed:</b> Virtual Analyzer was unable to complete the analysis for the reason specified.</li> <li>• <b>Processing completed:</b> Analysis was completed and the email message was discarded. This is the final status in BCC and SPAN/TAP mode.</li> </ul> |

| FIELD  | DESCRIPTION  |
|--------|--|
|        | <ul style="list-style-type: none"> <li>• <b>Quarantined</b> (reason): The email message was quarantined in keeping with your Deep Discovery Email Inspector policies. In BCC mode and SPAN/TAP mode, email messages are never quarantined.</li> <li>• <b>Queued for delivery</b>: The email message is pending delivery. In BCC mode and SPAN/TAP mode, email messages with this status are queued to be discarded.</li> <li>• <b>Received</b>: The email message was received by Deep Discovery Email Inspector.</li> <li>• <b>Recipient changed</b>: The recipient for the email message has been changed.</li> <li>• <b>Sent for analysis</b>: The email message was sent to Virtual Analyzer for analysis.</li> <li>• <b>Stripped</b>: Attachments were stripped from the email message and it was passed for delivery.</li> </ul> |
| Action | <p>Do any of the following:</p> <p>Quarantined Message:</p> <ul style="list-style-type: none"> <li>• <b>View in Quarantine</b></li> <li>• <b>Release from Quarantine</b></li> <li>• <b>View in Detected Messages</b></li> </ul> <p>Non-Quarantined Message, with high/medium/low risk level:</p> <p><b>View in Threat Messages</b></p> <p>No Risk Message:</p> <p><b>No Action Links</b></p>   |

**Note**

Deep Discovery Email Inspector sorts logs using **UTC 0** time, even if the display is in local time.

---

5. Perform additional actions.

- Click **Export** to save the query results in a CSV file.

**Note**

Only the first 50000 entries in the query results are included in the CSV file.

---

- The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.
- 

## MTA Events

View connection details about Postfix and SMTP activity on your network.

**Note**

Deep Discovery Email Inspector automatically purges logs when there are a total of 100 log files that are each 51200KB. The most recent 10 logs can be queried.

---

## Querying MTA Event Logs

---

### Procedure

1. Go to **Logs > MTA**.
2. Specify the time range to query logs.
3. Click **Query**.

All logs matching the time criteria appear in the table.

4. View the results.

| FIELD       | DESCRIPTION                               |
|-------------|---|
| Timestamp   | The date and time when the event occurred |
| Description | The log event description                 |

**Note**

Deep Discovery Email Inspector sorts logs using **UTC 0** time, even if the display is in local time.

---

**5. Perform additional actions.**

- Click **Export to CSV** to save the query results in a CSV file.
  - The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.
- 

## System Events

View details about user access, policy modification, network setting changes, and other events that occurred using the Deep Discovery Email Inspector management console.

Deep Discovery Email Inspector maintains two system event log types:

- Update events: All component update events
- Audit logs: All user access events
- EUQ logs: All End-User Quarantine events

**Note**

- Deep Discovery Email Inspector purges logs based on the settings you configure on the **Storage Maintenance** screen.

For details, see [Configuring Storage Maintenance on page 8-224](#).

- For a list of system event logs available, see [System Event Logs on page F-1](#).

## Querying System Event Logs

### Procedure

1. Go to **Logs > System**.
2. Specify the time range to query logs.
3. View the results.

| FIELD       | DESCRIPTION  |
|-------------|--|
| Timestamp   | The date and time when the event occurred  |
| Event Type  | Deep Discovery Email Inspector records the following system event log types: <ul style="list-style-type: none"><li>• Update events</li><li>• Audit logs</li><li>• EUQ logs</li></ul> |
| Description | The log event description  |

**Note**

Deep Discovery Email Inspector sorts logs using **UTC 0** time, even if the display is in local time.

4. Perform additional actions.

- From the **Show** drop-down menu at the top-right side, select an event type to filter the results.
  - Click **Export** to save the query results in a CSV file.
  - The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.
- 

## Message Queue Logs

When Deep Discovery Email Inspector receives an email message, the message is stored in one of the following message queues:

- **Incoming:** Stores email messages waiting to be processed and delivered
- **Active:** Stores email messages that Deep Discovery Email Inspector has opened for processing
- **Deferred:** Stores email messages that Deep Discovery Email Inspector cannot deliver after processing

You can view the message queue logs to determine when a message was added to a message queue and perform actions (deliver, reroute, or delete) on selected messages.

The following table describes the information on the **Message Queue Logs** screen.

| FIELD        | DESCRIPTION                                     |
|--------------|---|
| Received     | View the time the message was received          |
| Type         | View the message queue type                     |
| Message ID   | View the unique ID for the email message        |
| Sender       | View the sender email address                   |
| Recipient(s) | View the email address of the message recipient |
| Subject      | View the message subject                        |

| FIELD                | DESCRIPTION  |
|----------------------|--|
| Size (Bytes)         | View the message size in bytes   |
| Archive/MTA Server   | View the address of the archive server or MTA server to which Deep Discovery Email Inspector sends the message |
| Message Type         | View the message type  |
| Last Delivery Status | View the status of the last delivery action performed  |

## Querying Message Queue Logs

You can search for messages in the message queues and deliver, reroute, or delete the messages.

### Procedure

1. Go to **Logs > Message Queue**.
2. Specify the search criteria.



#### Note

- If you do not specify a search criteria, the system displays up to the latest 10000 log entries on the **Message Queue** screen.
- You can clear the search criteria by clicking **Clear filters**.

| FILTER       | DESCRIPTION   |
|--------------|---|
| Type         | Select a message queue type.                                    |
| Recipient(s) | Specify a recipient email address. Only one address is allowed. |
| Subject      | Specify the email message subject.                              |

| FILTER             | DESCRIPTION   |
|--------------------|---|
| Message Type       | Select one of the following options: <ul style="list-style-type: none"> <li>• <b>All:</b> All notifications and archive messages</li> <li>• <b>System generated:</b> Notifications and archive messages that are sent from Deep Discovery Email Inspector.</li> <li>• <b>Received:</b> Messages that are received and scanned by Deep Discovery Email Inspector.</li> </ul> |
| Sender             | Specify the sender email address.   |
| Message ID         | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com   |
| Archive/MTA server | Specify the address of an archive server or MTA server.   |

### 3. Click **Query**.

Messages matching the search criteria appear in the table.

You can perform one of the following actions on the messages:

- **Deliver:** Delivers the selected messages to recipients. You can check the delivery status in the log table.
- **Deliver All:** Delivers all messages in the deferred message queue to recipients
- **Reroute:** Reroutes the selected messages to an SMTP server you specify



#### Note

For more information, see [Rerouting Messages in Message Queues on page 7-13](#).

- **Reroute All:** Reroutes all messages in the deferred and incoming queues to the SMTP server you specify

**Note**

For more information, see [Rerouting Messages in Message Queues on page 7-13](#).

---

- **Delete:** Deletes the selected messages
  - **Delete All:** Deletes all messages
- 

## Rerouting Messages in Message Queues

---

**Note**

Message reroute settings only take effect when Deep Discovery Email Inspector is in MTA mode.

---

On the **Message Queue Logs** screen, you can reroute selected or all messages in the deferred and incoming message queues to an SMTP server that you specify.

---

### Procedure

1. Go to **Logs > Message Queue**.
2. Do one of the following:
  - Select one or more entries and click **Reroute** to reroute the selected messages.
  - Select **Reroute All** to reroute all messages in the deferred and incoming queues.
3. A dialog box appears if a message is in the active message queue. Click **OK**.
4. On the **Specify SMTP Server** screen that appears, specify the IP address or fully qualified domain name and port number of an SMTP server to forward email messages.

## 5. Click **Reroute**.

---

# Email Submission Logs

When you submit message samples to Deep Discovery Email Inspector for analysis, you can view the submission results in the logs.

## Querying Email Submission Logs

---

### Procedure

1. Go to **Logs > Email Submission**.
2. Specify the search criteria.

| FILTER              | DESCRIPTION   |
|---------------------|---|
| Risk level          | Select <b>All</b> or the email message risk level.                                |
| Period              | Select a predefined time range or specify a custom range.                         |
| Message ID          | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com |
| Email header (From) | Specify the author email address in the email header.                             |
| Submitter name      | Specify the user account name.  |
| Subject             | Specify the email message subject.  |
| Email header (To)   | Specify a primary recipient email address in the email header.                    |
| Recipients          | Specify a recipient email address. Only one address is allowed.                   |

3. Click **Query**.

Logs matching the search criteria appear in the table. The query results include received timestamp, message ID, submitter, subject, risk level, links to view detailed detection information (if available), and analysis completion time.

**Note**

You can clear the search criteria by clicking **Clear**.

## Time-of-Click Protection Logs

The Time-of-Click Protection logs provide detailed information on URL detections and the actions that Deep Discovery Email Inspector performed at the time of user clicks.

### Querying Time-of-Click Protection Logs

#### Procedure

1. Go to **Logs > Time-of-Click Protection**.
2. Specify the search criteria. To apply advanced filters, see [Applying Advanced Filters on page 7-15](#).

| FILTER | DESCRIPTION   |
|--------|---|
| Action | Select an action performed on detected URLs.                  |
| Period | Select a predefined time range or specify a custom range.     |
| URL    | Specify a keyword to search for URLs and click <b>Query</b> . |

Logs matching the search criteria appear in the table.

**Note**

You can clear the search criteria by clicking **Cancel**.

### Applying Advanced Filters

In addition to basic filters, you can apply advanced filters to query logs.

---

## Procedure

### 1. Click **Advanced filters**.

The advanced filters appear.

### 2. Specify the information to filter.

| FILTER              | DESCRIPTION  |
|---------------------|--|
| Message ID          | Specify the unique message ID.<br>Example: 20160603021433.F0304120A7A@example.com  |
| Email header (From) | Specify the author email address in the email header.  |
| Sender              | Specify one or more sender email addresses. Use a semicolon to separate multiple entries.                                |
| Subject             | Specify the email message subject.   |
| Email header (To)   | Specify one or more primary recipient email addresses in the email header. Use a semicolon to separate multiple entries. |
| Recipients          | Specify one or more recipient email addresses. Use a semicolon to separate multiple entries.                             |

### 3. Click **Query**.

---

# Chapter 8

## Administration

Topics include:

- *Component Updates on page 8-2*
- *Product Updates on page 8-6*
- *System Settings on page 8-187*
- *Sender Filtering/Authentication Settings on page 8-52*
- *End-User Quarantine on page 8-82*
- *Mail Settings on page 8-94*
- *Integrated Products/Services on page 8-123*
- *Scanning / Analysis on page 8-9*
- *System Maintenance on page 8-217*
- *Accounts / Contacts on page 8-209*
- *Licenses on page 8-228*
- *About Deep Discovery Email Inspector on page 8-233*

## 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 spear-phishing attacks and social engineering attack patterns.

## Components

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

**TABLE 8-1. Components**

| COMPONENT  | DESCRIPTION  |
|--|--|
| Advanced Threat Correlation Pattern  | The Advanced Threat Correlation Pattern contains a list of file features that are not relevant to any known threats.   |
| Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)<br>Advanced Threat Scan Engine for Deep Discovery (Linux, 32-bit) | The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection.                       |
| Antispam Engine (Enterprise Linux, 32-bit)   | The Trend Micro Antispam Engine detects spam and phishing content in email messages and email attachments.<br><br>The Antispam Engine also includes the Email Malware Threat Scan Engine that performs advanced threat scans on email attachments (including script files and Microsoft Office macroware) to detect malware. |
| Antispam Pattern   | The Antispam Pattern identifies the latest spam in email messages and email attachments.   |
| Contextual Intelligence Query Handler (Linux, 32-bit)<br>Contextual Intelligence Query Handler (Linux, 64-bit)                   | The Contextual Intelligence Query Handler processes the behaviors identified by the Contextual Intelligence Engine and sends the report to the Predictive Machine Learning engine.   |

| COMPONENT  | DESCRIPTION   |
|--|---|
| Deep Discovery Malware Pattern                               | <p>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.</p> <p>Deep Discovery Email Inspector also uses the Deep Discovery Malware Pattern to detect and protect organizations against mass-mailing attacks.</p> |
| Trusted Certificate Authorities                              | Trusted Certificate Authorities Pattern provides the trusted certificate authorities to verify PE signatures.   |
| IntelliTrap Exception Pattern                                | The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning.  |
| IntelliTrap Pattern  | The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats.   |
| Network Content Correlation Pattern                          | The Network Content Correlation Pattern implements detection rules defined by Trend Micro.  |
| Network Content Inspection Engine (Linux, User mode, 64-bit) | The Network Content Inspection Engine is used to perform network scanning.  |
| Network Content Inspection Pattern                           | The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning.  |
| Script Analyzer Pattern (Deep Discovery)                     | The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.   |
| Spyware/Grayware Pattern                                     | The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware.   |
| Virtual Analyzer Sensors                                     | The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer.   |

| COMPONENT                              | DESCRIPTION  |
|--|--|
| Virtual Analyzer Configuration Pattern | The Virtual Analyzer Configuration Pattern contains configuration information for Virtual Analyzer, such as supported threat types and supported file types. |

## Update Source

Deep Discovery Email Inspector downloads components from the Trend Micro ActiveUpdate server, the default update source. Deep Discovery Email Inspector can be configured to download components from another update source specifically set up in your organization.



### Note

If Deep Discovery Email Inspector is registered to Apex Central, you can configure Deep Discovery Email Inspector to download directly from Apex Central. For details on how a Apex Central server can act as an update source, see the *Trend Micro Apex Central Administrator's Guide*.

---

## Configuring the Update Source

Frequently update components to receive protection from the latest threats. By default, components automatically receive updates from the Trend Micro ActiveUpdate server. Receive updates from another Internet location by configuring a different update source.

---

### Procedure

1. Go to **Administration > Component Updates > Source**.
2. Configure the update source settings.

- **Trend Micro ActiveUpdate server**

Obtain the latest components from the Trend Micro ActiveUpdate server (default).

- **Other update source**

Specify a different update source location. The update source URL must begin with “http://” or “https://”.

Example: `http://update.mycompany.com`.

**Note**

The update source does not support UNC path format.

---

3. Click **Save**.
- 

## Updating Components

Update components to immediately download the component updates from the update source server. For information about the update source, see [Configuring the Update Source on page 8-4](#).

---

### Procedure

1. Go to **Administration > Component Updates > Components**.
  2. Select one or more components.
  3. Click **Update**.
  4. At the confirmation message, click **OK**.
- 

## 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**.

The components revert to the most recent version.

4. At the confirmation message, click **OK**.
- 

## 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 Email Inspector.

## System Updates

After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

**TABLE 8-2. System Updates**

| SYSTEM UPDATE | DESCRIPTION  |
|---------------|--|
| Hotfix        | <p>A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.</p> <hr/> <p> <b>Note</b><br/>A new hotfix may include previous hotfixes until Trend Micro releases a patch.</p> <hr/> |

| SYSTEM UPDATE  | DESCRIPTION   |
|----------------|---|
| Security patch | A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.      |
| Patch          | A patch is a group of hotfixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. |

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

<http://downloadcenter.trendmicro.com/>

## Managing Patches

From time to time, Trend Micro releases a new firmware version for a reported known issue or an upgrade that applies to the product. Find available firmware versions at <http://downloadcenter.trendmicro.com>.

You can install a patch file on Trend Micro using one of the following methods:

- The Deep Discovery Email Inspector management console
- Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

---

### Procedure

1. Go to **Administration > Product Updates > Hotfixes / Patches**.
2. Under **History**, verify the software 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 Email Inspector uses the most recent previous configuration. For example, rolling back patch 3 returns Deep Discovery Email Inspector to a patch 2 state.
- 

## Upgrading Firmware

From time to time, Trend Micro releases a new firmware version for a reported known issue or an upgrade that applies to the product. Find available firmware versions at <http://downloadcenter.trendmicro.com>.

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

You can upgrade the firmware on Deep Discovery Email Inspector using one of the following methods:

- The Deep Discovery Email Inspector management console
  - Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.
- 



### Note

Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete, and upgrading from Deep Discovery Email Inspector 5.0 or 3.6 to Deep Discovery Email Inspector 5.1 may take an hour or more. Trend Micro recommends starting the upgrade during off-peak office hours. Installing the update restarts Deep Discovery Email Inspector.

---

## Procedure

1. Back up configuration settings.

*[Backing Up or Restoring a Configuration on page 8-217](#)*

2. Obtain the firmware image.

- Download the Deep Discovery Email Inspector firmware image from the Trend Micro Download Center at:

<http://downloadcenter.trendmicro.com>

- Obtain the firmware package from your Trend Micro reseller or support provider.
- 3. Save the image to any folder on a computer.
- 4. Go to **Administration > Product Updates > Firmware**.
- 5. Next to **Software version**, verify your firmware version.
- 6. Browse for the firmware update package.
- 7. Click **Install**.

**Tip**

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

---

After the installation is complete, Deep Discovery Email Inspector automatically restarts and the command line interface appears.

- 8. Perform the following post-installation steps:
    - Clear the browser cache.
    - Manually log onto the web console.
    - If Deep Discovery Email 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.
- 

## Scanning / Analysis

Use the **Scanning / Analysis** screen to configure settings for the following features:

- [Virtual Analyzer on page 1-13](#)
- [File Passwords on page 8-32](#)

- [Smart Protection on page 8-36](#)
- [Smart Feedback on page 8-40](#)
- [YARA Rules on page 8-42](#)
- [Time-of-Click URL Protection on page 8-46](#)
- [Business Email Compromise on page 8-48](#)
- [Cousin Domains on page 8-50](#)

## Email Scanning

When an email message enters your network, Deep Discovery Email Inspector gathers security intelligence from several Trend Micro Smart Protection Network services to investigate the email message's risk level.

- Analyzing file attachments  
See [Advanced Threat Scan Engine on page 1-13](#).
- Analyzing embedded links (URLs)  
See [Web Reputation Services on page 1-14](#).
- Social Engineering Attack Protection  
See [Social Engineering Attack Protection on page 1-10](#).
- Predictive Machine Learning  
See [Predictive Machine Learning on page 1-14](#).
- Business Email Compromise Protection  
See [Business Email Compromise on page 8-48](#).

After scanning the email message for suspicious files, URLs, and characteristics, Deep Discovery Email Inspector correlates the results to either assign a risk level and immediately execute a policy action based on the risk level, or send the file, URL and message samples to Virtual Analyzer for further analysis.

**Note**

The file password settings affect both Deep Discovery Email Inspector email scanners and Virtual Analyzer.

## 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.

## Virtual Analyzer Overview

The **Overview** screen varies depending on whether Deep Discovery Email Inspector is configured to use the internal or external Virtual Analyzer sandbox environment.

If Deep Discovery Email Inspector is using an external Virtual Analyzer, you can configure the integration settings and check the status of the external Virtual Analyzer sandbox environment on the **External Integration** screen.

If Deep Discovery Email Inspector is using an internal Virtual Analyzer, click **Status** to check the status of the Virtual Analyzer sandbox environment. View the table to understand the real-time status of Virtual Analyzer and the sandbox images.

### Virtual Analyzer Statuses

The following table describes the Virtual Analyzer statuses.

**TABLE 8-3. Virtual Analyzer Statuses**

| STATUS                 | DESCRIPTION  |
|------------------------|--|
| Initializing...        | Virtual Analyzer is preparing the sandbox environment.                                       |
| Starting...            | Virtual Analyzer is starting all sandbox instances.  |
| Stopping...            | Virtual Analyzer is stopping all sandbox instances.  |
| Running                | Virtual Analyzer is analyzing samples.   |
| No images              | No images have been imported into Virtual Analyzer.  |
| Modifying instances... | Virtual Analyzer is increasing or decreasing the number of instances for one or more images. |
| Importing images...    | Virtual Analyzer is importing an image.  |

### Overall Status Table

The Virtual Analyzer **Overall Status** table shows the allocated instances, status (busy or idle), and the utilization information for each sandbox image.

**TABLE 8-4. Overall Status Table Descriptions**

| HEADER    | DESCRIPTION                          |
|-----------|--------------------------------------|
| Image     | Permanent image name                 |
| Instances | Number of deployed sandbox instances |

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

## 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.

Use the Image Preparation Tool to check that an image has the correct virtual machine settings, supported platforms and required applications before importing the image to Virtual Analyzer. For details about the Image Preparation Tool, see the *Virtual Analyzer Image Preparation User's Guide* at <http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx>.

## 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.

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

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

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

### Importing Virtual Analyzer Images

Virtual Analyzer supports OVA files between 1GB and 30GB 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.

If Deep Discovery Email Inspector is registered to Deep Discovery Director, you can also import an image to Deep Discovery Email Inspector through image deployment from Deep Discovery Director.

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Virtual Analyzer > Overview > 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 8-14](#).

- **HTTP or FTP server**

See [Importing an Image from an HTTP or FTP Server on page 8-16](#).

---

### 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 importing an image, verify

that your computer has established a connection to Deep Discovery Email Inspector. From the **Images** screen, check the connection status under **Step 1** on the management console.

---

### Procedure

1. Select **Local or network folder**.
2. Specify an image name with a maximum of 260 characters/bytes.
3. Click **Connect**.
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 Email Inspector management IP address.



#### Note

For information about configuring the Deep Discovery Email Inspector management IP address, see [Configuring Network Settings on page 8-187](#).

---

- 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.

**Note**

Virtual Analyzer deploys the imported image to sandbox instances immediately after the image uploads.

---

---

**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. For information about adding images, see [Importing Virtual Analyzer Images on page 8-14](#).

---

**Procedure**

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

| OPTION          | DESCRIPTION   |
|-----------------|---|
| URL             | Specify the HTTP or FTP URL.<br>Example: ftp://custom_ftp:1080/tmp/test.ova           |
| User name       | Optional: Specify the user name if authentication is required.                        |
| Password        | Optional: Specify the password if authentication is required.                         |
| Anonymous Login | Optional: Select to disable the user name and password, and authenticate anonymously. |

3. Click **Import**.
  4. Wait for deployment to complete.
- 

**Note**

Virtual Analyzer deploys instances immediately.

---


---

**Deleting Virtual Analyzer Images**

---

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Virtual Analyzer > Overview > 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 > Scanning / Analysis > Virtual Analyzer > Overview > Images**.
  2. Click **Modify**.  
The **Modify Instances** screen appears.
  3. Modify the instances allocated to any image.
  4. Click **Save**.
- 

## Configuring Virtual Analyzer Network and Filters

To reduce the number of files and messages in the Virtual Analyzer queues, configure filters for Virtual Analyzer submission.

---




### Note

- Object analysis is paused and settings are disabled whenever Virtual Analyzer is being configured.
  - Forcing file analysis and performing message filtering for Virtual Analyzer submission can impact system performance.
-

## Procedure

1. Go to **Administration > Scanning / Analysis > Virtual Analyzer**.
2. Specify **Settings**.

| OPTION             | DESCRIPTION  |
|--------------------|--|
| Network Connection | <div data-bbox="474 423 532 472"></div> <p><b>Note</b></p> <p>This section is available when Deep Discovery Email Inspector is using an internal Virtual Analyzer.</p> <p>When the internal Virtual Analyzer is set to connect to the Internet through a proxy server, reconfigure proxy settings after a configuration restore or firmware update on Deep Discovery Email Inspector.</p> <hr/> <p>From the <b>Network type</b> drop-down list, select how Virtual Analyzer connects to the network. For information about network types, see <a href="#">Virtual Analyzer Network Types on page 8-20</a>.</p> <p>If you select the <b>Custom Network</b> type, select a specific port for Virtual Analyzer traffic from the <b>Sandbox port</b> drop-down list and click <b>Configure IPv4 settings</b> to configure the network settings.</p> <p>If a proxy server is required for the internal Virtual Analyzer to connect to the Internet, select <b>Use a dedicated proxy server</b> from the drop-down list and provide the following information:</p> <ul style="list-style-type: none"> <li>• <b>Server address</b></li> <li>• <b>Port</b></li> <li>• <b>Proxy server requires authentication:</b> If authentication is required, select this check box and type the user name and password.</li> </ul> |

| OPTION                  | DESCRIPTION  |
|-------------------------|--|
| File Submission Filters | <p><b>Files:</b> Select the file types to have Virtual Analyzer perform one of the following actions:</p> <ul style="list-style-type: none"> <li>• Submit only highly suspicious files</li> <li>• Submit highly suspicious files and force analyze all selected file types</li> </ul> <p>To reduce the likelihood of false-positive detections, select <b>Do not analyze files found safe by the Certified Safe Software Service</b>.</p> <p>For details, see <a href="#">Certified Safe Software Service on page 8-20</a>.</p>  |
| URL Submission Filters  | <p>By default, URLs found safe are first submitted to the URL pre-filter before submitting to Virtual Analyzer. For messages with safe URLs, you can add one or more subject keywords to filter these messages for Virtual Analyzer submission. Safe URLs in matched messages are sent directly to Virtual Analyzer, bypassing the URL pre-filter.</p> <p><b>Keyword:</b> Type a subject keyword and click <b>Add</b> to add the keyword to the list.</p> <p>To delete a keyword from the list, select an entry and click <b>Delete</b>.</p> <hr/> <div data-bbox="569 883 626 932"></div> <p><b>Note</b><br/>You can specify up to 50 keywords.</p> <hr/> |
| Timeout Setting         | <p>Select how long Virtual Analyzer should wait before timing out a submitted object. By default, when the submission timeout is reached, Virtual Analyzer sends out submitted objects waiting in the queue without analysis. Timed out objects still receive risk levels from other scan engines.</p> <p>You can configure threat protection rules in policies to perform actions on timed out objects.</p> <p>For more information, see <a href="#">Configuring a Threat Protection Rule on page 5-50</a>.</p>   |

### 3. Click **Save**.

## Certified Safe Software Service

Certified Safe Software Service (CSSS) is the Trend Micro cloud database of known safe files. Trend Micro datacenters are queried to check submitted files against the database.

Enabling CSSS prevents known safe files from entering the Virtual Analyzer queue. This process:

- Saves computing time and resources
- Reduces the likelihood of false positive detections



### Tip

CSSS is enabled by default. Trend Micro recommends using the default settings.

---

## Virtual Analyzer Network Types

When simulating file and URL 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.

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



### Note

Internet access improves analysis by allowing samples to access C&C callback addresses or other external links.

---

| NETWORK TYPE       | DESCRIPTION  |
|--------------------|--|
| Management network | <p>Direct Virtual Analyzer traffic through the management port.</p> <hr/> <div data-bbox="561 329 619 391"></div> <div data-bbox="633 326 740 350"><b>Important</b></div> <p>Enabling connections to the management network may result in malware propagation and other malicious activity in the network.</p> <hr/>   |
| Custom network     | <p>Virtual Analyzer connects to the Internet using a port other than the management port.</p> <hr/> <div data-bbox="561 594 619 643"></div> <div data-bbox="633 591 682 615"><b>Note</b></div> <p>Trend Micro recommends using an environment isolated from the management network, such as a test network with Internet connection but without proxy settings, proxy authentication, and connection restrictions.</p> <hr/> |
| No network access  | <p>Isolate Virtual Analyzer traffic within the sandbox environment. The environment has no connection to an outside network.</p> <hr/> <div data-bbox="561 894 619 943"></div> <div data-bbox="633 891 682 915"><b>Note</b></div> <p>Virtual Analyzer has no Internet connection and relies only on its analysis engine.</p> <p>No URLs are submitted for analysis.</p> <hr/>  |


## Virtual Analyzer File Submission Filters

In addition to highly suspicious files, Virtual Analyzer can also scan for a variety of file types.

The following table shows the displayed file categories, contained full file types, and file extensions.

**TABLE 8-5. Virtual Analyzer File Submission Filters**

| <b>DISPLAYED FILE CATEGORY</b> | <b>FULL FILE TYPE</b>   | <b>EXAMPLE FILE EXTENSIONS</b>  |
|--------------------------------|---|---|
| Flash and other multimedia     | Scalable Vector Graphics (SVG)<br>Adobe™ Shockwave™ Flash file<br>Apple QuickTime media   | .svg<br>.swf<br>.mov  |
| HTML                           | Hypertext Markup Language file<br>Web page archive file   | .htm<br>.html<br>.xht<br>.xhtml<br>.mht<br>.mhtml   |
| Java                           | Java Archive (JAR)<br>Java class file   | .jar<br>.class  |
| Office                         | Microsoft™ Word™ document<br>Microsoft™ OLE document<br>Microsoft™ Office Word™ (2007 or later) document<br>Microsoft™ PowerPoint™ presentation<br>Microsoft™ Office PowerPoint™ (2007 or later) presentation<br>Microsoft™ Excel™ spreadsheet<br>Microsoft™ Office Excel™ (2007 or later) spreadsheet<br>Microsoft™ Office™ 2003 XML file<br>Microsoft™ Word™ 2003 XML document<br>Microsoft™ Excel™ 2003 XML spreadsheet<br>Microsoft™ PowerPoint™ 2003 XML presentation<br>Microsoft™ Publisher 2016 | .doc<br>.dot<br>.docx<br>.dotx<br>.pps<br>.ppsx<br>.ppt<br>.pptx<br>.pub<br>.xla<br>.xls<br>.xlsx<br>.xlt<br>.xlm |

| DISPLAYED FILE CATEGORY | FULL FILE TYPE   | EXAMPLE FILE EXTENSIONS  |
|-------------------------|--|--|
|                         | <p>Hancom™ Hancell spreadsheet</p> <p>Hancom™ Hangul Word Processor (HWP) document</p> <p>Hancom™ Hangul Word Processor (2014 or later) (HWPX) document</p> <p>JustSystems™ Ichitaro™ document</p> <p>JungUm™ Global document</p> <p>Microsoft™ Outlook™ Item</p> <p>Microsoft™ symbolic link format</p> <p>Microsoft™ Excel web query file</p> <p>Comma-separated values (CSV) file</p> <hr/> <p> <b>Note</b><br/>Only CSV files with suspicious DDEAuto commands are submitted to Virtual Analyzer for analysis.</p> <hr/> <p>OpenDocument Format (ODF)</p> | <p>.cell</p> <p>.xml</p> <p>.xlsb</p> <p>.xltx</p> <p>.hwp</p> <p>.hwp</p> <p>.hwp</p> <p>.jtd</p> <p>.gul</p> <p>.msg</p> <p>.slk</p> <p>.iqy</p> <p>.csv</p> <p>.odp</p> <p>.ods</p> <p>.odt</p> |
| Office with Macros      | <p>Microsoft™ Office Word™ (2007 or later) macro-enabled document</p> <p>Microsoft™ Office PowerPoint™ (2007 or later) macro-enabled presentation</p> <p>Microsoft™ Office Excel™ (2007 or later) macro-enabled spreadsheet</p>  | <p>.docm</p> <p>.dotm</p> <p>.potm</p> <p>.ppam</p> <p>.ppsm</p> <p>.pptm</p> <p>.xlam</p> <p>.xlsm</p> <p>.xltm</p>   |

| DISPLAYED FILE CATEGORY | FULL FILE TYPE                                 | EXAMPLE FILE EXTENSIONS |
|-------------------------|--|-------------------------|
| Other document formats  | Compiled HTML (CHM) help file                  | .chm                    |
|                         | Microsoft™ Windows™ Shell Binary Link shortcut | .lnk                    |
|                         | Microsoft™ Rich Text Format (RTF) document     | .rtf                    |
| PDF                     | Adobe™ Portable Document Format (PDF)          | .pdf                    |
| Scripts                 | Microsoft™ Windows™ Batch file                 | .bat                    |
|                         | Microsoft™ Windows™ Command Script file        | .cmd                    |
|                         | JavaScript™ file                               | .js                     |
|                         | JavaScript™ encoded script file                | .jse                    |
|                         | HTML Application file                          | .hta                    |
|                         | Microsoft™ Windows™ PowerShell script file     | .ps1                    |
|                         | Visual Basic™ encoded script file              | .vbe                    |
|                         | Visual Basic™ script file                      | .vbs                    |
|                         | Microsoft™ Windows™ script file                | .wsf                    |
|                         | Internet shortcut file                         | .url                    |
|                         | Linux shell executable file                    | .sh                     |
| Portable executables    | AMD™ 64-bit DLL file                           | .com                    |
|                         | Microsoft™ Windows™ 16-bit DLL file            | .cpl                    |
|                         | Microsoft™ Windows™ 32-bit DLL file            | .crt                    |
|                         | Executable and Linkable Format (ELF) file      | .dll                    |
|                         | Executable file (EXE)                          | .drv                    |
|                         |  | .elf                    |

**Note**

Only plain text or generic script files with .js or .vbs true file types are submitted to Virtual Analyzer for analysis.

| DISPLAYED FILE CATEGORY | FULL FILE TYPE                           | EXAMPLE FILE EXTENSIONS |
|-------------------------|--|-------------------------|
|                         | AMD™ 64-bit EXE file                     | .exe                    |
|                         | DIET DOS EXE file                        | .ocx                    |
|                         | Microsoft™ DOS EXE file                  | .scr                    |
|                         | IBM™ OS/2 EXE file                       | .sys                    |
|                         | LZEXE DOS EXE file                       |                         |
|                         | MIPS EXE file                            |                         |
|                         | MSIL Portable executable file            |                         |
|                         | Microsoft™ Windows™ 16-bit EXE file      |                         |
|                         | Microsoft™ Windows™ 32-bit EXE file      |                         |
|                         | ARJ compressed EXE file                  |                         |
|                         | ASPACK 1.x compressed 32-bit EXE file    |                         |
|                         | ASPACK 2.x compressed 32-bit EXE file    |                         |
|                         | GNU UPX compressed EXE file              |                         |
|                         | LZH compressed EXE file                  |                         |
|                         | LZH compressed EXE file for ZipMail      |                         |
|                         | MEW 0.5 compressed 32-bit EXE file       |                         |
|                         | MEW 1.0 compressed 32-bit EXE file       |                         |
|                         | MEW 1.1 compressed 32-bit EXE file       |                         |
|                         | PEPACK compressed executable             |                         |
|                         | PKWARE™ PKLITE™ compressed DOS EXE file  |                         |
|                         | PETITE compressed 32-bit executable file |                         |
|                         | PKZIP compressed EXE file                |                         |
|                         | WWPACK compressed executable file        |                         |

**Note**

Deep Discovery Email Inspector submits files of the following types to the external Virtual Analyzer only:

- Linux shell executable files (.sh)
- Executable and Linkable Format (ELF) file

Virtual Analyzer can scan the files that match the supported file types in an archive file. The following table lists the supported archive file types.

**TABLE 8-6. Archive file types**

| TRUE FILE TYPE | FULL FILE TYPE          | EXAMPLE FILE EXTENSIONS |
|----------------|-------------------------|-------------------------|
| 7ZIP           | 7-zip archive           | .7z                     |
| ACE            | WinAce archive          | .ace                    |
| ALZ            | ALZip archive           | .alz                    |
| AMG            | Fujitsu AMG archive     | .amg                    |
| ARJ            | ARJ archive             | .arj                    |
| BINHEX         | BinHex file             | .hqx                    |
| BZIP2          | BZIP2 archive           | .bz2<br>.bz2ip2         |
| CAB            | Microsoft™ Cabinet file | .cab                    |
| CPIO           | CPIO archive            | .cpio<br>.cpgz          |
| EGG            | ALZip archive           | .egg                    |
| GZIP           | GNU ZIP archive         | .gzip<br>.gz            |
| ICS            | iCalendar file          | .ics                    |

| TRUE FILE TYPE | FULL FILE TYPE   | EXAMPLE FILE EXTENSIONS           |
|----------------|--|-----------------------------------|
| LHA            | LHARC compressed archive   | .lha<br>.lharc                    |
| LZH            | Lempel-Ziv-Welch (LZW) Compressed Amiga archive                        | .lzh                              |
| MIME           | Multipurpose Internet Mail Extensions (MIME) Base64 file               | .eml<br>.email                    |
| MSG            | Microsoft™ Outlook™ Item   | .msg                              |
| RAR            | Roshal Archive (RAR) archive   | .rar                              |
| SIT            | Smith Micro™ StuffIt archive   | .sit<br>.sitx                     |
| TAR            | TAR archive  | .tar<br>.tgz                      |
| TNEF           | Microsoft™ Outlook™ Transport Neutral Encapsulation Format (TNEF) file | .tnef<br>.winmail.dat<br>.win.dat |
| UDF            | Universal Disk Format file   | .iso                              |
| UUCODE         | Uuencode file  | .uue                              |
| VCS            | vCalendar file   | .vcs                              |
| XZ             | XZ archive   | .xz                               |
| ZIP            | PKWARE PKZIP archive (ZIP)   | .zip                              |

The following table lists the Mac file types that Deep Discovery Email Inspector automatically submits to the external Mac sandbox for analysis, regardless of the submission settings. These files are not submitted to the internal Virtual Analyzer.

**Note**

If you configure Deep Discovery Email Inspector to use an external Virtual Analyzer and select the Java file category, Deep Discovery Email Inspector also submits Java archive (.jar) and class (.class) files to the external Mac sandbox for analysis.

**TABLE 8-7. Mac file types**

| TRUE FILE TYPE | FULL FILE TYPE             | EXAMPLE FILE EXTENSIONS |
|----------------|----------------------------|-------------------------|
| DMG            | Apple disk image file      | .dmg                    |
| PKG            | Mac OS X installation file | .pkg                    |
| Mach-O         | Mach object file           | .o                      |

## Configuring an External Virtual Analyzer

You can configure Deep Discovery Email Inspector to integrate with Deep Discovery Analyzer to perform suspicious object analysis.

### Procedure

1. Go to **Administration > Scanning / Analysis > Virtual Analyzer > External Integration**.
2. In the **Source** drop-down, select **External**.
3. In the **Server address** field, provide the IP address or FQDN of the Deep Discovery Analyzer server.
4. If your company uses a proxy server, select **Connect using a proxy server**.

**Note**

For information about configuring proxy settings, see [Configuring Proxy Settings on page 8-193](#).

5. Type the API key.
  6. (Optional) Click **Test Connection** to verify the server settings.
  7. Click **Save**.
- 

## Email Submissions

You can manually upload email message samples (in EML or MSG format) directly to Deep Discovery Email Inspector for analysis.

After the file upload process is complete, you can view the message summary information (for example, email header, recipients, policies matched, etc.). After submitting to Virtual Analyzer and the analysis process is complete, you can view the submission results by querying the email submission logs.

**Note**

- Deep Discovery Email Inspector supports message samples in EML and MSG formats only.
- For manually submitted message samples, Deep Discovery Email Inspector does NOT perform the following actions:
  - Send message copies to archive servers or detection notifications as specified in matched policies
  - Analyze content based on Email Reputation Service (ERS) or sender filtering/authentication settings
  - Generate message tracking logs
  - Quarantine and generate log entries for End-User Quarantine (EUQ)
  - Send email submission logs to syslog servers, Apex Central, or Deep Discovery Director

If a threat detection occurs on submitted message samples, Deep Discovery Email Inspector sends the detection logs to syslog servers, Apex Central, or Deep Discovery Director.

- Deliver messages when Deep Discovery Email Inspector is configured in MTA mode
- 

## Manually Submitting Email Message Samples

You can send suspicious email message samples in EML or MSG format to Deep Discovery Email Inspector for analysis.

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Email Submissions**.

The **Email Submissions** screen appears.

2. Do one of the following:

- Click **Select** to locate the .eml or .msg file to upload.
- Drag and drop an .eml or .msg file into the panel area.

The management console displays the following information in the **Message Details** section.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Message ID          | View the unique message ID.  |
| Email Header (From) | View the author email address in the email header.   |
| Email Header (To)   | View the primary recipient email address in the email header.  |
| Email Subject       | View the email subject of the suspicious email message.  |
| Message body        | View the body (up to 4K in length) of the email message.   |
| Polices             | View the policies and rules that are matched.<br><br>For more information on how Deep Discovery Email Inspector matches policies, see <a href="#">Policy Matching on page 5-25</a> and <a href="#">Policy Splintering on page 5-28</a> . |

3. Click **Submit**.

You can view the submission results on the **Email Submission Logs** screen.

For more information, see [Querying Email Submission Logs on page 7-14](#).

## URL Scanning

By default, Deep Discovery Email Inspector scans URLs in email messages and performs actions based on the risk levels and reputation scores.

Deep Discovery Email Inspector performs URL scanning for the following functions:

- Web Reputation Services

- Time-of-Click protection
- Suspicious object matching
- Virtual Analyzer analysis
- URL exceptions

Depending on your application needs, you can manually disable URL scanning in Deep Discovery Email Inspector.

**WARNING!**

Disabling URL scanning will severely affect the ability of Deep Discovery Email Inspector to detect and analyze malicious URLs.

---

## Disabling URL Scanning

Depending on your application needs, you can manually disable URL scanning in Deep Discovery Email Inspector.

**WARNING!**

Disabling URL scanning will severely affect the ability of Deep Discovery Email Inspector to detect and analyze malicious URLs.

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > URL Scanning**.
  2. Select **Disable URL Scanning**.
  3. Click **Save**.
- 

## File Passwords

Always handle suspicious files with caution. Trend Micro recommends adding such files to a password-protected archive file or password-protecting document files from being opened before transporting the files across the

network. Deep Discovery Email Inspector can also heuristically discover passwords in email messages to extract files.

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

For information on the password-protected file types Deep Discovery Email Inspector supports, see [Password-protected File Types on page 8-34](#).



#### Note

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

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

| TASK                       | DESCRIPTION  |
|----------------------------|--|
| Configure analysis timeout | Type the number of minutes in the <b>Analysis timeout</b> field to quarantine a message when Deep Discovery Email Inspector is unable to open and analysis a password-protected file in the message within the specified time. |
| Add a password             | Click <b>Add Password</b> to add a password to the list.<br>For more information, see <a href="#">Adding File Passwords on page 8-34</a> .   |
| Import passwords           | Click <b>Import Passwords</b> to import passwords from a selected file.<br>For more information, see <a href="#">Importing File Passwords on page 8-35</a> .   |
| Export all passwords       | Click <b>Export Passwords</b> to export all file passwords and save the file on your computer.   |

## Password-protected File Types

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

- 7z
- alz
- arj
- egg
- rar
- zip

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

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

## Adding File Passwords

A maximum of 100 passwords is allowed.

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > File Passwords**.
2. Click **Add Password**.
3. Type a password with only ASCII characters.



### Note

Passwords are case-sensitive and must not contain spaces.

---

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

## Importing File Passwords

You can add up to 100 passwords in Deep Discovery Email Inspector.

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > File Passwords**.

The **File Passwords** screen appears.

2. Click **Import Passwords**.

The **Import Passwords** window appears.

3. Browse and select the file to import.
- 



### Note

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

---

Deep Discovery Email Inspector checks the entries in the selected file to identify any invalid or duplicate passwords.

**4. Click **Import**.**

---


## **Smart Protection**

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

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

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

**TABLE 8-8. Smart Protection Sources**

| <b>BASIS OF COMPARISON</b> | <b>TREND MICRO SMART PROTECTION NETWORK</b>  | <b>SMART PROTECTION SERVER</b>  |
|----------------------------|--|---|
| Purpose                    | A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology | <p>Localizes the File and Web Reputation Services to the corporate network to optimize efficiency.</p> <p>The Smart Protection Server also provides the following:</p> <ul style="list-style-type: none"> <li>• Certified Safe Software Service</li> <li>• Community File Reputation</li> <li>• Web Inspection Service</li> <li>• Web Reputation Service</li> <li>• Predictive Machine Learning engine</li> <li>• Community Domain/IP Reputation Service</li> </ul> <hr/> <p> <b>Note</b></p> <p>The Dynamic URL Scanning service is only available on the Smart Protection Network.</p> |
| Administration             | Hosted and maintained by Trend Micro   | Installed and managed by Trend Micro product administrators   |
| Connection protocol        | HTTP   | HTTP and HTTPS  |

| BASIS OF COMPARISON | TREND MICRO SMART PROTECTION NETWORK   | SMART PROTECTION SERVER  |
|---------------------|--|--|
| Usage               | <p>Use if you do not plan to install Smart Protection Server</p> <p>To configure Smart Protection Network as source, see <a href="#">Configuring Smart Protection Settings on page 8-39</a>.</p> | <p>Use as primary source and the Smart Protection Network as an alternative source</p> <p>For guidelines on setting up Smart Protection Server and configuring it as source, see <a href="#">Setting Up Smart Protection Server on page 8-38</a> and <a href="#">Configuring Smart Protection Settings on page 8-39</a>.</p> |

## About Smart Protection Server

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

## Setting Up Smart Protection Server

### Procedure

1. Install Smart Protection Server on a VMware ESX/ESXi server.

For more information, see <http://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx>.

2. Configure Smart Protection Server settings from the Deep Discovery Email Inspector management console.

For more information, see *Configuring Smart Protection Settings on page 8-39*.

**Note**

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

---

## Configuring Smart Protection Settings

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Smart Protection**.
2. Select **Connect to Smart Protection Server for Web Reputation Services**.
3. Configure the Smart Protection Server.
  - a. Specify the Smart Protection Server IP address or fully qualified domain name.

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

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

- b.** Select **Connect using a proxy server** if proxy settings for Deep Discovery Email Inspector have been configured for use with Smart Protection Server connections.

**Note**

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

---

- c.** Specify the port number.
- 4.** Click **Test Connection** to verify that specified Smart Protection Server can connect to global services.

**Important**

Deep Discovery Email Inspector supports global services when connecting to Smart Protection Server version 3.0 Patch 2 or later.

---

- 5.** (Optional) Select **Connect to global services using Smart Protection Server** to configure Deep Discovery Email Inspector to query global Smart Protection services.
      - If your organization uses a CA certificate, select **Use certificate** and click **Browse** to select the certificate file; then, click **Import** to import the certificate file.
        - If your organization uses a Certificate Revocation List (CRL), select **Use CRL** and click **Browse** to select the CRL file; then, click **Import** to import the Certificate Revocation List file.
  - 6.** Click **Save**.
- 

## Smart Feedback

Deep Discovery Email Inspector integrates the new Trend Micro Feedback Engine. This engine sends protected threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Participation in Smart Feedback authorizes Trend Micro

to collect certain information from your network, which is kept in strict confidence.

Information collected by Smart Feedback:

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

## Enabling Smart Feedback

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Smart Feedback**.
  2. Select Smart Feedback settings.
    - Select **Enable Smart Feedback (recommended)** to send protected information to Trend Micro from your network.
    - Select **Send suspicious files to Trend Micro** to send suspicious files found as high-risk to Trend Micro for further investigation.

For details about detected risk levels, see [Virtual Analyzer Risk Levels on page 4-4](#).
  3. Click **Save**.
-

## YARA Rules

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

Deep Discovery Email Inspector supports a maximum of 5,000 enabled YARA rules regardless of the number of YARA rule files. On the top-right corner of the YARA rule table, the **Rules in use** field indicates the number of YARA rules currently enabled in the system.



### Important

After you register Deep Discovery Email Inspector to Deep Discovery Director, Deep Discovery Email Inspector automatically synchronizes YARA rule settings from Deep Discovery Director and overwrites existing YARA rule settings that you have configured.

The following table shows information about YARA rule files.

**TABLE 8-9. YARA Rules**

| FIELD            | DESCRIPTION   |
|------------------|---|
| File name        | Name of the YARA rule file.                                       |
| Risk level       | Risk level of the YARA rules.                                     |
| Rules            | Number of YARA rules contained in the YARA rule file.             |
| Files to analyze | File types to analyze using the YARA rules in the YARA rule file. |
| Last Updated     | Date and time the YARA rule file was last updated.                |
| Status           | Toggle to enable or disable the YARA rule file.                   |

## Creating a YARA Rule File

Deep Discovery Email Inspector supports YARA rules that follow version 3.10.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

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

<https://yara.readthedocs.io/en/v3.10.0/writingrules.html>

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

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


The following example shows a simple YARA rule:

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

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

**TABLE 8-10. YARA Rule Parts and Usage**

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

| PART              | USAGE  |
|-------------------|--|
| weight            | <p>Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met:</p> <ul style="list-style-type: none"> <li>• 1 to 9 = Low risk</li> <li>• 10 = High risk</li> </ul> <hr/> <div>  <b>Note</b><br/>           The weight value does not correspond to the risk level assigned by Deep Discovery Email Inspector.         </div> <hr/> |
| strings:          | Indicates that the "strings" section begins. Strings are the main means of detecting malware.  |
| \$a / \$b / \$c   | Strings used to detect malware. Must begin with a \$ character followed by one of more alphanumeric characters and underscores.  |
| condition:        | Indicates that the "condition" section begins. Conditions determine how your strings are used to detect malware.   |
| \$a or \$b or \$c | <p>Conditions are Boolean expressions that define the logic of the rule. They tell the condition under which a submitted object satisfies the rule or not. Conditions can range from the typical Boolean operators and, or and not, to relational operators &gt;=, &lt;=, &lt;, &gt;, == and !=. Arithmetic operators (+, -, *, \, %) and bitwise operators (&amp;,  , &lt;&lt;, &gt;&gt;, ~, ^) can be used on numerical expressions.</p>                     |

## Adding a YARA Rule File

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > YARA Rules**.
2. Click **Add** to add a YARA rule file.  
The **Add YARA Rule File** window appears.
3. In the new window that opens, configure the following:

- a. **Rule file:** Browse and select a YARA rule file to add.
  - b. **Risk level:** Select the detection risk level for the YARA rules in the file.
  - c. **Files to analyze:** Type or select file types that Virtual Analyzer processes specific to this YARA rule file.
4. Click **Add** when you have selected the YARA rule file to add and the file types to analyze.

Virtual Analyzer validates the YARA rule file before adding it. For details about creating valid YARA rule files, see [Creating a YARA Rule File on page 8-42](#).

---

## Editing a YARA Rule File

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > YARA Rules**.
2. Click a file name to edit a YARA rule file.  
The **Edit YARA Rule File** window appears.
3. Make changes to the settings.
4. Click **Save**.

---

## Deleting a YARA Rule File

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > YARA Rules**.
  2. Select one or several YARA rule files to remove.
  3. Click **Delete**.
-

## Exporting a YARA Rule File

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > YARA Rules**.
2. Select a YARA rule file to export.



#### Note

You can export only one YARA rule at a time.

---

3. Click **Export**.
- 

## Time-of-Click URL Protection

Deep Discovery Email Inspector provides Time-of-Click protection against malicious URLs in email messages. When this feature is enabled, Deep Discovery Email Inspector rewrites URLs in email messages for further analysis and displays the blocking or warning redirect pages on endpoints. Trend Micro Smart Protection Network (SPN) analyzes a rewritten URL every time the URL is clicked and applies specified actions based on the risk levels of the URLs.

## Configuring Time-of-Click Protection Settings

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Time-of-Click Protection**.
2. Select **Enable Time-of-Click Protection** to activate this feature and rewrite URLs that Virtual Analyzer considers safe and unrated URLs in email messages for further analysis.
3. (Optional) Select **Rewrite all safe URLs** to also rewrite URLs that Web Reputation Services (WRS) consider safe in email messages for further analysis.

4. Select an action for each URL rating.

| FIELD       | DESCRIPTION  |
|-------------|--|
| High risk   | <p>Select an action (<b>Allow</b>, <b>Warn</b>, or <b>Block</b>) to take on dangerous URLs. The default action is <b>Block</b>.</p> <p>High-risk URLs are verified to be fraudulent or known sources of threats.</p>   |
| Medium risk | <p>Select an action (<b>Allow</b>, <b>Warn</b>, or <b>Block</b>) to take on highly suspicious URLs. The default action is <b>Block</b>.</p> <p>Medium-risk URLs are suspected to be fraudulent or possible sources of threats.</p>   |
| Low risk    | <p>Select an action (<b>Allow</b>, <b>Warn</b>, or <b>Block</b>) to take on suspicious URLs. The default action is <b>Warn</b>.</p> <p>Low-risk URLs are associated with spam or possibly compromised.</p>   |
| Unrated     | <p>Select an action (<b>Allow</b>, <b>Warn</b>, or <b>Block</b>) to take on untested URLs. The default action is <b>Warn</b>.</p> <p>While Trend Micro actively tests URLs for safety, users may encounter unrated pages when visiting new or less popular web sites. Blocking access to unrated pages can improve safety but can also prevent access to safe pages.</p> |

5. (Optional) To configure redirect pages, select **Customize redirect pages** and configure the required settings.

- Click **Import** and **Export** to manage the template file.
- Click the Content tab for each risk level to display a preview of the redirect pages.

**Note**

You can use the following HTML tags in the Content area to customize redirect pages:

- `<a>`
- `<b>`
- `<i>`

---

**6. Click **Save**.**

---

## Business Email Compromise

Using Business Email Compromise (BEC) scams, an attacker gains access to a corporate email account and spoofs the owner's identity to initiate fraudulent wire transfers. The attacker typically uses the identity of a top-level executive to trick the target or targets into sending money into the attacker's account. Also known as Man-in-the-Email scams, BEC scams often target businesses that regularly send wire transfers to international clients and may involve the use of malware, social engineering, or both.

With the integrated Antispam Engine, Deep Discovery Email Inspector performs the following to effectively protect organizations against BEC scams:

- Scan email messages from specified high-profile users to block social engineering attacks
- Check sender and recipient domain information to prevent email message spoofing
- Bypass email messages from approved senders to enhance detection

### Adding a High-Profile User

Add high-profile user names to allow Deep Discovery Email Inspector to scan email messages for potential social engineering attacks.

High-profile users are top-level executives in your organization. For example, CEOs, CFOs, or managers.

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Business Email Compromise Protection**.
2. Under **High-Profile Users**, type the user name.



### Note

- You can type up to 30 UTF-8 encoded characters for family, given, and middle names. Do not use hash "#" or semi-colon ";" characters.
- Specifying complete user names is important. Deep Discovery Email Inspector performs both partial and complete matches on message display names.

For example, if you add a high-profile user name *John A. Smith*, Deep Discovery Email Inspector blocks forged email messages that use *John A Smith*, *John Smith*, or *Smith John* as the display name.

3. Click **Add**.
  - You can add up to 500 high-profile user names.
  - To delete a user name, select the entry and click **Delete**.

---

## Adding an Internal Domain

Add all internal domains you use in your organization to allow Deep Discovery Email Inspector to detect potential email message spoofing.

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Business Email Compromise Protection**.
2. Under **Internal Domains**, type a domain name (for example, `domain.com`).

You can specify up to 255 printable ASCII characters for the domain name. Do not use semi-colon ";" characters.

3. Click **Add**.

- You can add up to 500 domains.
  - To delete a domain, select the entry and click **Delete**.
- 

## Adding an Approved Sender

You can add the email addresses of senders that you trust to reduce false-positives and enhance Business Email Compromise (BEC) scam detections. Deep Discovery Email Inspector does not scan messages from approved sender for BEC scams.



**Note**

You can add up to 1000 senders that you trust to bypass BEC scam detection in Deep Discovery Email Inspector.

---

## Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Business Email Compromise Protection**.
2. Under **Approved Senders**, type a sender email address (up to 255 characters).
3. Click **Add**.

To remove an approved sender from the list, select the entry and click **Delete**.

---

## Cousin Domains

A cousin domain (or look-alike domain) is a domain that looks deceptively similar to a legitimate target domain, which is well-known or familiar to users. Cousin domains are often used in phishing attacks to steal sensitive or confidential information from users. Cousin domains are usually created by replacing one or more characters (for example, replacing the letter "l" with the number "1") or adding or removing an extra character in the domain

name. Without careful inspection of the email addresses, users may not notice the trick and think that an email message is sent from a legitimate domain being forged.

Using the advanced antispam engine, Deep Discovery Email Inspector can scan domains in email messages (from and replyto headers) based on the settings you configure to detect spam and phishing messages.

## Configuring Cousin Domain Settings

On the **Cousin Domains** screen, you can configure legitimate sender domains and the detection threshold setting that Deep Discovery Email Inspector uses to detect cousin domains in email messages.

---

### Procedure

1. Go to **Administration > Scanning / Analysis > Other Settings > Cousin Domains**.
2. Add one or more legitimate sender domains. Do the following:
  - a. Type a domain name (for example, `domain.com`).

You can specify up to 255 printable ASCII characters for the domain name. Do not use semi-colon ";" characters.
  - b. Click **Add**.
    - You can add up to 1000 domains.
    - To delete a domain, select the entry and click **Delete**.
3. Select a detection threshold.
  - **Aggressive**: This option provides the most number of detections based on fuzzy matches. This is the most rigorous level of spam and phishing detection.
  - **Normal**: This is the default and recommended setting. This option provides a moderate number of detections.
  - **Conservative**: This option provides the most accurate detections based on near-exact matches.

4. (Optional) Specify one or more domains that Deep Discovery Email Inspector excludes from scanning. Type a domain and press [Enter] to add an entry.
  5. Click **Save**.
- 

## Sender Filtering/Authentication Settings

With sender filtering and sender authentication, Deep Discovery Email Inspector filters and validate senders of incoming email messages to effectively block spam messages.

---

**Note**

Sender filtering and sender authentication settings take effect only when Deep Discovery Email Inspector is deployed in MTA mode.

---

The following table describes the settings that you can configure.

| SETTING          | DESCRIPTION  |
|------------------|--|
| Approved Senders | A list of trusted senders that bypass sender filtering and sender authentication settings in Deep Discovery Email Inspector  |
| Blocked Senders  | A list of senders that Deep Discovery Email Inspector blocks permanently or temporarily  |
| Email Reputation | <p>When deployed as an edge MTA, Deep Discovery Email Inspector filters connections from senders when establishing SMTP sessions based on the reputation of the sender IP addresses.</p> <p>When deployed as a non-edge MTA, Deep Discovery Email Inspector filters connections from senders of the last relay MTA based on the reputation of the sender IP addresses in the email message header.</p> |

| SETTING  | DESCRIPTION   |
|--|---|
| DHA protection                                   | <p>Prevents senders from using a directory harvest attack (DHA) to obtain user email addresses for spam message transmission based on one of the following information:</p> <ul style="list-style-type: none"> <li>• Sender IP address (when Deep Discovery Email Inspector is deployed as an edge MTA)</li> <li>• Sender IP address in the email message header (when Deep Discovery Email Inspector is deployed as a non-edge MTA)</li> </ul>                 |
| Bounce attack protection                         | <p>Blocks senders if the number of returned email messages reaches the specified threshold based on the following information:</p> <ul style="list-style-type: none"> <li>• Sender IP address (when Deep Discovery Email Inspector is deployed as an edge MTA)</li> <li>• Sender IP address in the email message header (when Deep Discovery Email Inspector is deployed as a non-edge MTA)</li> </ul>  |
| SMTP traffic throttling                          | Blocks messages from a sender based on the IP address or email address for a certain time when the number of connections or messages reaches the specified threshold  |
| Sender Policy Framework (SPF)                    | <p>A sender authentication feature that prevents spoofing and phishing by allowing only messages that are sent from authorized servers for a domain based on the following information:</p> <ul style="list-style-type: none"> <li>• Sender IP address (when Deep Discovery Email Inspector is deployed as an edge MTA)</li> <li>• Sender IP address in the email message header (when Deep Discovery Email Inspector is deployed as a non-edge MTA)</li> </ul> |
| DomainKeys Identified Mail (DKIM) authentication | A sender authentication feature that prevents spoofing and phishing by verifying signatures in incoming messages  |
| DomainKeys Identified Mail (DKIM) signatures     | A list of DKIM signatures that Deep Discovery Email Inspector adds to message headers in outgoing messages  |

| SETTING  | DESCRIPTION   |
|--|---|
| Domain-based Message Authentication, Reporting & Conformance (DMARC) | A sender authentication feature that verifies message senders for specified domains to prevent spoofing |

## Sender Filter Order of Evaluation

Before Deep Discovery Email Inspector applies scanning settings on messages, message sender email addresses and IP addresses first go through Approved Senders and Blocked Senders list filtering. Sender email addresses and IP addresses are evaluated until the first match is found.

- By default, Deep Discovery Email Inspector applies sender filtering and sender authentication settings in the following order:
  - For SMTP traffic throttling:
    - Approved Senders list (IP address)
    - Blocked Senders list (user-defined IP address)
    - SMTP traffic throttling (IP address)
    - Approved Senders list (email address)
    - Blocked Senders list (user-defined email address)
    - SMTP traffic throttling (email address)
  - For sender filtering (ERS, DHA, and Bounce Attack) and domain-based message authentication (SPF, DKIM, and DMARC):
    - Approved Senders list (IP address)
    - Blocked Senders list (user-defined IP address)
    - Approved Senders list (message envelop sender address)
    - Blocked Senders list (user-defined email address for message envelop sender address)

- Approved Senders list (message header FROM address)
  - Blocked Senders list (user-defined email address for message header FROM address)
  - Sender filtering (ERS , DHA, Bounce Attack)
  - Domain-based message authentication (SPF, DKIM, and DMARC)
- If a sender IP address or email address is not in the Approved Senders list and does not match user-defined entries in the Blocked Senders list, Deep Discovery Email Inspector applies sender filtering and sender authentication settings in the following order:
    - SMTP traffic throttling (IP address and email address)
    - Email Reputation Services (ERS)
    - Directory harvest attack (DHA) protection
    - Bounce attack protection
    - Sender Policy Framework (SPF)
    - DomainKeys Identified Mail (DKIM)
    - Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - If a sender IP address or email address is in the Approved Senders list, Deep Discovery Email Inspector does not apply user-defined entries in the Blocked Senders list, and sender filtering (ERS, DHA, and bounce attack) and sender authentication (SPF, DKIM, and DMARC) settings on messages from the sender.
  - If a sender IP address or email address matches a user-defined entry in the Blocked Senders list, Deep Discovery Email Inspector blocks messages from the sender without scanning.
  - When you enable both IP address-based and email address-based SMTP traffic throttling, Deep Discovery Email Inspector blocks messages from a sender if both conditions are met:

- The sender IP address is in the Blocked Senders list
- The sender email address is in the Approved Senders list

## SMTP Error Codes

When Deep Discovery Email Inspector blocks an email message based on Sender Filtering settings, Deep Discovery Email Inspector sends the following SMTP error codes to the upstream MTA.



### Note

Make sure that the upstream MTA can take the necessary pre-configured actions upon receiving these error codes. For example, creating an event log or sending notifications to senders.

| BLOCKING FEATURE   | SMTP ERROR CODE | MESSAGE   |
|--|-----------------|---|
| Sender Filtering/Authentication settings (DHA Protection, Bounce Attack Protection, SMTP Traffic Throttling, SPF, DKIM, DMARC) | 421             | Block temporarily (Sender Filtering/Authentication)           |
|  | 521             | Block permanently (Sender Filtering/Authentication)           |
| Email Reputation Service   | 450             | Temporary denial of connection (450) for Zombie matches (ERS) |
|  | 550             | Permanent denial of connection (550) for RBL+ matches (ERS)   |

## Configuring Email Reputation Services

Deep Discovery Email Inspector uses Email Reputation Services (ERS) technology to maximize spam protection. ERS technology allows Deep Discovery Email Inspector to determine spam based on the reputation of the originating Mail Transfer Agent (MTA). With ERS enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been blocked as a known spam vector.

**Note**

For Email Reputation Services to function properly, all address translation on inbound SMTP traffic must occur after traffic passes through Deep Discovery Email Inspector. If NAT or PAT takes place before the inbound SMTP traffic reaches Deep Discovery Email Inspector, Deep Discovery Email Inspector always treats the local address as the originating MTA. ERS only blocks connections from suspect MTA public IP addresses, not private or local addresses.

---

**Procedure**

1. Go to **Administration > Sender Filtering/Authentication > Email Reputation**.
2. Select **Enable Email Reputation Services**.
3. Under **Scan Settings**, select **Match message header FROM address** to scan the message envelop sender address and the message header FROM address. A match is found if either address is matched.

By default, Deep Discovery Email Inspector scans the envelop sender address only.

4. Visit the Email reputation management console at <https://ers.trendmicro.com/> to access global spam information, view statistics, manage Email reputation settings, and perform service settings.

---

**Approved Senders List**

The Approved Senders list contains trusted senders that bypass sender filtering and sender authentication settings in Deep Discovery Email Inspector.

**Note**

- Deep Discovery Email Inspector matches senders against the Approved Senders and Blocked Senders lists only in MTA mode.
- Deep Discovery Email Inspector still checks incoming SMTP traffic from approved senders using Trend Micro Email Reputation Services (ERS) without blocking the traffic.
- For information on how Deep Discovery Email Inspector filters senders based on the Approved Senders and Blocked Senders list, see [Sender Filter Order of Evaluation on page 8-54](#).

The following table describes the tasks that you can perform on the **Approved Senders** list.

| TASK           | DESCRIPTION   |
|----------------|---|
| Add a sender   | Click <b>Add</b> to add a sender to the list.<br>For more information, see <a href="#">Adding Approved Senders on page 8-59</a> . |
| Delete senders | Select one or more senders and click <b>Delete</b> .  |
| Import senders | Click <b>Import</b> .<br>For more information, see <a href="#">Importing Approved Senders on page 8-61</a> .                      |

The following table describes the Approved Senders list.

| HEADER               | DESCRIPTION   |
|----------------------|---|
| IP Address           | View the sender IP address or resolved domain IP address that bypasses sender filtering and sender authentication settings in Deep Discovery Email Inspector. |
| Domain/Email Address | View the sender domain or email address.  |
| Resource Record      | View the type of resource record for a sender domain.   |
| Description          | View the description for the entry.   |

| HEADER       | DESCRIPTION                           |
|--------------|---------------------------------------|
| Last Updated | View when the entry was last updated. |

## Adding Approved Senders

You can add one or more senders to the Approved Senders list. Deep Discovery Email Inspector does not apply sender filtering and sender authentication settings on messages from approved senders.



### Important

- Deep Discovery Email Inspector does not apply sender filtering and sender authentication settings on messages with IP addresses, domain-resolved IP addresses, or email addresses that match an entry in the Approved Senders list.
- For SMTP traffic throttling, Deep Discovery Email Inspector checks the senders against the Approved Senders and Blocked Senders lists in the following order:
  - Approved Senders list (IP address)
  - Blocked Senders list (user-defined IP address)
  - SMTP traffic throttling (IP address)
  - Approved Senders list (email address)
  - Blocked Senders list (user-defined email address)
  - SMTP traffic throttling (email address)



### Note

You can add up to 2048 entries to the list.

---

## Procedure

1. Go to **Administration > Sender Filtering/Authentication > Approved Senders**.

The **Approved Senders** screen appears.

2. Click **Add**.

The **Add Approved Senders** screen appears.

3. Select and configure one of the following:

- **Domain:** Select this option to specify the domain of the senders. You can select one or more **Resource record** types.



### Note

Deep Discovery Email Inspector regularly resolves the specified domain, and adds the resolved IP addresses in an entry in the Approved Senders list or updates the resolved IP addresses in the entry.

- **IP address or subnet:** Select this option to specify the IPv4/IPv6 address of a sender or the subnet of multiple senders.
- **Email address:** Select this option to specify the email address of the sender.



### Tip

Deep Discovery Email Inspector support email domains. For example, \*@\* indicates all email addresses .

4. Type a description.
  5. Click **Save**.
-

## Importing Approved Senders

---

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > Approved Senders**.

The **Approved Senders** screen appears.

2. Click **Import**.
  3. Click **Select** to locate the file to import.
  4. Select one of the options:
    - Merge with current list: Add the imported entries into the current list.
    - Overwrite current list: Overwrite all existing entries with the entries in the imported file.
  5. Click **Import**.
- 

## Blocked Senders List

Deep Discovery Email Inspector blocks messages from sender IP addresses, resolved IP address, or email addresses in the Blocked Senders list.

A sender is added to the Blocked Senders list in one of the following ways:


- Automatically when a message from the sender is detected based on the sender filtering (DHA protection, bounce attack protection, and SMTP traffic throttling).
- Manually by the administrator

**Note**

- Deep Discovery Email Inspector matches senders against the Approved Senders and Blocked Senders lists only in MTA mode.
- Deep Discovery Email Inspector automatically removes a sender from the list after the blocking expiry time is reached.
- The time period filter setting is not applicable for user-defined entries when you select **User defined** or **All** from the **Rule** drop-down list
- For information on how Deep Discovery Email Inspector filters senders based on the Approved Senders and Blocked Senders list, see [Sender Filter Order of Evaluation on page 8-54](#).

The following table describes the tasks that you can perform on the **Blocked Senders** list.

| TASK                          | DESCRIPTION  |
|-------------------------------|--|
| Filter the list               | Filter the list based on the selected rule type and time period.   |
| Search for a sender           | Type a keyword to search for a sender.   |
| Add a sender                  | Click <b>Add</b> to add a sender to the list.<br>For more information, see <a href="#">Adding Blocked Senders on page 8-64</a> . |
| Delete senders                | Select one or more senders and click <b>Delete</b> .   |
| Import senders                | Click <b>Import</b> .<br>For more information, see <a href="#">Importing Blocked Senders on page 8-65</a> .                      |
| Export All User-defined Rules | Click <b>Export All User-defined Rules</b> to export all entries that are manually added to the list.                            |

| TASK                                      | DESCRIPTION   |
|---|---|
| Export Selected User-defined Rules        | <p>Select one or more user-defined entries and click <b>Export Selected User-defined Rules</b>.</p> <hr/> <p> <b>Tip</b><br/>Select <b>User defined</b> from the <b>Rule</b> drop-down list to filter the entries.</p> <hr/> |
| Move senders to the Approved Senders list | <p>Select one or more senders and click <b>Move to Approved Senders</b>.</p> <p>For more information, see <a href="#">Approved Senders List on page 8-57</a>.</p>   |

The following table describes the Blocked Senders list.

| HEADER               | DESCRIPTION  |
|----------------------|--|
| IP Address           | View the sender IP address resolved domain IP address for the sender that Deep Discovery Email Inspector blocks.   |
| Domain/Email Address | View the sender domain or email address.   |
| Rule                 | View the name of the sender filtering/authentication rule that is matched.   |
| Resource Record      | View the type of resource record for a sender domain.  |
| Action               | View whether Deep Discovery Email Inspector blocks the sender address temporarily or permanently.  |
| Expiration           | <p>View when Deep Discovery Email Inspector stops temporarily block senders.</p> <p>When the temporary blocking action expires, Deep Discovery Email Inspector removes a sender from the list.</p> |
| Description          | View the description for the entry.  |
| Last Updated         | View when the entry was last updated.  |

## Adding Blocked Senders

---



### Important

For SMTP traffic throttling, Deep Discovery Email Inspector checks the senders against the Approved Senders and Blocked Senders lists in the following order:

- Approved Senders list (IP address)
  - Blocked Senders list (user-defined IP address)
  - SMTP traffic throttling (IP address)
  - Approved Senders list (email address)
  - Blocked Senders list (user-defined email address)
  - SMTP traffic throttling (email address)
- 



### Note

You can add up to 2048 entries to the list.

---

## Procedure

1. Go to **Administration > Sender Filtering/Authentication > Blocked Senders**.

The **Blocked Senders** screen appears.

2. Click **Add**.

The **Add Blocked Senders** screen appears.

3. Select and configure one of the following:

- **Domain:** Select this option to specify the domain of the senders. You can select one or more **Resource record** types.

**Note**

Deep Discovery Email Inspector regularly resolves the specified domain, and adds the resolved IP addresses as a user-defined entry in the Blocked Senders list or updates the resolved IP addresses in the entry.

- **IP address or subnet:** Select this option to specify the IPv4/IPv6 address of a sender or the subnet of multiple senders.
- **Email address:** Select this option to specify the email address of the sender.

**Tip**

Deep Discovery Email Inspector support email domains. For example, \*@\* indicates all email addresses .

4. Type a description.
5. Click **Save**.

## Importing Blocked Senders

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > Blocked Senders**.

The **Blocked Senders** screen appears.

2. Click **Import**.
3. Click **Select** to locate the file to import.
4. Select one of the options:
  - Merge with current list: Add the imported entries into the current list.

- Overwrite current list: Overwrite all existing entries with the entries in the imported file.

5. Click **Import**.

---

## Configuring DHA Protection Settings

Configure DHA protection settings to prevent senders from using a directory harvest attack (DHA) to obtain user email addresses for spam message transmission.



**Note**

- Before you enable this feature, configure Microsoft Active Directory settings.


For more information, see [Configuring an LDAP Server on page 8-166](#).

- When SMTP traffic volume is extremely high, Deep Discovery Email Inspector might not precisely block email messages based on the configuration due to the time delay between rule trigger and activation.
- 

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > DHA Protection**.
2. Select **Enable directory harvest attack protection**.
3. Configure the following settings.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Monitoring duration | Select the number of hours that Deep Discovery Email Inspector monitors email traffic to see if the percentage of messages signaling a DHA threat exceeds the specified threshold. |
| Rate                | Type the maximum percentage of messages with detected threats (the numerator).   |

| FIELD                   | DESCRIPTION   |
|-------------------------|---|
| Total messages          | Type the total number of messages (received from the same sender) that Deep Discovery Email Inspector uses to calculate the threshold percentage (the denominator).   |
| Recipient threshold     | Type the maximum number of recipients allowed.  |
| Non-existing recipients | Type the maximum number of non-existent recipients allowed for the threshold value. DHA often include randomly generated email addresses in the receiver list.  |
| Action                  | <p>Select one of the following block actions:</p> <ul style="list-style-type: none"> <li>• <b>Block temporarily:</b> Blocks messages from the IP address temporarily and allow the upstream MTA to try again after the block duration ends</li> <li>• <b>Block permanently:</b> Never allow another message from the IP address and do not allow the upstream MTA to try again</li> </ul> |
| Blocking duration       | <p>If you select the <b>Block temporarily</b> action, select the number of hours to block.</p> <hr/> <div>  <b>Note</b><br/>           After blocking a sender for the specified time, Deep Discovery Email Inspector removes the sender from the Blocked Senders list.         </div> <hr/>             |

For example, if you configure the following settings:

- Monitoring duration: 1 hour
- Rate: 20
- Total messages: 100
- Recipient threshold: 10
- Non-existing recipients: 5

During each one-hour period that DHA protection is active, Deep Discovery Email Inspector starts blocking senders when it receives more than 20% of the messages that were sent to more than 10 recipients

(with more than five of the recipients not in your organization) and the total number of messages exceeds 100.

4. Click **Save**.

To use the default settings, click **Restore Default** to discard your configuration.

---

## Configuring Bounce Attack Protection Settings

You can configure bounce attack protection settings to block senders if the number of returned email messages reaches the specified threshold.

---




### Note

- Before you enable this feature, configure Microsoft Active Directory settings.  
  
For more information, see [Configuring an LDAP Server on page 8-166](#).
  - Deep Discovery Email Inspector considers an email message with non-existing recipient as a bounce attack attempt.
  - When SMTP traffic volume is extremely high, Deep Discovery Email Inspector might not precisely block email messages based on the configuration due to the time delay between rule trigger and activation.
- 

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > Bounce Attack Protection**.
2. Select **Enable bounce attack protection**.
3. Configure the following settings.

| FIELD               | DESCRIPTION   |
|---------------------|---|
| Monitoring duration | Select the number of hours that Deep Discovery Email Inspector monitors email traffic to see if the percentage of messages signaling a bounce attack exceeds the specified threshold.   |
| Rate                | Type the maximum percentage of messages with detected threats (the numerator).  |
| Total messages      | Type the total number of messages (received from the same sender) that Deep Discovery Email Inspector uses to calculate the threshold percentage (the denominator).   |
| Action              | <p>Select one of the following block actions:</p> <ul style="list-style-type: none"> <li>• <b>Block temporarily:</b> Blocks messages from the IP address temporarily and allow the upstream MTA to try again after the block duration ends</li> <li>• <b>Block permanently:</b> Never allow another message from the IP address and do not allow the upstream MTA to try again</li> </ul> |
| Blocking duration   | <p>If you select the <b>Block temporarily</b> action, select the number of hours to block.</p> <hr/> <div>  <b>Note</b><br/>           After blocking a sender for the specified time, Deep Discovery Email Inspector removes the sender from the Blocked Senders list.         </div> <hr/>             |

For example, if you configure the following settings:

- Monitoring duration: 1 hour
- Rate: 20
- Total messages: 100

During each one-hour period that blocking for bounced mail is active, Deep Discovery Email Inspector starts blocking senders when more than 20% of the messages it receives are bounced messages and the total number of messages exceeds 100.

#### 4. Click **Save**.

To use the default settings, click **Restore Default** to discard your configuration.

---

## Configuring SMTP Traffic Throttling Settings

Configure SMTP traffic throttling settings to block messages from a single IP address or sender email address for a certain time when the number of connections or messages reaches the specified threshold.

---



### Note

- Disable SMTP traffic throttling when you deploy Deep Discovery Email Inspector as a non-edge MTA in your network.
  - When SMTP traffic volume is extremely high, Deep Discovery Email Inspector might not precisely block email messages based on the configuration due to the time delay between rule trigger and activation.
  - For information on how Deep Discovery Email Inspector blocks messages based on the Approved Senders and Blocked Senders lists, see [Sender Filter Order of Evaluation on page 8-54](#).
- 


## Procedure

1. Go to **Administration > Sender Filtering/Authentication > SMTP Traffic Throttling**.
2. Select one or both of the following options:
  - **Enable SMTP traffic throttling based on sender IP addresses:**  
Monitors traffic based on sender IP addresses
  - **Enable SMTP traffic throttling based on sender email addresses:**  
Monitors traffic based on sender email addresses

**Note**

If you enable SMTP traffic throttling based on email addresses, Deep Discovery Email Inspector does not apply SMTP traffic throttling settings on traffic from sender email addresses in the Approved Senders list.

### 3. Configure the following settings.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Maximum connections | Type the maximum number of connections allowed for a single IP address.  |
| Maximum messages    | Type the maximum number of messages allowed from a single IP address or email address.   |
| Blocking duration   | Select the number of hours to block.<br><br><hr/> <div>  <b>Note</b><br/>           After blocking a sender for the specified time, Deep Discovery Email Inspector removes the sender from the Blocked Senders list.         </div> <hr/> |

### 4. Click **Save**.

To use the default settings, click **Restore Default** to discard your configuration.

## Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an email validation system that detects spoofing and phishing by verifying servers that are authorized to send email messages for a domain. Using SPF, Deep Discovery Email Inspector can verify the "envelop from" addresses in email messages against a list of authorized sending IP addresses and determine if an email message has been forged.

SPF requires the owner of a domain to publish the email sending policy (for example, which email servers are used to send email messages from that domain) in an SPF record in the Domain Name System (DNS). When Deep Discovery Email Inspector receives an email message claiming to come from that domain, Deep Discovery Email Inspector checks the SPF records to verify whether the email message complies with the domain's stated policy. For example, if the message comes from an unknown server, the email message can be considered as fake.

Evaluation of an SPF record can return any of the following results.

| RESULT    | DESCRIPTION   |
|-----------|---|
| Pass      | The SPF record designates the host to be allowed to send.                                 |
| Fail      | The SPF record has designated the host as not being allowed to send.                      |
| SoftFail  | The SPF record has designated the host as not being allowed to send but is in transition. |
| Neutral   | The SPF record specifies explicitly that nothing can be said about validity.              |
| None      | The domain does not have an SPF record or the SPF record does not evaluate to a result.   |
| PermError | A permanent error has occurred (for example, badly formatted SPF record).                 |
| TempError | A transient error has occurred.   |

## Configuring SPF Settings

Configure Sender Policy Framework (SPF) settings to allow Deep Discovery Email Inspector to determine whether a sender is permitted to send email messages for a domain, before delivering the email messages to the intended recipients.

**Note**

Deep Discovery Email Inspector is unable to perform HELO/EHLO identification if it is deployed as a non-edge MTA.

---

---

## Procedure

1. Go to **Administration > Sender Filtering/Authentication > SPF**.
2. Select **Enable Sender Policy Framework (SPF)**.
3. For **HELO/EHLO identity**, select **Enabled** to check the sender information in HELO/EHLO commands; otherwise, select **Disabled**.
4. To add verification result into the message header, select **Insert X-Header into email messages**.
5. Specify the sender domains to verify. Select **All** to perform SPF record checking for messages from all sender domains; otherwise, select **Specify sender domains** and complete the following steps to add sender domains to the verification list.
  - a. Type a domain.
  - b. Click **Add**.



### Note

- Enabling SPF validation for all domains may affect system performance.
- To remove a sender domain from the list, select the entry and click **Delete**.

- 
6. Specify the action to perform based on the verification result.
    - **Bypass**: Select this option to allow Deep Discovery Email Inspector to continue processing of the message.
    - **Block temporarily**: Select this option to temporarily block the message. The sender can send the same message to Deep Discovery Email Inspector to perform the verification again.
    - **Block permanently**: Select this option to permanently block the message. When a new message is received from the sender, Deep Discovery Email Inspector performs the verification again.

## 7. Click **Save**.

---

### **DomainKeys Identified Mail (DKIM)**

DomainKeys Identified Mail (DKIM) is an email validation system that detects email spoofing by validating a domain name identity associated with a message through cryptographic authentication. In addition, DKIM is used to ensure the integrity of incoming messages or ensure that a message has not been tampered with in transit.

To ensure the validity and integrity of email messages, DKIM uses a public and private key pair system. A public and private key pair is created for the sending domain. The private key is stored securely on the mail server and used to sign outgoing messages. The public key is stored and published in the Domain Name System (DNS). When an email message is sent, the mail server uses the private key to digitally sign it, which is a part of the message header. When the email message is received, the DKIM signature can be verified against the public key on the domain's DNS.

Deep Discovery Email Inspector implements DKIM authentication only in the following scenarios:

- Verifies DKIM signatures for incoming messages from specified sender domains or from all senders.
- Adds DKIM signatures to outgoing message headers to prevent spoofing only when the value of the “From” field in the message header is the same as the MAIL FROM address (envelope sender).

### **Configuring DKIM Authentication Settings**

Deep Discovery Email Inspector verifies DomainKeys Identified Mail (DKIM) signatures in incoming email messages and applies actions on messages that fail to pass signature verification. If a message's DKIM signature passes verification, the message will continue to the next step in the message delivery process.

---

## Procedure

1. Go to **Administration > Sender Filtering/Authentication > DKIM Authentication**.
2. Select **Enable DomainKeys Identified Mail (DKIM) authentication**.
3. To add verification result into the message header, select **Insert X-Header into email messages**.
4. Select the maximum number of signatures to verify in a message.

**Note**

- If a message contains more than the maximum number of signatures you select, Deep Discovery Email Inspector terminates the DKIM authentication process for the message.
- Selecting a larger number of signatures to verify may require more processing load.

- 
5. Specify the sender domains to verify. Select **All** to verify DKIM signatures in messages from all sender domains; otherwise, select **Specify sender domains** and complete the following steps to add sender domains to the verification list.
    - a. Type a domain.
    - b. Click **Add**.

**Note**

To remove a sender domain from the list, select the entry and click **Delete**.

- 
6. Specify the action to perform based on the verification result.
    - **Bypass**: Select this option to allow Deep Discovery Email Inspector to continue processing of the message.

- **Block temporarily:** Select this option to temporarily block the message. The sender can send the same message to Deep Discovery Email Inspector to perform the verification again.
- **Block permanently:** Select this option to permanently block the message. When a new message is received from the sender, Deep Discovery Email Inspector performs the verification again.

7. Click **Save**.

---

## DKIM Signatures

You can configure Deep Discovery Email Inspector to add a digital signature to outgoing message headers to prevent spoofing. Recipients can verify that the email messages from a specific domain are authorized by the domain's administrator and that the messages, including attachments, have not been modified during transport.



### Important

If you configure Deep Discovery Email Inspector to sign an incoming message that already contains digital signatures from other email services (for example, Gmail) or MTAs, Deep Discovery Email Inspector removes all existing signatures from the message before adding the new signature and sending the message.

---

On the management console, you can add or delete DKIM signatures and import or export DKIM signature files.

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

| TASK                 | DESCRIPTION   |
|----------------------|---|
| Add a DKIM signature | Configure DKIM signature settings to sign outgoing messages from a domain.<br><br>For more information, see <a href="#">Configuring a DKIM Signature on page 8-77</a> . |

| TASK                               | DESCRIPTION   |
|------------------------------------|---|
| Edit a DKIM signature              | Click a domain to edit the settings.  |
| Delete a DKIM signature            | Select an entry and click <b>Delete</b> to remove it from the list.   |
| Import a list of DKIM signatures   | You can import a list of DKIM signatures from another Deep Discovery Email Inspector appliance.<br><br>For more information, see <a href="#">Importing DKIM Signatures on page 8-79</a> .                         |
| Export the list of DKIM signatures | Click <b>Export</b> to save the list of DKIM signatures to a file.<br><br>You can use the exported file to replicate the same settings across multiple Deep Discovery Email Inspector appliances on your network. |


## Configuring a DKIM Signature

You can add or edit a DKIM signature that Deep Discovery Email Inspector uses to all outgoing messages from a specific domain.

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > DKIM Signatures**.
2. Do one of the following:
  - Click **Add** to add a new signature.
  - Click a domain to edit the signature.
3. Select **Enable DKIM signature**.
4. Configure the general settings.

| FIELD  | DESCRIPTION  |
|--------|--|
| Domain | Type the domain where messages are sent. For example, domain.com or *.domain.com |
| SDID   | Type the signing domain identifier. For example, domain.com.                     |

| FIELD           | DESCRIPTION   |
|-----------------|---|
| Headers to sign | Select one or more headers to sign, or add a custom header.   |
| Private key     | <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Import existing key:</b> Select this option and click <b>Select</b> to locate a private key file to import.</li> <li>• <b>Generate:</b> Select this option and select a key length have Deep Discovery Email Inspector create a private key.</li> </ul> <hr/> <div>  <b>Note</b> </div> <p>After saving the settings, use the generated DNS TXT record name and DNS TXT record value to publish the key pair to your DNS server.</p> <hr/> |

## 5. (Optional) Configure the advanced settings.

| FIELD                   | DESCRIPTION  |
|-------------------------|--|
| Header canonicalization | <p>Select a cononicalization algorithm:</p> <ul style="list-style-type: none"> <li>• <b>Relaxed:</b> Select this option to allow common modifications such as whitespace replacement or header field line rewrapping.</li> <li>• <b>Simple:</b> Select this option to allow no modifications in the header.</li> </ul> |
| Body canonicalization   | <p>Select a cononicalization algorithm:</p> <ul style="list-style-type: none"> <li>• <b>Relaxed:</b> Select this option to allow common modifications such as whitespace replacement.</li> <li>• <b>Simple:</b> Select this option to allow no modifications in the body.</li> </ul>                                   |
| Signature expiration    | Type the number of days that the signature will be valid.  |
| Body length             | Type the number of bytes allowed for the email body.   |
| AUID                    | Type the Agent or User Identifier on behalf of which SDID is taking responsibility.  |

| FIELD                 | DESCRIPTION   |
|-----------------------|---|
| Sub-domain exceptions | Type a sub-domain to be excluded from DKIM signing and press ENTER. |

6. Click **Save**.

**Note**

If you specify Deep Discovery Email Inspector to create a private key, use the generated DNS TXT record name and DNS TXT record value to publish the key pair to your DNS server.

## Importing DKIM Signatures

You can import a list of DKIM signatures from another Deep Discovery Email Inspector appliance.

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > DKIM Signatures**.
2. Click **Import**.  
The **Import DKIM Signatures** screen appears.
3. Click **Select** to locate the file containing the list of DKIM signatures.
4. Specify the password.
5. Click **Import**.

## Domain-based Message Authentication, Reporting & Conformance (DMARC)

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system designed to detect and prevent email spoofing. DMARC is intended to combat certain techniques often used in phishing and email spam, such as email messages with forged sender

addresses that appear to originate from legitimate organizations. DMARC provides a way to authenticate email messages for specific domains, send feedback to senders, and conform to a published policy.

DMARC is designed to fit into the existing inbound email authentication process of Deep Discovery Email Inspector. DMARC helps email recipients to determine if the purported message aligns with what the recipient knows about the sender. If not, DMARC includes guidance on how to handle the non-aligned messages.

DMARC requires the following:

- A message that passes the SPF check
- A message that passes the DKIM authentication check
- Alignment of identifier domains

Identifier alignment requires that a domain authenticated by SPF and DKIM is the same as the message header domain or parent domain.

By configuring DMARC settings, Deep Discovery Email Inspector allows you to specify actions to take on messages and add enforced peers to make sure email messages from certain sender domains always pass DMARC authentication.

## Configuring DMARC Settings

Use the **DMARC** screen to configure DMARC settings for certain domains and specify the actions based on the DMARC authentication results.

---

### Procedure

1. Go to **Administration > Sender Filtering/Authentication > DMARC**.
2. Select **Enable Domain-based Message Authentication, Reporting & Conformance (DMARC)**.
3. To add verification result into the message header, select **Insert X-Header into email messages**.

4. (Optional) Select **Send daily reports to senders** and configure the following settings to send aggregated reports of unsuccessful authentications to the senders on a daily basis.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Organization name   | Type the name or domain of the sending organization.                                 |
| Email address       | Type the email address that Deep Discovery Email Inspector uses to send the reports. |
| Contact information | Type the contact information (for example, phone number or URL).                     |

5. Specify the sender domains to verify. Select **All** to check messages from all sender domains; otherwise, select **Specify sender domains** and complete the following steps to add sender domains to the verification list.
- Type a domain (with or without wildcard). For example, domain.com or \*.domain.com.
  - Click **Add**.



#### Note

To remove a sender domain from the list, select the entry and click **Delete**.

6. Specify the action to perform based on the verification result.
- **Bypass:** Select this option to allow Deep Discovery Email Inspector to continue processing of the message.
  - **Block temporarily:** Select this option to temporarily block the message. The sender can send the same message to Deep Discovery Email Inspector to perform the verification again.
  - **Block permanently:** Select this option to permanently block the message. When a new message is received from the sender, Deep Discovery Email Inspector performs the verification again.

## 7. Click **Save**.

---

# End-User Quarantine

Deep Discovery Email Inspector includes the End-User Quarantine (EUQ) feature to improve spam management. Messages that are determined to be spam are quarantined and are available for users to review, delete, release, or approve for delivery. You can configure Deep Discovery Email Inspector to automatically send EUQ digest notifications with inline action links. With the web-based EUQ console, users can manage the spam quarantine of their personal accounts and of distribution lists that they belong to and add senders to the Approved Senders list.

For quarantine storage maintenance, you can manually remove data or configure automatic data purge thresholds.

For more information, see [Configuring Storage Maintenance on page 8-224](#).



### Note

When Deep Discovery Email Inspector is registered to Deep Discovery Director 5.0 (or later), Deep Discovery Director provides central management of End-User Quarantine settings. After registration is successful, Deep Discovery Email Inspector performs the following actions:

- Obtains EUQ settings from Deep Discovery Director and prevents manual configuration of EUQ settings on the management console
  - Stops sending EUQ digests
  - Disables EUQ console access
- 

## Configuring User Quarantine Access Settings

You can configure Deep Discovery Email Inspector to allow users to access the EUQ console and manage quarantined messages.

**Note**

When Deep Discovery Email Inspector is registered to Deep Discovery Director 5.0 (or later), Deep Discovery Director provides central management of End-User Quarantine settings. After registration is successful, Deep Discovery Email Inspector performs the following actions:

---

**Procedure**

1. Go to **Administration > End-User Quarantine**.
2. Click the **User Quarantine Access** tab.
3. Select **Enable EUQ console access**.
4. Select an authentication method for EUQ console access.
  - **LDAP**: Select this option to authenticate users based on their LDAP account credentials for EUQ console access. When you select this option, you can specify the following settings:
    - Select **Enable distribution list EUQ management** to allow users to manage the EUQ of distribution lists that they belong to.
    - Select **Allow only users in selected groups to access the EUQ console** to enable EUQ console access for selected LDAP groups.

You can type a keyword in the text box and click **Query** to search for user groups. Click a group name in the **Available Groups** list to add to the **Selected Groups** list.

---

**Tip**

To remove a group, click the group name in the **Selected Groups** list.

---

**Note**

Configure LDAP integration settings before using an LDAP server for user authentication.

For more information, see [Configuring an LDAP Server on page 8-166](#).

---

- **SAML:** Select this option to authenticate users based on SAML single sign-on account credentials from an identity provider.

To have Deep Discovery Email Inspector send EUQ digest notifications to only users in selected user groups, select **Send EUQ digest notifications to only users in the selected LDAP groups**, and add one or more user groups to the Selected Groups list.

- **SMTP:** Select this option to authenticate users based on their email address account credentials for EUQ console access.

Click + **Add** to add an SMTP server.

For more information, see [Adding an SMTP Server for EUQ Authentication on page 8-85](#).

5. Under **Advanced Settings**, configure the following settings:

- From the **Maximum approved senders per user** drop-down list, select the maximum number of approved sender email address that users can add on the EUQ console.
- Select **Deliver released messages directly without reprocessing** to allow users to release quarantined messages directly to recipients without scanning.

**Note**

If you do not select this option, users can still release quarantined messages by clicking inline action links in EUQ digest notifications or on the EUQ console. However, Deep Discovery Email Inspector scans these messages before delivery. Depending on the scanning results, Deep Discovery Email Inspector may quarantine these messages again.

---

6. Click **Save**.

After you select the **Enable EUQ console access** option, you can click the URL or send the URL to users to access the EUQ console.

For more information, see [Accessing the End-User Quarantine Console on page 8-89](#).

---

## Adding an SMTP Server for EUQ Authentication

On the **End-User Quarantine** screen, you can add one or more SMTP servers for EUQ authentication.

---

### Procedure

1. Go to **Administration > End-User Quarantine**.

The **End-User Quarantine** screen appears.

2. Select **Use SMTP server for EUQ authentication**.

3. Click **+ Add**.

The **Add SMTP Server** screen appears.

4. Configure the SMTP server settings.

| FIELD             | DESCRIPTION  |
|-------------------|--|
| Domain            | Type the domain name to use for EUQ console authentication.<br>You can use an asterisk character (*) in a domain name. |
| Server address    | Type the server IP address or FQDN.  |
| Port              | Type the server port.  |
| Encryption method | Select a data encryption method ( <b>None</b> , <b>StartTLS</b> , or <b>SSL/TLS</b> ) from the drop-down list.         |

5. Click **Add**.

---

## EUQ Digest

An EUQ digest is a notification that Deep Discovery Email Inspector sends to inform users about email messages that were detected as spam and temporarily stored in the EUQ.

**Note**

- When Deep Discovery Email Inspector is registered to Deep Discovery Director 5.0 (or later), Deep Discovery Director provides central management of End-User Quarantine settings. After registration is successful, Deep Discovery Email Inspector performs the following actions:
  - Deep Discovery Email Inspector sends EUQ digests only if there are new quarantined messages since the last digest.
  - If Active Directory authentication is enabled, Deep Discovery Email Inspector does not send EUQ digests to user groups (or distribution lists).
  - If SMTP authentication is enabled and a detected message is sent to a distribution list, Deep Discovery Email Inspector sends EUQ digests to the distribution list.
- 

An EUQ digest provides the following information:

- Total spam message count: Total number of new email messages in the EUQ since the last notification
- New spam message size: Size of the new email messages in the EUQ since the last notification
- Message list: Summary of email messages detected as spam.
  - Sender: The sender email address
  - Subject: The email subject
  - Size: The message size, including attachments
  - Received: The time the message was received

- **Actions:** Links that users can click to apply actions to quarantine messages or to add sender email address to the approved list

**Note**

Inline action links display only if you enable this feature on the **EUQ Digest** screen.

---

## Inline Action Links

You can configure Deep Discovery Email Inspector to include inline action links in EUQ digest notifications. Users can click the links in EUQ digest notifications to manage quarantined messages without having to access the EUQ console.

Inline action links allows users to perform the following actions on quarantined messages:

- **Delete:** Deletes the message and the associated attachments
- **Release:** Releases the message directly from the quarantine.
- **Release and add to Approved Senders list:** Releases the message directly from quarantine and adds the sender email address to the Approved Senders list.

**Important**

If you select the **Deliver released messages directly without scanning** option on the **User Quarantine Access** screen, Deep Discovery Email Inspector delivers released messages to recipients without scanning.

For more information, see [Configuring User Quarantine Access Settings on page 8-82](#).

---

## Configuring EUQ Digest Settings

You can configure Deep Discovery Email Inspector to send EUQ digests to notify users of new messages that are detected as spam.

---

## Procedure

1. **Administration > End-User Quarantine.**
2. Click the **EUQ Digest** tab.
3. Select **Enable EUQ digest notifications.**
4. From the **Notification frequency** drop-down list, select the number of hours Deep Discovery Email Inspector waits before sending an EUQ digest notification.
5. Select **Enable inline action** to allow users to apply actions from the EUQ digest.
6. Configure the settings for the digest notification template.

| FIELD   | DESCRIPTION  |
|---------|--|
| Subject | Type the subject for the notification email message.   |
| Content | <p>Type the content for the notification email message.</p> <p>You can include the following tokens in the message:</p> <ul style="list-style-type: none"><li>• %USER_NAME%</li><li>• %TOTAL_SPAM_COUNT%</li><li>• %TOTAL_SPAM_SIZE%</li><li>• %START_TIME%</li><li>• %END_TIME%</li></ul> |

7. Click **Save.**
- 

## End-User Quarantine Console

When you configure the End-User Quarantine settings, Deep Discovery Email Inspector provides the EUQ console that allows users to perform the following tasks:

- Manage the spam quarantine of their personal accounts

- Manage the spam quarantine of Active Directory distribution lists that they belong to
- Add senders to the Approved Senders list

**Note**

You can enable EUQ console access on the **User Quarantine Access** screen.

For more information, see [Configuring User Quarantine Access Settings on page 8-82](#).

---

## Accessing the End-User Quarantine Console

Access the EUQ console to manage quarantined spam messages and the Approved Senders list.

---

### Procedure

1. In a web browser, type the Deep Discovery Email Inspector server address with the port number **4459**.

`https://<target server IP address>:4459`

2. Do one of the following:

- To log on using a local user account:
  - a. Specify the logon credentials (user name and password).

The following table describes the logon user name format depending on the authentication method.

| AUTHENTICATION METHOD  | LOGON NAME FORMAT   |
|--|---|
| Active Directory   | Domain credentials in one of the following formats: <ul style="list-style-type: none"><li>User Principal Name (UPN)<br/>For example, <code>user1@domain.com</code>.</li><li>Down-level logon name<br/>For example, <code>domain\user1</code>.</li></ul> |
| <ul style="list-style-type: none"><li>SMTP</li><li>OpenLDAP</li><li>Domino</li></ul> | A valid email address   |

b. Click **Log On**.

• To log on with single sign-on:

a. Select a service name from the drop-down list.

b. Click **Single Sign-on (SSO)**.

The system automatically navigates to the logon page for your organization.

c. Follow the on-screen instructions and provide your account credentials to access the Deep Discovery Email Inspector management console.

---


## Viewing Quarantined Messages

You can view the list of quarantined email messages that Deep Discovery Email Inspector considers as spam/graymail for your account.

Access the EUQ console to display the **Quarantined Messages** screen.

For more information, see [Accessing the End-User Quarantine Console on page 8-89](#).

The following table describes the fields.

| FIELD   | DESCRIPTION  |
|---|--|
|  | View detailed message information such as message size, message ID, attachment file name, and message content (up to the first 2K of the content). |
| Sender  | View the sending email address of the detected message.  |
| Recipient   | View the detected message recipient email address.   |
| Email Subject   | View the email subject of the suspicious email message.  |
| Detected  | View the date and time that the suspicious email message was detected.   |

You can perform one of the following actions to manage quarantined messages:

- **Release:** Select one or more messages and click **Release** to release the selected messages.
- **Release and Approve Sender:** Select one or more messages and click **Release and Approve Sender** to release the selected messages and adds the sender email addresses to the Approved Senders list.
- **Delete:** Select one or more messages and click **Delete** to remove the selected message from the quarantine folder.



### Important

- Deep Discovery Email Inspector sends a released message directly to the intended recipient without reprocessing the message.
- To allow users to deliver released messages directly from without scanning, select **Deliver released messages directly without scanning** on the **User Quarantine Access** screen.

For more information, see [Configuring User Quarantine Access Settings on page 8-82](#).

- After deleting a message, you cannot recover the message.

## Adding Approved Senders

You can configure the Approved Senders list on the End-User Quarantine console to reduce false-positives for spam detections.



### Note

The Approved Senders list has priority over the Blocked Senders list. If a sender IP address is in both the Blocked Senders list and the Approved Senders list, Deep Discovery Email Inspector does not block messages from the sender.

For more information, see [Blocked Senders List on page 8-61](#).

---

### Procedure

1. Access the EUQ console.

For more information, see [Accessing the End-User Quarantine Console on page 8-89](#)

2. Click the **Approved Senders** tab.
3. To add an entry to the list, type an email address in the text field and click **Add**.

You can click **Delete** to remove a selected entry from the list.

4. Click **Save**.
- 

## Viewing Quarantined Messages for Distribution Lists

You can view the list of quarantined email messages that Deep Discovery Email Inspector considers as spam/graymail for the email distribution lists that you belong to.

---

### Procedure

1. Access the EUQ console.

For more information, see [Accessing the End-User Quarantine Console on page 8-89](#)

2. Click the **Distribution List Quarantine** tab.

The following table describes the fields.

| FIELD         | DESCRIPTION  |
|---------------|--|
| Sender        | View the sending email address of the detected message.                |
| Recipient     | View the detected message recipient email address.                     |
| Email Subject | View the email subject of the suspicious email message.                |
| Detected      | View the date and time that the suspicious email message was detected. |

You can perform one of the following actions to manage quarantined messages:

- **Query:** Click to filter messages based on the specified LDAP group name.
- **Release:** Select one or more messages and click **Release** to release the selected messages.
- **Delete:** Select one or more messages and click **Delete** to remove the selected message from the quarantine folder.

**Important**

- Deep Discovery Email Inspector sends a released message directly to the intended recipient without reprocessing the message.

When you release a message for a distribution list, the message is sent to all recipients in the distribution list.

- To allow users to deliver released messages directly from without scanning, select **Deliver released messages directly without scanning** on the **User Quarantine Access** screen.

For more information, see [Configuring User Quarantine Access Settings on page 8-82](#).

- After deleting a message, you cannot recover the message.
- 

## Mail Settings

Topics include:

- [Message Delivery on page 8-94](#)
- [Configuring SMTP Connection Settings on page 8-95](#)
- [Configuring Message Delivery Settings on page 8-98](#)
- [Configuring Limits and Exceptions on page 8-101](#)
- [Configuring the SMTP Greeting Message on page 8-105](#)
- [Configuring Edge MTA Relay Servers on page 8-106](#)
- [Internal Domains on page 8-107](#)
- [Transport Layer Security \(TLS\) on page 8-112](#)

## Message Delivery

Deep Discovery Email Inspector maintains a routing table based on domains and email addresses. Deep Discovery Email Inspector uses this routing table to route email messages (with matching recipient domains or email

addresses) to specified destination servers or to destination servers that match specified mail exchanger records (MX records).

There are two message delivery methods:

- Look up MX record

When delivering an email message using MX record lookup, Deep Discovery Email Inspector queries the specified MX record, and then delivers the email message to the destination server identified by the MX record.

- Specify servers

When delivering an email message using specified servers, Deep Discovery Email Inspector first sends the email message to the destination server with the highest priority. If the server is unavailable, Deep Discovery Email Inspector chooses the remaining servers in descending order of their priority. If multiple destination servers have the same priority, Deep Discovery Email Inspector randomly selects a server for message delivery.

Email messages destined to unspecified domains and email addresses are routed based on the records in the Domain Name Server (DNS). For example, if the delivery domain includes “example.com” and the associated SMTP server is 10.10.10.10 on port 25, then all email messages sent to “example.com” deliver to the SMTP server at 10.10.10.10 using port 25.

## Configuring SMTP Connection Settings

Configure SMTP connection settings to control which MTAs and mail user agents are allowed to connect to the server.



### Note

Connection control settings take priority over mail relay settings.

---

## Procedure

1. Go to **Administration > Mail Settings > Connections**.

## 2. Specify the **SMTP Interface** settings.

| OPTION                                     | DESCRIPTION  |
|--|--|
| Port                                       | Specify the listening port of the SMTP service.  |
| Disconnect after { } minutes of inactivity | Specify a time-out value.  |
| Simultaneous connections                   | Click <b>No limit</b> or <b>Allow up to { } connections</b> and specify the maximum allowed connections. |

## 3. Specify the **Connection Control** settings.

- a. Select a connections “deny list” or “permit list”.
  - Select **Accept all, except the following list** to configure the “deny list”.
  - Select **Deny all, except the following list** to configure the “permit list”.
- b. Select an option and then specify the IP addresses.

| OPTION             | DESCRIPTION  |
|--------------------|--|
| Single computer    | Specify an IPv4 or IPv6 address, and then click [ >> ] to add it to the list.  |
| Group of computers | <ol style="list-style-type: none"> <li>1. Select the IP version.</li> <li>2. Type the <b>Subnet address</b>.</li> <li>3. If IPv4 was selected, type the <b>Subnet mask</b>.</li> <li>4. Click [ &gt;&gt; ] to add it to the list.</li> </ol> |

| OPTION           | DESCRIPTION  |
|------------------|--|
| Import from File | Click to import an IP list from a file. The following list shows sample content of an IP list text file:<br><br>192.168.1.1<br><br>192.168.2.0:255.255.255.0<br><br>192.168.3.1:255.255.255.128<br><br>192.168.4.100<br><br>192.168.5.32:255.255.255.192 |

4. Specify the **Transport Layer Security** settings.

See [Configuring TLS Settings on page 8-97](#).

5. Click **Save**.

---

## Configuring TLS Settings

Transport Layer Security (TLS) provides a secure communication channel between hosts over the Internet, ensuring the privacy and integrity of the data during transmission.

For details about TLS settings, see [Transport Layer Security \(TLS\) on page 8-112](#).



### Note

Deep Discovery Email Inspector supports TLS 1.2 and earlier versions.

---

## Procedure

1. Go to **Administration > Mail Settings > Connections**.
2. Go to the bottom of the page to the section titled **Transport Layer Security**.
3. Select **Enable incoming TLS**.

This option allows the Deep Discovery Email Inspector SMTP Server to provide Transport Layer Security (TLS) support to SMTP email relays, but does not require that email relays use TLS encryption to establish the connection.

4. Select **Only accept SMTP connections through TLS** for Deep Discovery Email Inspector to only accept secure incoming connections.

This option enables the Deep Discovery Email Inspector SMTP server to accept messages only through a TLS connection.

5. Click a **Browse** button next to one of the following:

| OPTION                    | DESCRIPTION   |
|---------------------------|---|
| CA certificate            | The CA certificate verifies an SMTP email relay. However, Deep Discovery Email Inspector does not verify the email relay and only uses the CA certificate for enabling the TLS connection.  |
| Private key               | <p>The SMTP email relay creates the session key by encrypting a random number using the Deep Discovery Email Inspector SMTP server's public key.</p> <p>The Deep Discovery Email Inspector SMTP server then uses the private key to decrypt the random number in order to establish the secure connection.</p> <p>This key must be uploaded to enable a TLS connection.</p> |
| SMTP server certification | <p>SMTP email relays can generate session keys with the Deep Discovery Email Inspector SMTP server public key.</p> <p>Upload the key to enable a TLS connection.</p>  |

6. Select **Enable outgoing TLS**.

7. Click **Save**.
- 

## Configuring Message Delivery Settings

The following procedure explains how to configure message delivery settings for downstream mail servers.

For more information about configuring connections, importing message delivery settings, and setting message rules, see [Mail Settings on page 8-94](#).

Specify settings for email message delivery to Deep Discovery Email Inspector downstream mail servers. Deep Discovery Email Inspector checks the recipient domains or email addresses, determines destination servers, and sends the message to the next SMTP host for the matched domain or email address.

---

### Procedure

1. Go to **Administration > Mail Settings > Message Delivery**.

2. Click **Add**.

The **Add Delivery Profile** screen appears.

3. Select the status of the delivery profile.

4. Specify the recipient domain or email address. Type a wildcard (\*) to manage email message delivery from a domain and any subdomains.

- \* (Include all domains)
- example.com (Include only example.com)
- \*.example.com (Include example.com and any subdomains)

5. Select either of the following from the **Destination servers** drop-down list:

- **Look up MX record:** Specify the MX record name, and a port number when connecting through a non-default port.
- **Specify server:** Specify the IP address or fully qualified domain name, port number, and priority to forward email messages.

**Note**

- The lower the priority value, the higher the priority.
  - Optionally add multiple destination servers by clicking on **Add server**.
  - To disable a destination server, click on the check mark for the server behind the **Priority** field. Then the check mark becomes a dash mark. To enable the server again, click the dash mark.
- 

**6. Click **Save**.**

---

## Importing Message Delivery Settings

Use this option if you have a properly formatted .xml file containing message delivery settings. Optionally, export existing settings from the management console, or download a sample XML from the **Import Delivery Profiles** screen and generate a file according to the exported file.

Specify settings for email message delivery to Deep Discovery Email Inspector downstream mail servers. Deep Discovery Email Inspector checks the recipient domains or email addresses, determines destination servers, and sends the message to the next SMTP host for the matched domain or email address.

---

### Procedure

1. Go to **Administration > Mail Settings > Message Delivery**.
2. Click  **Import**.

The **Import Delivery Profiles** screen appears.

3. Click **Browse** to locate the file to import.
4. Select one of the options:
  - Merge with existing profiles: Add the imported profiles into the current message delivery list.

- Replace existing profiles: Overwrite all existing profiles with the profiles in the XML file.

5. Click **Continue**.

The profiles are added to the **Message Delivery** list.

---

## Configuring Limits and Exceptions

Set limits on the email messages that Deep Discovery Email Inspector processes to:

- Improve performance by reducing the total number of email messages required to process
- Restrict senders of relayed messages and recipient domains to prevent Deep Discovery Email Inspector from acting as an open mail relay
- Reject messages from unknown sender domains or sender IP addresses to prevent unwanted spam messages



### Note

Connection control settings take priority over mail relay settings.

---

## Procedure

1. Go to **Administration > Mail Settings > Limits and Exceptions**.
2. Specify the **Message Limits** settings:

| OPTION                       | DESCRIPTION                                     |
|------------------------------|---|
| Maximum message size         | Specify maximum message size from 1 to 2047 MB. |
| Maximum number of recipients | Specify number of recipients from 1 to 99,999.  |

3. Specify the **Relay Control** options to filter incoming messages.

**Note**

- Relay control settings only take effect when Deep Discovery Email Inspector is in MTA mode.
  - When you enable the message rejection options, Deep Discovery Email Inspector matches the permitted sender list first and then checks for unknown recipients.
- 

- **Reject messages from unknown sender domains:** Select this option to block messages from senders with no matching domain through DNS lookup.
  - **Reject messages from unknown sender IP addresses:** Select this option to block messages from senders with no matching IP address through reverse DNS lookup.
- 

**Note**

Enabling this feature blocks all messages from an edge MTA.

---

- **Reject messages to unknown recipients:** Select this option to have Deep Discovery Email Inspector block messages with a sender not in the approved list and an unknown recipient. A recipient is considered as unknown if no result is found through LDAP query.
- 

**Note**

If you enable this option, configure the permitted recipient domains. Otherwise, Deep Discovery Email Inspector will block the messages.

---

#### 4. Specify the **Permitted Recipient Domains**.

Do one of the following:

- Add an single domain:
  - a. Type a domain name.

- b. Click > to include the entry in the **Permitted recipient domains** list.
- Import a list of domains:

**Note**

Deep Discovery Email Inspector can import domain names from a text file. Ensure that the text file contains only one email address per line.

---

- a. Click **Import From File**.
- b. Select a text file and click **OK**.

The new entries appear in the **Permitted recipient domains** list.

**Note**

- To export the permitted recipient domain list, click **Export** and save the text file on your computer. To replicate the same permitted recipient domain settings on several Deep Discovery Email Inspector appliances, import the text file on the target appliances.
- Deep Discovery Email Inspector bypasses SPF and DKIM verifications for domains you configure in the **Permitted Recipient Domains** list.

For more information, see [Sender Policy Framework \(SPF\) on page 8-71](#) and [DomainKeys Identified Mail \(DKIM\) on page 8-74](#).

---

- 5. Specify the **Permitted Senders of Relayed Mail**.
  - **Deep Discovery Email Inspector only**
  - **Hosts in the same subnet**
  - **Hosts in the same address class**

**Note**

When this option is selected, Deep Discovery Email Inspector will check if the IP address of Deep Discovery Email Inspector and hosts are in the same address class and subnet.

- Deep Discovery Email Inspector will only allow hosts to relay messages if they are in the same address class and subnet.

For example:

- Class A: The Deep Discovery Email Inspector IP address is 10.1.2.3, and the hosts' IP address is 10.1.2.x.

Class B: The Deep Discovery Email Inspector IP address is 172.31.2.3, and the hosts' IP address is 172.31.x.x.

Class C: The Deep Discovery Email Inspector IP address is 192.168.10.3, and the hosts' IP address is 192.168.10.x.

- Deep Discovery Email Inspector will not allow hosts to relay messages if they are in the same address class, but not in the same subnet.

For example:

- Class A: The Deep Discovery Email Inspector IP address is 10.1.2.3, and the hosts' IP address is 11.2.3.x.

Class B: The Deep Discovery Email Inspector IP address is 172.31.2.3, and the hosts' IP address is 172.32.x.x.

Class C: The Deep Discovery Email Inspector IP address is 192.168.10.3, and the hosts' IP address is 192.168.11.x.

---

- **Specified IP addresses**

**Note**

Import settings from a file by clicking **Import from a File**.

Export settings to a file by clicking **Export**.

---

6. Click **Save**.

---

## Configuring the SMTP Greeting Message

The SMTP greeting message presents to the mail relay whenever Deep Discovery Email Inspector establishes an SMTP session.

---

### Procedure

1. Go to **Administration > Mail Settings > SMTP Greeting**
  2. In the text box, specify a greeting message.
  3. Click **Save**.
- 

## Edge MTA Relay Servers

When you deploy Deep Discovery Email Inspector as a non-edge MTA in your network, you can specify the edge MTA servers that relay external email messages to Deep Discovery Email Inspector on your internal network.

The following table describes information on the **Edge MTA Relay Servers** screen.

| HEADER            | DESCRIPTION  |
|-------------------|--|
| IP address/Domain | View the IP address or domain name of the edge MTA relay server. |
| Description       | View a description for the edge MTA relay server.                |

**Note**

- If you deploy Deep Discovery Email Inspector as an edge MTA in your network, the sender IP address is the public IP address of the external MTA nearest to your network.
  - If you deploy Deep Discovery Email Inspector as a non-edge MTA in your network, the sender IP address is the IP address of the MTA nearest to the edge MTA relay server.
- 

## Configuring Edge MTA Relay Servers

When Deep Discovery Email Inspector is not deployed as an edge MTA in your network, configure the edge MTA relay servers.

---

**Note**

You can configure up to 256 edge MTA relay servers.

---


### Procedure

1. Go to **Administration > Mail Settings**.
2. Click the **Edge MTA Relay Servers**.
3. Click **Add**.

The **Add Edge MTA Relay Server** screen appears.

4. Configure the settings.

| FIELD             | DESCRIPTION   |
|-------------------|---|
| IP address/Domain | Type the IP address or domain name for the edge MTA relay server. |
| Description       | Type a description for the entry.                                 |

5. (Optional) To add more entries, click **Add More** and do the following:  
To delete an entry from the list, click the icon (  ) in the **Action** column.

6. Click **Save**.

A new entry displays in the edge MTA relay servers list.

To remove one or more entries, select the entries and click **Delete**.

---

## Internal Domains

You can configure the internal domain list to allow Deep Discovery Email Inspector to determine whether a message is incoming or outgoing.

If the domain of a sender address is in the internal domain list, Deep Discovery Email Inspector considers messages from the sender as outgoing messages. Deep Discovery Email Inspector applies policies based on the message direction.



**Note**

If you do not add any entries in the internal domain list, Deep Discovery Email Inspector considers all messages as incoming messages by default.

---

## Adding Internal Domains

You can add up to 1024 internal domains.

---

### Procedure

1. Go to **Administration > Mail Settings > Internal Domains**.
2. Click **Add**.
3. Type a domain. You can use the \* wildcard character as a prefix in the domain.  
  
For example, example.com, sub.example.com, or \*.example.com.
4. Type additional information for the domain.
5. (Optional) Specify a note.
6. (Optional) Click **Add more** to add more domains.

7. Click **Save**.
8. (Optional) Select **Include permitted recipient domains** to set the recipient domains you specify on the **Limits and Exceptions** screen as internal domains.

For more information, see [Configuring Limits and Exceptions on page 8-101](#).

9. Click **Save**.

After adding a domain:

- Click **Delete** to remove the selected entry.
  - Click **Export** to download all entries as a CSV file.
- 

## Importing Internal Domains

You can import internal domains from a properly-formatted CSV file.

---

### Procedure

1. Go to **Administration > Mail Settings > Internal Domains**.
2. Click **Import**.
3. Click **Select File** to locate the file to import
4. Select one of the following options:
  - **Merge with current list**: Add the imported entries into the existing internal domain list.
  - **Overwrite current list**: Replace all entries with entries in the CSV file.
5. Click **Import**.

The imported entries display in the list.

---

## Address Modification

When Deep Discovery Email Inspector is in MTA mode, you can configure address modification settings in Deep Discovery Email Inspector to:

- Rewrite sender or recipient addresses in message envelopes or message headers
- Rewrite domains in email addresses



### Note

- Deep Discovery Email Inspector modifies email addresses before policy matching and message delivery.
  - Deep Discovery Email Inspector does not generate event logs for address modification actions.
- 

## Configuring Address Rewriting

Configure address rewriting settings in Deep Discovery Email Inspector to change the recipient or sender addresses in email messages before delivery. You can use the address rewriting feature, for example, to reroute specific messages to a different email host, or to map one user name to another user name.



### Note

- Deep Discovery Email Inspector scans email messages and applies policy rules based on the rewritten email addresses.
  - Deep Discovery Email Inspector performs email submission, sender filtering, and sender authentication before email address modification.
- 

You can configure rewriting rules to replace the entire email address or only the domain portion of the address. The following table shows some examples.

| ORIGINAL ADDRESS  | NEW ADDRESS         |
|-------------------|---------------------|
| test@example.com  | myname@mydomain.com |
| test1@example.com | test2@example.com   |
| test@test.com     | test@example.com    |

---

## Procedure

1. Go to **Administration > Mail Settings > Address Modification**.

The **Address Rewriting** screen appears.

2. Select **Enable address rewriting** to enable this feature.
3. Select the location of the sender and recipient addresses to match.
4. Configure one or more address rewriting rules. Do one of the the following:
  - To import rules from a file, click **Import** and select the CSV file that contains the rule settings.
  - To manually add a rule, complete the following steps:
    - a. Type the original email address.
    - b. Type the new email address to replace the original email address.
    - c. Select the address type (**Sender**, **Recipient**, or **Sender and recipient**) to apply the rule.
    - d. Click **Add**.

After you have configured one or more rules, you can:

- Click **Delete** to remove the selected entries.
- Click **Export** to export the selected entries in a CSV file.

5. Click **Save**.
-

## Configuring Email Domain Rewriting

Address domain rewriting or address masquerading modifies the domain information in email addresses, allowing you to hide hosts in a domain behind an email gateway (or Deep Discovery Email Inspector). Address domain rewriting makes it appear as if email messages originate from the gateway and not from individual endpoints.



### Note

- Deep Discovery Email Inspector scans email messages and applies policy rules based on the rewritten email addresses.
  - Deep Discovery Email Inspector performs email submission, sender filtering, and sender authentication before email address modification.
- 

## Procedure

1. Go to **Administration > Mail Settings > Address Modification** and click the **Domain Rewriting**.
2. Select **Enable domain rewriting** to enable this feature.
3. Select the location of the sender and recipient addresses to match.
4. (Optional) Under User Name Exceptions, type one or more email address user names to bypass domain rewriting.



### Note

User name exceptions have priority over domain exceptions.

---

5. Under Settings, configure the domain rewrite and exception lists.  
Type a domain name and click **Add to Rewrite List** or **Add to Exception List**.
  6. Click **Save**.
-

## Transport Layer Security (TLS)

Transport Layer Security (TLS) provides a secure communication channel between hosts over the Internet, ensuring the privacy and integrity of the data during transmission.

Two hosts (the Deep Discovery Email Inspector appliance and the email relay) establish a TLS session as follows:

1. The sending host requests a secure connection with the receiving host by sending a cipher list.
2. The two hosts establish a connection.
3. The receiving host selects one cipher and replies with its digital certificate signed by a Certificate Authority (CA).
4. The sending host verifies the identity with the trusted CA certificate and generates the session keys by encrypting a message using a public key.
5. The receiving host decrypts the message using the corresponding private key.
6. The sending host's identity verifies when the receiving host can decrypt the message with the private key.
7. The TLS session establishes and email messages passed between the hosts are encrypted.



### Tip

By default, Deep Discovery Email Inspector does not apply TLS or email encryption, nor does it verify email relay host identities. Enable TLS for Deep Discovery Email Inspector to encrypt incoming email messages.

---

## Deploying Deep Discovery Email Inspector in TLS Environments

Enable the TLS settings for messages entering and exiting Deep Discovery Email Inspector.

---

## Procedure

1. Review the prerequisites.

See [Prerequisites for Using TLS on page 8-113](#).

2. Enable incoming TLS.

See [Configuring TLS Settings for Incoming Messages on page 8-114](#).

3. Enable outgoing TLS.

See [Configuring TLS Settings for Outgoing Messages on page 8-121](#).

---

## Prerequisites for Using TLS

Establishing the TLS infrastructure requires that the organization has its own Certificate Authority (CA) key or is able to sign all generated certificate requests by an external CA. Private keys and certificate requests must be generated for each SMTP server in the network. The certificate requests should be signed by the CA.

### Obtaining a Digital Certificate

To obtain a digital certificate, perform one of the following actions:

- Create a certificate signing request (CSR) on the management console. Request a CA to sign the certificate. Import the signed certificate into Deep Discovery Email Inspector.
- Create a self-signed certificate on the management console
- Apply for the certificate and public/private key pairs from a CA. Import the certificate and key file into Deep Discovery Email Inspector.

To configure certificate signing requests and manage certificates in Deep Discovery Email Inspector, see [Certificate Management on page 8-202](#).

## Configuring TLS Settings


Use the management console to enable the TLS settings for messages entering and exiting Deep Discovery Email Inspector. With Deep Discovery

Email Inspector acting as the SMTP server, configure TLS settings for incoming messages. With Deep Discovery Email Inspector acting as the SMTP client, configure TLS settings for outgoing messages.

## Incoming Messages

When Deep Discovery Email Inspector acts as the SMTP server that receives email messages from an upstream MTA, configure TLS settings for messages entering Deep Discovery Email Inspector.

The following table describes the tasks you can perform on the **Incoming Messages** screen.

| TASK                | DESCRIPTION  |
|---------------------|--|
| Add TLS settings    | Click <b>Add</b> .<br>For more information, see <a href="#">Configuring TLS Settings for Incoming Messages on page 8-114</a> .   |
| Edit TLS settings   | Click an IP address or domain.<br>For more information, see <a href="#">Configuring TLS Settings for Incoming Messages on page 8-114</a> .   |
| Import TLS settings | Click <b>Import</b> .<br>For more information, see <a href="#">Importing TLS Settings on page 8-116</a> .  |
| Export TLS settings | Select one or more entries and click <b>Export</b> ; otherwise, click <b>Export All</b> to export all entries in a comma-separated values (CSV) file.<br><br><div>  <b>Note</b><br/>           When exporting TLS settings, the system also includes the default entry (indicated by an asterisk "**") in the exported file.         </div> |
| Delete TLS settings | Select one or more entries and click <b>Delete</b> .   |

## Configuring TLS Settings for Incoming Messages

---

## Procedure

1. Go to **Administration > Mail Settings > TLS**.

The **Incoming Messages** screen appears.

2. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry.
3. Select a status option.
4. Specify the IP address of, subnet, or the domain of target email senders.



### Note

You cannot change the IP address or domain setting for the default entry.

---

5. Select a security level.

| SECURITY LEVEL | DESCRIPTION   |
|----------------|---|
| Never          | Deep Discovery Email Inspector does not use TLS for the specified IP address or domain.   |
| Opportunistic  | Deep Discovery Email Inspector declares support for TLS for the specified IP address or domain. The client can choose whether to start a TLS connection.  |
| Must           | Deep Discovery Email Inspector requires TLS for communication for the specified IP address or domain. Communication between Deep Discovery Email Inspector and the client is encrypted.                   |
| Verify         | Deep Discovery Email Inspector requires the client to start a TLS connection for the specified IP address or domain and send its certificate to Deep Discovery Email Inspector for client identification. |

6. Select a cipher grade option.

**Note**

This field is not applicable if you select the **Never** security level.

---

| CIPHER GRADE | DESCRIPTION   |
|--------------|---|
| Medium       | Communication between Deep Discovery Email Inspector and clients uses "medium" and "strong" encryption cipher suites. |
| High         | Communication between Deep Discovery Email Inspector and clients uses "strong" encryption cipher suites.              |

---

**7. Click **Save**.**

---

**Importing TLS Settings**

---

**Note**

You can include the default entry (using an astrisk "\*") in the import file to update the settings.

---

**Procedure****1. Go to **Administration** > **Mail Settings** > **TLS**.**

The **Incoming Messages** screen appears.

**2. Click **Import**.****3. Click **Select**.****4. Select a comma-separated values (CSV) file containing a list of IP addresses or domains.**


The new entries appear in the table.

---

**Outgoing Messages**

When Deep Discovery Email Inspector acts as the SMTP client that sends email messages to a downstream MTA, configure TLS settings for messages existing Deep Discovery Email Inspector.

The following table describes the tasks you can perform on the **Outgoing Messages** screen.

| TASK                | DESCRIPTION  |
|---------------------|--|
| Add TLS settings    | Click <b>Add</b> .<br>For more information, see <a href="#">Configuring TLS Settings for Outgoing Messages on page 8-121</a> .   |
| Edit TLS settings   | Click an IP address or domain.<br>For more information, see <a href="#">Configuring TLS Settings for Outgoing Messages on page 8-121</a> .   |
| Import TLS settings | Click <b>Import</b> .<br>For more information, see <a href="#">Importing TLS Settings on page 8-123</a> .  |
| Export TLS settings | Click <b>Export All</b> to export all entries in a comma-separated values (CSV) file.<br><br><div> <b>Note</b><br/>When exporting TLS settings, the system also includes the default entry (indicated by an astrisk "**") in the exported file.</div> |
| Delete TLS settings | Select one or more entries and click <b>Delete</b> .   |

### DANE for SMTP

Deep Discovery Email Inspector supports DANE (DNS-based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity.

You can specify the DANE or DANE-only security level for outbound messages. For more information, see [Configuring TLS Settings for Outgoing Messages on page 8-121](#).

The following tables show the actions performed on outbound messages depending on the DNS and TLSA records and verification results.

**TABLE 8-11. DANE-only**

| <b>MX RECORD</b> | <b>A RECORD</b> | <b>TLSA</b> | <b>CERTIFICATE<br/>VERIFICATION</b> | <b>DANE<br/>VERIFICATION</b> | <b>ACTION</b>                                  |
|------------------|-----------------|-------------|-------------------------------------|------------------------------|--|
| Secure           | Secure          | Secure      | Successful                          | Successful                   | Deliver  |
| Secure           | Secure          | Secure      | Unsuccessful                        | Unsuccessful                 | Defer (server<br>certificate<br>not trusted)   |
| Secure           | Secure          | Insecure    | N/A                                 | Unsuccessful                 | Defer (non-<br>DNSSEC<br>destination)          |
| Secure           | Secure          | NXDOMAIN    | N/A                                 | Unsuccessful                 | Defer (no<br>TLSA record)                      |
| Secure           | Secure          | Bogus       | N/A                                 | Unsuccessful                 | Defer (TLSA<br>lookup error)                   |
| Secure           | Insecure        | N/A         | N/A                                 | Unsuccessful                 | Defer (non-<br>DNSSEC<br>destination)          |
| Secure           | Bogus           | N/A         | N/A                                 | Unsuccessful                 | Defer (host or<br>domain<br>name not<br>found) |
| Insecure         | Secure          | Secure      | Successful                          | Unsuccessful                 | Defer (non-<br>DNSSEC<br>destination)          |
| Insecure         | Secure          | Secure      | Unsuccessful                        | Unsuccessful                 | Defer (non-<br>DNSSEC<br>destination)          |
| Insecure         | Secure          | Insecure    | N/A                                 | Unsuccessful                 | Defer (non-<br>DNSSEC<br>destination)          |

| <b>MX RECORD</b> | <b>A RECORD</b> | <b>TLSA</b> | <b>CERTIFICATE<br/>VERIFICATION</b> | <b>DANE<br/>VERIFICATION</b> | <b>ACTION</b>                         |
|------------------|-----------------|-------------|-------------------------------------|------------------------------|---------------------------------------|
| Insecure         | Secure          | NXDOMAIN    | N/A                                 | Unsuccessful                 | Defer (non-DNSSEC destination)        |
| Insecure         | Secure          | Bogus       | N/A                                 | Unsuccessful                 | Defer (non-DNSSEC destination)        |
| Insecure         | Insecure        | N/A         | N/A                                 | Unsuccessful                 | Defer (non-DNSSEC destination)        |
| Insecure         | Bogus           | N/A         | N/A                                 | Unsuccessful                 | Defer (host or domain name not found) |
| Bogus            | N/A             | N/A         | N/A                                 | Unsuccessful                 | Defer (host or domain name not found) |

**TABLE 8-12. DANE**

| <b>MX RECORD</b> | <b>A RECORD</b> | <b>TLSA</b> | <b>CERTIFICATE<br/>VERIFICATION</b> | <b>DANE<br/>VERIFICATION</b> | <b>ACTION</b>                          |
|------------------|-----------------|-------------|-------------------------------------|------------------------------|--|
| Secure           | Secure          | Secure      | Successful                          | Successful                   | Deliver                                |
| Secure           | Secure          | Secure      | Unsuccessful                        | Unsuccessful                 | Defer (server certificate not trusted) |
| Secure           | Secure          | Insecure    | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |
| Secure           | Secure          | NXDOMAIN    | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |

| <b>MX RECORD</b> | <b>A RECORD</b> | <b>TLSA</b> | <b>CERTIFICATE<br/>VERIFICATION</b> | <b>DANE<br/>VERIFICATION</b> | <b>ACTION</b>                          |
|------------------|-----------------|-------------|-------------------------------------|------------------------------|--|
| Secure           | Secure          | Bogus       | N/A                                 | Unsuccessful                 | Defer (TLSA lookup error)              |
| Secure           | Insecure        | N/A         | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |
| Secure           | Bogus           | N/A         | N/A                                 | Unsuccessful                 | Defer (host or domain name not found)  |
| Insecure         | Secure          | Secure      | Successful                          | Unsuccessful                 | Fall back to opportunistic TLS         |
| Insecure         | Secure          | Secure      | Unsuccessful                        | Unsuccessful                 | Defer (server certificate not trusted) |
| Insecure         | Secure          | Insecure    | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |
| Insecure         | Secure          | NXDOMAIN    | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |
| Insecure         | Secure          | Bogus       | N/A                                 | Unsuccessful                 | Defer (TLSA lookup error)              |
| Insecure         | Insecure        | N/A         | N/A                                 | Unsuccessful                 | Fall back to opportunistic TLS         |
| Insecure         | Bogus           | N/A         | N/A                                 | Unsuccessful                 | Defer (host or domain name not found)  |

| <b>MX RECORD</b> | <b>A RECORD</b> | <b>TLSA</b> | <b>CERTIFICATE<br/>VERIFICATION</b> | <b>DANE<br/>VERIFICATION</b> | <b>ACTION</b>                         |
|------------------|-----------------|-------------|-------------------------------------|------------------------------|---------------------------------------|
| Bogus            | N/A             | N/A         | N/A                                 | Unsuccessful                 | Defer (host or domain name not found) |

### Configuring TLS Settings for Outgoing Messages

#### Procedure

1. Go to **Administration > Mail Settings > TLS**.
2. Click **Outgoing Messages**.
3. Do one of the following:
  - Click **Add** to create a new entry.
  - Click an entry.
4. Select a status option.
5. Specify the domain of target message recipients.



#### Note

You cannot change the domain setting for the default entry.

6. Select a security level.

| <b>SECURITY LEVEL</b> | <b>DESCRIPTION</b>  |
|-----------------------|---|
| Never                 | Deep Discovery Email Inspector does not use TLS for the specified IP address or domain.   |
| Opportunistic         | Deep Discovery Email Inspector declares support for TLS for the specified IP address or domain. The mail server can choose whether to start a TLS connection. |

| SECURITY LEVEL | DESCRIPTION   |
|----------------|---|
| Must           | Deep Discovery Email Inspector requires TLS for communication for the specified IP address or domain. Communication between Deep Discovery Email Inspector and the mail server is encrypted.  |
| Verify         | Deep Discovery Email Inspector requires the mail server to start a TLS connection for the specified IP address or domain. Deep Discovery Email Inspector sends its certificate to the mail server for client identification.  |
| DANE           | <p>Deep Discovery Email Inspector uses DANE for email message verification first. If DANE verification is unsuccessful, Deep Discovery Email Inspector performs one of the following based on the error condition: revert to using opportunistic TLS for secured connections, add the message to the deferred queue, or reject the message.</p> <p>For more information, see <a href="#">DANE for SMTP on page 8-117</a>.</p> |
| DANE only      | <p>Deep Discovery Email Inspector uses DANE for email message verification. If DANE verification is unsuccessful, Deep Discovery Email Inspector adds the message to the deferred queue or rejects the message, depending on the error condition.</p> <p>For more information, see <a href="#">DANE for SMTP on page 8-117</a>.</p>   |

## 7. Select a cipher grade option.



### Note

This field is not applicable if you select the **Never** security level.

| CIPHER GRADE | DESCRIPTION  |
|--------------|--|
| Medium       | Communication between Deep Discovery Email Inspector and SMTP servers uses "medium" and "strong" encryption cipher suites. |
| High         | Communication between Deep Discovery Email Inspector and SMTP servers uses "strong" encryption cipher suites.              |

8. Click **Save**.

---

### Importing TLS Settings

---

**Note**

You can include the default entry (using an astrisk "\*") in the import file to update the settings.

---

### Procedure

1. Go to **Administration > Mail Settings > TLS**.
  2. Click **Outgoing Messages**.
  3. Click **Import**.
  4. Click **Select**.
  5. Select a comma-separated values (CSV) file containing a list of domains.  
The new entries appear in the table.
- 

## Integrated Products/Services

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

- [Trend Vision One on page 8-124](#)
- [Apex Central on page 8-127](#)
- [Deep Discovery Director on page 8-132](#)
- [Auxiliary Products/Services on page 8-138](#)
- [Threat Intelligence Sharing on page 8-137](#)
- [LDAP on page 8-165](#)
- [SAML Integration on page 8-168](#)

- [Log Settings on page 8-178](#)
- [SFTP on page 8-181](#)
- [Email Encryption on page 8-182](#)

## Integrated Trend Micro Products

For seamless integration, make sure that the Trend Micro products that integrate with Deep Discovery Email Inspector run the required or recommended versions.

**TABLE 8-13. Trend Micro Products and Services that Integrate with Deep Discovery Email Inspector**

| PRODUCT/ SERVICE                              | VERSION   |
|---|---|
| Trend Vision One                              |   |
| Deep Discovery Director - On-premises version | <ul style="list-style-type: none"><li>• 5.3</li></ul>               |
| Deep Discovery Analyzer                       | <ul style="list-style-type: none"><li>• 7.0</li><li>• 6.9</li></ul> |
| Apex Central                                  | <ul style="list-style-type: none"><li>• 2019</li></ul>              |
| Smart Protection Server                       | <ul style="list-style-type: none"><li>• 3.3</li><li>• 3.2</li></ul> |
| TippingPoint Security Management System (SMS) | <ul style="list-style-type: none"><li>• 5.4</li><li>• 5.3</li></ul> |

## Trend Vision One

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

Deep Discovery Email Inspector integrates with Trend Vision One to perform the following tasks for collaborative security analytics in a hybrid environment:

- Synchronize suspicious object and exception lists with Trend Vision One
- Upload analysis reports from the internal Virtual Analyzer to Trend Vision One

**Note**

If you register Deep Discovery Email Inspector to Trend Vision One, Deep Discovery Director 3.0 (or later), and Trend Micro Apex Central, Deep Discovery Email Inspector synchronizes suspicious objects and exception lists with the integrated products in the following priority: Trend Vision One, Deep Discovery Director, Apex Central.

---

## Integrating Deep Discovery Email Inspector with Trend Vision One

You can integrate Deep Discovery Email Inspector with Trend Vision One directly or through a Service Gateway.

**Important**

Before you can configure integration settings, apply the latest hotfix or patch.

---

### Procedure

1. On the Trend Vision One console, go to **Point Product Connection > Product Connector**.
2. Click **Connect**.
3. In the **Product name** field, select **Deep Discovery Email Inspector**.
4. Click the link to generate an enrollment token.
5. Copy the enrollment token for use on the Deep Discovery Email Inspector web console.

6. Click **Save**.
  7. On the Deep Discovery Email Inspector web console, go to **Administration > Integrated Products/Services** and click **Trend Vision One**.
  8. Paste the enrollment token you obtained from the Product Connector in Trend Vision One.
  9. To integrate Deep Discovery Email Inspector with Trend Vision One through a Service Gateway, do the following:
    - a. On the Trend Vision One console, go to **Workflow and Automation > Service Gateway Management**. If available, click the **Service Gateway Management 2.0** tab.
    - b. If you do not have an existing Service Gateway deployed, install a Service Gateway.

For detailed deployment instructions, see [Deploying a Service Gateway Virtual Appliance](#).
    - c. Click the Service Gateway name.
    - d. Click **Manage Services**.
    - e. Click the install icon to install and then enable the **Forward proxy** service.
    - f. Record the Service Gateway IP address that is needed for connection settings on the Deep Discovery Email Inspector console.
    - g. On the Deep Discovery Email Inspector web console, go to **Administration > Integrated Products/Services** and click **Trend Vision One**.
    - h. Select **Enable Service Gateway connection**.
    - i. Specify the IPv4 or IPv6 address of the Service Gateway.
  10. Click **Register**.
  11. Click **Test Connection** to verify.
-

## Unregistering Deep Discovery Email Inspector from Trend Vision One

---



### Important

- Unregistering Deep Discovery Email Inspector from Trend Vision One clears entries in the suspicious object lists that originated from Trend Vision One.
  - After unregistering Deep Discovery Email Inspector from Trend Vision One, you must obtain a new enrollment token to register to Trend Vision One again.
- 

### Procedure

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

The **Trend Vision One** tab appears.

2. Click **Unregister**.

A warning screen appears.

3. Click **Unregister** to confirm.
- 

## Apex Central

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



### Note

Ensure that both Deep Discovery Email Inspector and the Apex Central server belong to the same network segment. If Deep Discovery Email Inspector is not in the same network segment as Apex Central, configure the port forwarding settings for Deep Discovery Email Inspector.

---

For details about Apex Central features, see [Apex Central Features on page 8-128](#).

On Deep Discovery Email Inspector, use the **Administration > Integrated Products/Services > Apex Central** tab to perform the following tasks:

- Register to an Apex Central server.

For details, see [Registering to Apex Central on page 8-129](#).

- Check the connection status between Deep Discovery Email Inspector and Apex Central.
- Unregister from an Apex Central server.

For details, see [Unregistering from Apex Central on page 8-132](#).

- Synchronize suspicious objects with Apex Central.



#### Note

If you register Deep Discovery Email Inspector to both Deep Discovery Director 5.0 (or later) and Apex Central, Deep Discovery Email Inspector synchronizes suspicious objects and exception lists from Deep Discovery Director only. You can check the synchronization status on the Deep Discovery Director management console.

## Apex Central Features

Apex Central offers the following features:

**TABLE 8-14. Apex Central Features**

| FEATURE                            | APEX CENTRAL SCREEN  |
|------------------------------------|--|
| Log data aggregation               | <b>Log Aggregation Settings</b>  |
| Suspicious object data aggregation | <b>Suspicious Objects</b>  |
| Reports                            | <ul style="list-style-type: none"> <li>• One-time report: <b>One-time Reports</b></li> <li>• Scheduled report: <b>Scheduled Reports</b></li> </ul> |

| FEATURE                   | APEX CENTRAL SCREEN             |
|---------------------------|---------------------------------|
| Notifications             | <b>Event Notifications</b>      |
| Single sign-on (SSO)      | <b>Products</b>                 |
| Product component updates | <b>Products</b>                 |
| Exceptions                | <b>Virtual Analyzer Objects</b> |

For details, see the *Trend Micro Apex Central Administrator's Guide*.

## Apex Central Components

**TABLE 8-15. Apex Central Components**

| COMPONENT                                     | DESCRIPTION   |
|---|---|
| Apex Central server                           | The computer upon which the Apex Central application is installed. This server hosts the web-based Apex Central product console   |
| Management Communication Protocol (MCP) Agent | An application installed along with Deep Discovery Email Inspector that allows Apex Central to manage the product. The agent receives commands from the Apex Central server, and then applies them to Deep Discovery Email Inspector. It also collects logs from the product, and sends them to Apex Central. The Apex Central agent does not communicate with the Apex Central server directly. Instead, it interfaces with a component called the Communicator. |
| Entity  | A representation of a managed product (such as Deep Discovery Email Inspector) on the Apex Central console's product directory tree. The product directory tree includes all managed entities.  |

## Registering to Apex Central

### Procedure

1. Go to **Administration > Integrated Products/Services > Apex Central**.
2. Configure **General** settings.
  - View the registration status.

- Specify the display name that identifies Deep Discovery Email Inspector in the Apex Central Product Directory.

**Tip**

Use the host name or specify a unique and meaningful name to help you quickly identify Deep Discovery Email Inspector.

### 3. Configure **Server Settings**.

| OPTION                       | DESCRIPTION   |
|------------------------------|---|
| Server address               | Type the Apex Central server FQDN or IP address.  |
| Port                         | <p>Type the port number that the MCP agent uses to communicate with Apex Central.</p> <p>Select <b>Use HTTPS</b> if the Apex Central security is set to medium or high.</p> <p>Medium: Trend Micro allows HTTPS and HTTP communication between Apex Central and the MCP agent of managed products.</p> <p>High: Trend Micro only allows HTTPS communication between Apex Central and the MCP agent of managed products.</p> |
| User name and password       | Type the logon credentials for the IIS server used by Apex Central if your network requires authentication.   |
| Connect using a proxy server | <p>Optionally select <b>Connect using a proxy server</b>.</p> <p>For details, see <a href="#">Configuring Proxy Settings on page 8-193</a>.</p>   |

4. (Optional) Configure **Incoming Connections from Apex Central** settings.
  - a. Select **Receive connections through a NAT device** to use a NAT device.
  - b. Type the IP address of the NAT device.
  - c. Type the port number.
5. (Optional) Under **Suspicious Object Synchronization**, do the following:
  - a. Select **Synchronize suspicious objects from Apex Central**.

**b.** Type an API Key.



**Note**

Log on to Apex Central to obtain an API key.

---

Deep Discovery Email Inspector synchronizes suspicious object lists from Apex Central every 20 seconds, and displays the time of the last synchronization.



**Attention**

- You can only choose to synchronize suspicious objects with one source. If you enable Deep Discovery Email Inspector to synchronize with Apex Central, you will not receive suspicious objects from any other external sources.
  - If you register Deep Discovery Email Inspector to both Deep Discovery Director 5.0 (or later) and Apex Central, Deep Discovery Email Inspector synchronizes suspicious objects and exception lists from Deep Discovery Director only. You can check the synchronization status on the Deep Discovery Director management console.
  - If you unregister Deep Discovery Email Inspector from Deep Discovery Director and Deep Discovery Email Inspector is still registered to Apex Central, you must configure the settings again to synchronize suspicious objects from Apex Central.
  - If you are using an external sandbox, verify that the external sandbox is configured to send suspicious objects to Apex Central before selecting this option.
- 

**6.** Click **Save**.

---

Deep Discovery Email Inspector registers to Apex Central.

To verify the registration, on Apex Central go to **Directories > Products**.

## Unregistering from Apex Central

---

### Procedure

1. Go to **Administration > Integrated Products/Services > Apex Central**.
2. Under **General**, click the **Unregister** button.



#### Note

Use this option to unregister Deep Discovery Email Inspector from Apex Central. After unregistering, Deep Discovery Email Inspector can register to another Apex Central.

---

Deep Discovery Email Inspector unregisters from Apex Central.

To verify the result, on Apex Central go to **Directories > Products**.

## Deep Discovery Director

Trend Micro Deep Discovery Director is a management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication and log aggregation for Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

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

Deep Discovery Email Inspector supports integration with Deep Discovery Director 5.0 and later versions.

The Deep Discovery Director screen displays the following information:

**TABLE 8-16. Deep Discovery Director Fields**

| FIELD                        | INFORMATION   |
|------------------------------|---|
| Status                       | <p>The following appliance statuses can be displayed:</p> <ul style="list-style-type: none"> <li>• Not registered: The appliance is not registered to Deep Discovery Director.</li> <li>• Registering: The appliance is registering to Deep Discovery Director.</li> <li>• Registered   Connected: The appliance is registered and connected to Deep Discovery Director.</li> <li>• Registered   Unable to connect: The appliance is registered to Deep Discovery Director, but unable to connect. Verify that the Deep Discovery Director network settings are valid.</li> <li>• Registered   Untrusted fingerprint: The appliance is registered to Deep Discovery Director, but the connection was interrupted. To restore the connection, trust the new fingerprint.</li> <li>• Unregistering: The appliance is unregistering from Deep Discovery Director.</li> </ul> |
| Last connected               | The last time this appliance connected to Deep Discovery Director.  |
| Host name                    | The host name of this appliance.  |
| Server address               | The Deep Discovery Director server address.   |
| Port                         | The Deep Discovery Director port.   |
| API key                      | The Deep Discovery Director API key.  |
| Fingerprint (SHA-256)        | The Deep Discovery Director fingerprint.  |
| Connect using a proxy server | Select to use the system proxy settings to connect to Deep Discovery Director.  |

## Deep Discovery Director Registration Considerations

Consider the following when registering to integrate with Deep Discovery Director:

- Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering Deep Discovery Email Inspector to Deep Discovery Director 5.0 (or later), configure Deep Discovery Email Inspector to delete logs when the total free disk space is less than 20%.
- If you register Deep Discovery Email Inspector to both Deep Discovery Director 5.0 (or later) and Apex Central, Deep Discovery Email Inspector synchronizes suspicious objects and exception lists from Deep Discovery Director only. You can check the synchronization status on the Deep Discovery Director management console.
- When Deep Discovery Email Inspector is registered to Deep Discovery Director 5.0 (or later), Deep Discovery Director provides central management of End-User Quarantine settings. After registration is successful, Deep Discovery Email Inspector performs the following actions:
  - Synchronizes YARA rule settings from Deep Discovery Director and overwrites existing YARA rule settings that you have configured
  - Obtains EUQ settings from Deep Discovery Director and prevents manual configuration of EUQ settings on the management console
  - Stops sending EUQ digests
  - Disables EUQ console access

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

## Registering to Deep Discovery Director


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

---


### Procedure

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

2. Configure **Connection Settings**.

| OPTION         | DESCRIPTION   |
|----------------|---|
| Server address | Type the server address for Deep Discovery Director.  |
| Port           | Type the server port number for Deep Discovery Director.<br>The default port number is 443.   |
| API key        | Type the API key for Deep Discovery Director.<br><div> <b>Note</b><br/>You can find this information on the <b>Help</b> screen on the management console of Deep Discovery Director.</div> |

3. (Optional) If you have configured proxy settings for Deep Discovery Email Inspector and want to use these settings for Deep Discovery Director connections, select **Connect using a proxy server**.

 **Note**

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

To update this setting without unregistering from Deep Discovery Director, click **Update Settings**.

4. Click **Register**.

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

**Note**

If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust**.

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

---

**Important**

Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering Deep Discovery Email Inspector to Deep Discovery Director 5.0 (or later), configure Deep Discovery Email Inspector to delete logs when the total free disk space is less than 20%.

For more information, see [Configuring Storage Maintenance on page 8-224](#).

---

## Unregistering from Deep Discovery Director

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

---

### Procedure

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

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

---

## Threat Intelligence Sharing

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



### Note

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

---

## Configuring Threat Intelligence Sharing Settings

---

### Procedure

1. On the Deep Discovery Email Inspector management console, go to **Administration > Integrated Products/Services > Threat Intelligence Sharing**.
2. Select **Enable Threat Intelligence Sharing to allow integrated products/services to obtain information from Deep Discovery Email Inspector**.
3. Under **Criteria**, select the risk level of the objects to be included in the threat intelligence data file.
4. (Optional) By default, Deep Discovery Email Inspector shares threat intelligence data through HTTPS web service. You can also enable HTTP web service for data sharing. Under **Server Settings**, select **Share information using HTTP (in addition to HTTPS)** and specify the HTTP port number.
5. (Optional) Under **Schedule Settings**, select **Enabled** for **Scheduled file generation** and configure the schedule settings.
6. Click **Save**.
7. Click **Generate Now**.

**Note**

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

---

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

## Auxiliary Products/Services

To help provide effective detection and blocking at the perimeter, Deep Discovery Email Inspector can distribute Virtual Analyzer suspicious objects list to auxiliary products and services.

Deep Discovery Email Inspector integrates with the following solutions:

**TABLE 8-17. Solutions that integrate with Deep Discovery Email Inspector**

| NAME  | VERSION            |
|---|--------------------|
| Trend Micro TippingPoint Security Management System (SMS) | SMS 5.3 or 5.4     |
| Check Point Open Platform for Security (OPSEC)            | Check Point R80.10 |
| IBM Security Network Protection (XGS)                     | XGS 5.2            |
| Palo Alto Panorama  | PAN-OS 7.0.1       |
| Palo Alto Firewalls                                       | PAN-OS 4.1.0       |

**Note**

- Deep Discovery Email Inspector supports only one auxiliary product/service at a time.
- Deep Discovery Email Inspector does not synchronize user-defined suspicious objects with supported auxiliary products and services.
- When enabled, Deep Discovery Email Inspector distributes the list of selected suspicious object types every 10 minutes.

---

## Trend Micro TippingPoint Security Management System (SMS)

Both Deep Discovery Email Inspector and Apex Central can send suspicious objects to Trend Micro TippingPoint SMS. Deep Discovery Email Inspector sends each suspicious object with the following optional information:

- Risk level: Severity of each suspicious object attempt
- Product Name: Trend Micro Deep Discovery Email Inspector (not configurable)
- Appliance Host Name: Trend Micro Deep Discovery Email Inspector host name (not configurable)

Trend Micro TippingPoint SMS uses reputation filters to apply block, permit, or notify actions across an entire reputation group. For more information about reputation filters, refer to your Trend Micro TippingPoint documentation.

## Configuring Trend Micro TippingPoint Security Management System (SMS)

---

### Procedure

1. On the Deep Discovery Email Inspector management console, go to **Administration > Integrated Products/Services > Auxiliary Products/Services**.
2. Select **Trend Micro TippingPoint Security Management System (SMS)**.

3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, provide the following information:

- Server name

**Note**

The server name must be the FQDN or IPv4 address of the auxiliary product.

---

- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-18. Valid Character Sets**

|                | USER NAME     | PASSWORD      |
|----------------|---------------|---------------|
| Minimum length | 1 character   | 1 character   |
| Maximum length | 15 characters | 15 characters |

5. (Optional) Click **Test Connection**.
6. To send object information from Deep Discovery Email Inspector to this product/service, configure the following criteria:

- Object type:
  - Suspicious Object
    - IPv4 address
    - Domain

**Note**

You must select at least one object.

---

- Risk level:
  - High only
  - High and medium

- High, medium, and low

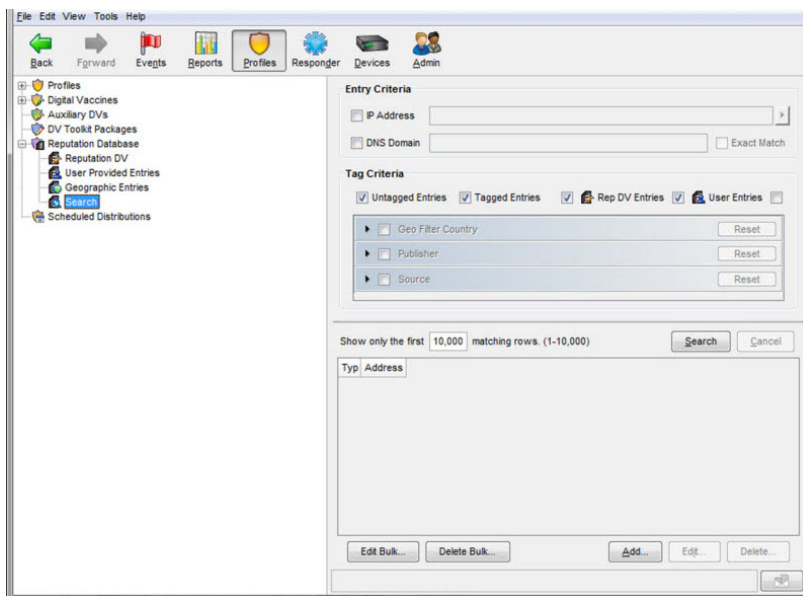
7. Click **Save**.

The following table displays the mappings between the data columns in Deep Discovery Email Inspector and the tag categories in the TippingPoint reputation database.

**TABLE 8-19. Tag categories added to the reputation database**

| COLUMN              | TAG CATEGORY                   |
|---------------------|--------------------------------|
| Product Name        | Trend Micro Publisher          |
| Appliance Host Name | Trend Micro Source             |
| Object Type         | Trend Micro Detection Category |
| Risk Level          | Trend Micro Severity           |

8. (Optional) To view distributed suspicious objects in Trend Micro TippingPoint SMS, do the following:
- On the **Profile** tab, go to **Reputation Database > Search**.



- b. On the **Entry Criteria** screen, type search parameters and then click **Search**.

Suspicious objects distributed by Deep Discovery Email Inspector are displayed.

## Check Point Open Platform for Security (OPSEC)

Check Point Open Platform for Security (OPSEC) manages network security through an open, extensible management framework.

Deep Discovery Email Inspector integrates with Check Point OPSEC via the Suspicious Activities Monitoring (SAM) API.

The SAM API implements communications between the SAM client (Deep Discovery Email Inspector) and the Check Point firewall, which acts as a SAM Server. Deep Discovery Email Inspector uses the SAM API to request that the Check Point firewall take specified actions for certain connections.

For example, Deep Discovery Email Inspector may ask Check Point OPSEC to block a connection with a client that is attempting to issue illegal commands or repeatedly failing to log on.

## Configuring Check Point Open Platform for Security (OPSEC)

---

### Procedure

1. On the Deep Discovery Email Inspector management console, go to **Administration > Integrated Products/Services > Auxiliary Products/Services**.
2. Select **Check Point Open Platform for Security (OPSEC)**.
3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, select a connection type.



#### Note

Ensure that your network configuration allows Deep Discovery Email Inspector to connect to the Check Point appliance.

Deep Discovery Email Inspector may connect to the Check Point appliance through the secured connection port or clear connection port that is configured on the Check Point appliance. Deep Discovery Email Inspector also pulls the certificate from the Check Point appliance through port 18210.

If you selected **Secured connection**, the **OPSEC application name** and **SIC one-time password** settings appear.

5. Type a server name.



#### Note

The server name must be the FQDN or IPv4 address of the auxiliary product.

6. If you selected **Secured connection**, type the **OPSEC application name** and **SIC one-time password**.

For more details, see [Configuring a Secured Connection on page 8-153](#).

**Note**

If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

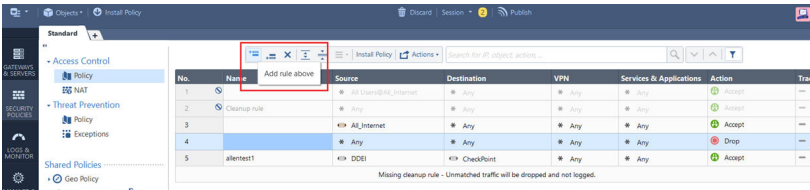
- 
7. Type the port.


**Note**

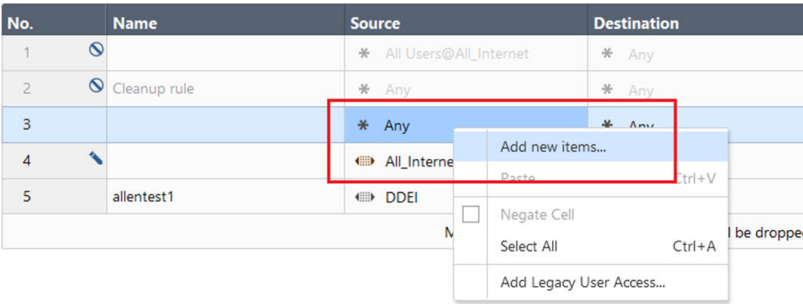
This port must be the same port that is configured on the security gateway. For details, see [Preconfiguring a Security Gateway on page 8-151](#).

- 
8. (Optional) Click **Test Connection**.
9. To send object information from Deep Discovery Email Inspector to this product/service, configure the following criteria:
- Object type:
    - Suspicious Object
    - IPv4 address
  - Risk level:
    - High only
    - High and medium
    - High, medium, and low
10. Click **Save**.
11. On your Check Point firewall appliance, preconfigure a security gateway. For details see [Preconfiguring a Security Gateway on page 8-151](#).

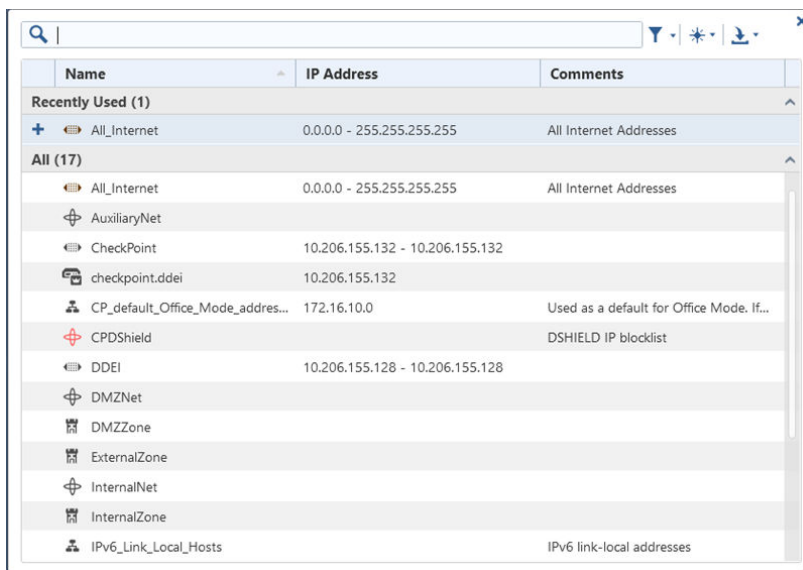
12. Go to Check Point SmartConsole and do the following to configure your Check Point appliance for deploying suspicious objects from Deep Discovery Email Inspector:
- a. On the **SECURITY POLICIES** tab, go to **Access Control > Policy**.



- b. To add a rule, click the **Add rule above**  icon.
- c. To configure the new policy, right-click the action.
- d. Change the action to **Accept**.
- e. Right-click the source.

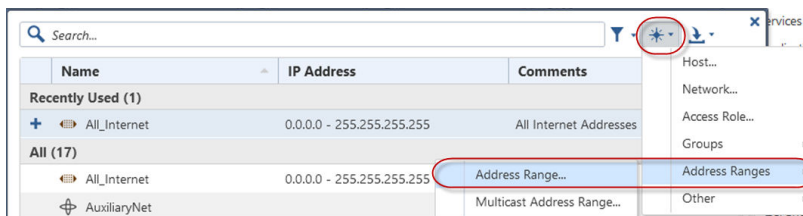


- f. Select **Add new items....**
- The following screen appears.



| Name                             | IP Address                      | Comments                                 |
|----------------------------------|---------------------------------|--|
| <b>Recently Used (1)</b>         |                                 |  |
| All_Internet                     | 0.0.0.0 - 255.255.255.255       | All Internet Addresses                   |
| <b>All (17)</b>                  |                                 |  |
| All_Internet                     | 0.0.0.0 - 255.255.255.255       | All Internet Addresses                   |
| AuxiliaryNet                     |                                 |  |
| CheckPoint                       | 10.206.155.132 - 10.206.155.132 |  |
| checkpoint.ddei                  | 10.206.155.132                  |  |
| CP_default_Office_Mode_addres... | 172.16.10.0                     | Used as a default for Office Mode. If... |
| CPDShield                        |                                 | DSHIELD IP blocklist                     |
| DDEI                             | 10.206.155.128 - 10.206.155.128 |  |
| DMZNet                           |                                 |  |
| DMZZone                          |                                 |  |
| ExternalZone                     |                                 |  |
| InternalNet                      |                                 |  |
| InternalZone                     |                                 |  |
| IPv6_Link_Local_Hosts            |                                 | IPv6 link-local addresses                |

- g. Click the new icon (✱).



| Name                     | IP Address                | Comments               |
|--------------------------|---------------------------|------------------------|
| <b>Recently Used (1)</b> |                           |                        |
| All_Internet             | 0.0.0.0 - 255.255.255.255 | All Internet Addresses |
| <b>All (17)</b>          |                           |                        |
| All_Internet             | 0.0.0.0 - 255.255.255.255 |                        |
| AuxiliaryNet             |                           |                        |

- h. Select **Address Ranges > Address Range....**

The **New Address Range** window appears.

New Address Range

Enter Object Name

Enter Object Comment

General

NAT

IPv4

First IP address:

Last IP address:

IPv6

First IPv6 address:

Last IPv6 address:

Add Tag

OK Cancel

- i. In the **Enter Object Name** field, type **DDEI**.
- j. In **First IP address**, type the Deep Discovery Email Inspector IP address.
- k. In **Last IP address**, type the Deep Discovery Email Inspector IP address.
- l. Click **OK**.
- m. Right-click the destination.

- n. Select **Add new items....**
- o. Click the new icon ( \* ).
- p. Select **Address Ranges > Address Range....**

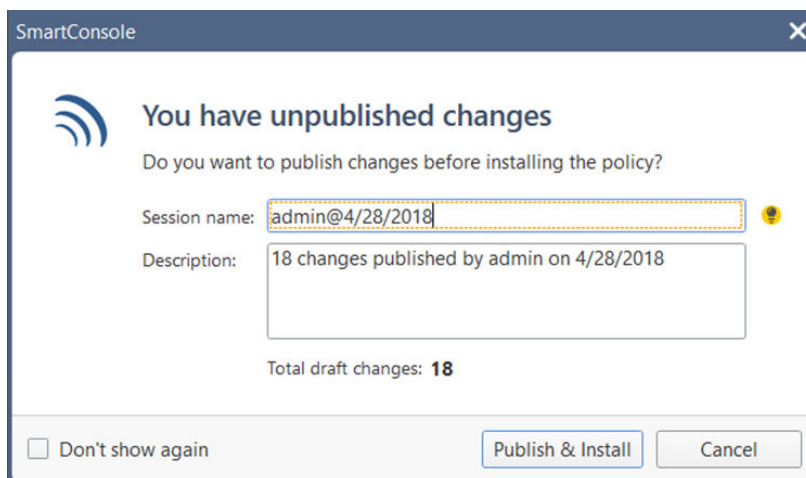
The **New Address Range** window appears.

The screenshot shows the 'New Address Range' window. At the top, there's a title bar with 'New Address Range' and standard window controls. Below the title bar, there's a section for 'Enter Object Name' with a dotted border and a sub-label 'Enter Object Comment'. To the left of this section is a grid icon. Below this section, there's a 'General' tab with a 'NAT' sub-tab. The 'IPv4' section has fields for 'First IP address' and 'Last IP address'. The 'IPv6' section has fields for 'First IPv6 address' and 'Last IPv6 address'. At the bottom of the main area is an 'Add Tag' button. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- q. In the **Enter Object Name** field, type **CheckPoint**.
- r. In **First IP address**, type the CheckPoint IP address.
- s. In **Last IP address**, type the CheckPoint IP address.

- t. Click **OK**.
- u. Click **Install Policy**.

The following window opens.



- v. Click **Publish & Install**.

The target gateway installs.

- w. Click **Install**.

The Check Point appliance is enabled to receive suspicious objects from Deep Discovery Email Inspector.

13. On the Deep Discovery Email Inspector management console, configure the following criteria to send suspicious object information from Deep Discovery Email Inspector to this product/service:
  - Object type:
    - Suspicious Object
    - IPv4 address
  - Risk level:

- High only
- High and medium
- High, medium, and low

14. Under **Advanced Settings**, click one of the following actions:

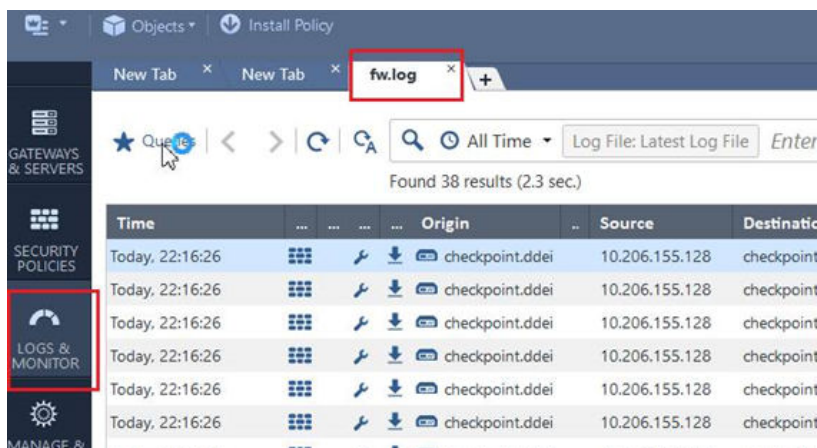
- **Reject:** Packets will be rejected and a notification sent to the communicating peer that the packet has been rejected.
- **Drop:** Packets will be dropped without sending the communicating peer a notification.
- **Notify:** A notification about the defined activity will be sent but the activity will not be blocked.

15. Click **Save**.

16. (Optional) Click **Distribute Now** to distribute suspicious objects to Check Point immediately.

17. To view suspicious objects distributed by Deep Discovery Email Inspector on Check Point SmartView Monitor, do the following:

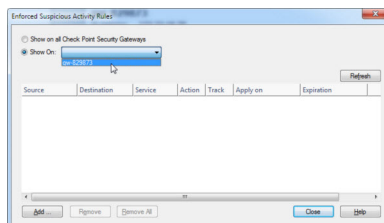
- On Check Point SmartConsole, go to **Logs & Monitor**.
- Add a new tab.



- c. Click **Tunnels & User Monitoring** to open SmartView Monitor.
- d. Click the **Launch Menu** icon and go to **Tools > Suspicious Activity Rules**.

The **Enforced Suspicious Activity Rules** window opens.

- e. At **Show On**, select the target Check Point appliance name.



- f. Click **Refresh**.

Suspicious objects distributed by Deep Discovery Email Inspector are displayed.

## Preconfiguring a Security Gateway

### Procedure

1. Log on to your Check Point appliance.



- 
2. (Optional) Set a password for expert mode.
3. Type the password to enter expert mode.

```
gw-b8810> expert
Enter expert password:

Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@gw-b8810:0]# vi /var/opt/CPsuite-R80/fw1/conf/fwopsec.conf _
```

- 
- 
- 
4. Use the vi editor to open /var/opt/CPsuite-R80/fw1/conf/fwopsec.conf.

```
% To change the default setting of an entry:
% a. Remove the comment sign (#) at the beginning of the line.
% b. Change the port number.

% The Security Gateway/Management default settings are:
%
sam_server auth_port 10103
sam_server port 0
lea_server auth_port 10104
lea_server port 0
sla_server auth_port 10107
sla_server port 0
cpul_server auth_port 10190
aaa_server auth_port 15151
aaa_server port 0
```

**Note**

The image of the default configuration is for reference only. The actual file contents may vary.

---

- 
- 
- 
- 
5. In fwopsec.conf, configure the SAM communication mode ports using one of the following options:
  - Secured connection (default port)
    - No changes in fwopsec.conf are necessary. The default port 18183 is used for the **sam\_server auth\_port** setting.

**Note**

On Deep Discovery Email Inspector, verify that the **Check Point Open Platform for Security (OPSEC) Port** setting at **Administration > Integrated Products/Services > Auxiliary Products/Services** is also 18183.

---

- Secured connection (user-defined port)
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server_auth_port: 18183` and then change the port number.

**Note**

Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Email Inspector at **Administration > Integrated Products/Services > Auxiliary Products/Services**.

---

- Clear connection (user-defined port)
  - In `fwopsec.conf`, remove the comment sign (#) from `sam_server_port: 0` and then change the port number.

**Note**

Configure the same port in `fwopsec.conf` and in the **Check Point Open Platform for Security (OPSEC) Port** setting on Deep Discovery Email Inspector at **Administration > Integrated Products/Services > Auxiliary Products/Services**.


---

6. If changes were made to the `fwopsec.conf` file, save the `fwopsec.conf` file and restart your Check Point appliance.
- 

## Configuring a Secured Connection

---

### Procedure

1. Open the Check Point SmartConsole and click the main menu icon ()
2. Go to **New object > More object types > Server > OPSEC Application > New Application....**

The **OPSEC Application Properties** window appears.

The screenshot shows the 'OPSEC Application Properties' dialog box. It has a title bar with a question mark and a close button. The 'General' tab is selected. The 'Name' field is empty. The 'Comment' field is empty. The 'Color' dropdown is set to 'Black'. The 'Host' dropdown is empty, and there is a 'New...' button next to it. Below these is a section for 'Application properties' with a 'Vendor' dropdown set to 'User defined', a 'Product' dropdown, and a 'Version' dropdown. There is an 'Activate...' button. Below this are two sections: 'Server Entities' with checkboxes for 'CVP', 'UFP', and 'AMON'; and 'Client Entities' with checkboxes for 'ELA', 'LEA', 'SAM', 'CPMI', 'OMI', and 'UAA'. At the bottom is a 'Secure Internal Communication' section with a 'Communication...' button and a 'DN:' field. The 'OK' and 'Cancel' buttons are at the bottom right.

OPSEC Application Properties

General

Name:

Comment:

Color:

Host:

Application properties

Vendor:

Product:  Version:

Server Entities

☐ CVP  
☐ UFP  
☐ AMON

Client Entities

☐ ELA  
☐ LEA  
☐ SAM  
☐ CPMI  
☐ OMI  
☐ UAA

Secure Internal Communication

DN:

---

3. Type a **Name**.



**Note**

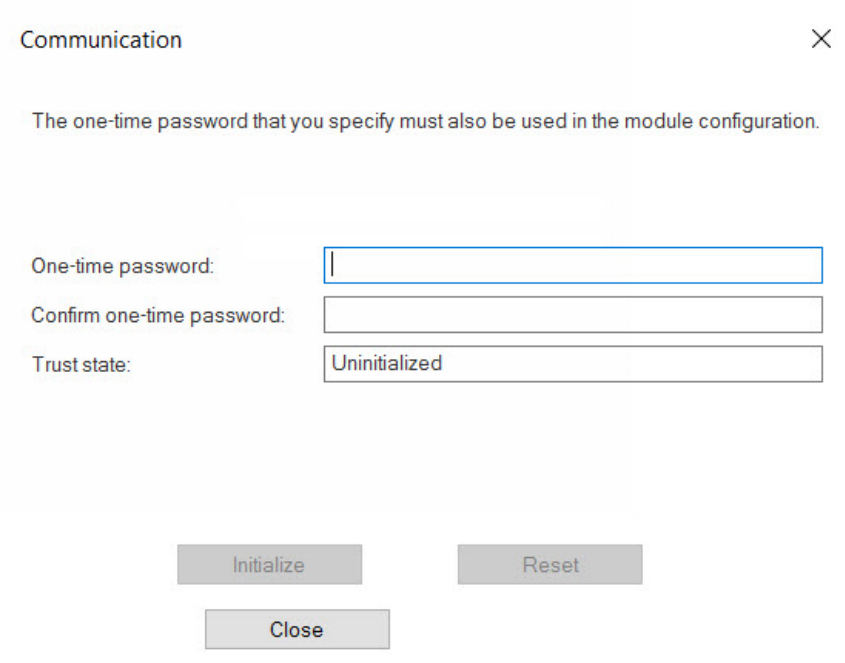
- Use this name as the **OPSEC application name** in Deep Discovery Email Inspector.
  - The application name must be less than 101 characters, start with an English alphabetical letter, and contain only English alphabetical letters, periods, underscores, or dashes.
- 

4. Select a **Host**.

5. Under **Client Entities**, select **SAM**.

6. Click **Communication....**

The **Communication** window appears.



Communication

The one-time password that you specify must also be used in the module configuration.

One-time password:

Confirm one-time password:

Trust state:

Initialize Reset Close

7. Type a password in **One-time password** and type the same password in **Confirm one-time password**.

**Note**

Use this password as the **SIC one-time password** in Deep Discovery Email Inspector.


**Note**

If the one-time password is reset on the Check Point appliance, the new one-time password must be different than the previous one-time password.

8. Click **Initialize**.

The **Trust state** becomes **Initialized but trust not established**.

9. Install the user definition.

- a. In the **Check Point SmartConsole** main window, click  and select **Install database....**

The **Install database** window appears.

- b. Choose the installation components and then click **OK**.

The user definition starts installing.

---

## IBM Security Network Protection

IBM Security Network Protection (XGS), provides a web services API that enables third-party applications such as Deep Discovery Email Inspector to directly submit suspicious objects. IBM XGS can perform the following functions:

- Quarantine hosts infected with malware
- Block communication to C&C servers
- Block access to URLs found to be distributing malware

To integrate Deep Discovery Email Inspector with IBM XGS, configure a generic agent to do the following:

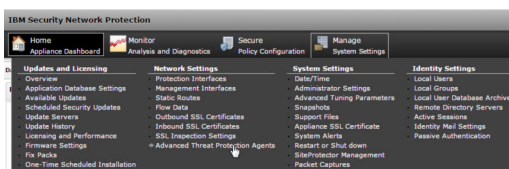
- Accept alerts that adhere to a specific schema
- Create quarantine rules based on a generic ATP translation policy

The ATP translation policy allows several categories of messages to take different actions on IBM XGS, including blocking and alerting.

## Configuring IBM Security Network Protection

### Procedure

1. On the IBM XGS console, do the following to configure the generic agent:
  - a. Go to **Manage System Settings > Network Settings > Advanced Threat Protection Agents**.

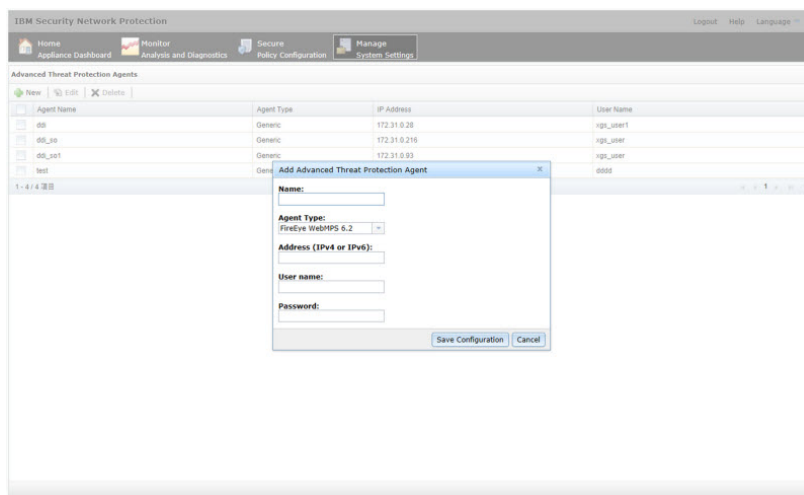


The **Advanced Threat Protection Agents** window opens.

- b. Click **New**.
- c. Provide the following information:
  - Name: Type a name
  - Agent Type: Select **Generic**
  - Address: Deep Discovery Email Inspector management port IP address in IPv4 or IPv6 format
  - User name: Existing authentication credential
  - Password: Existing authentication credential

**TABLE 8-20. Valid Character Sets**

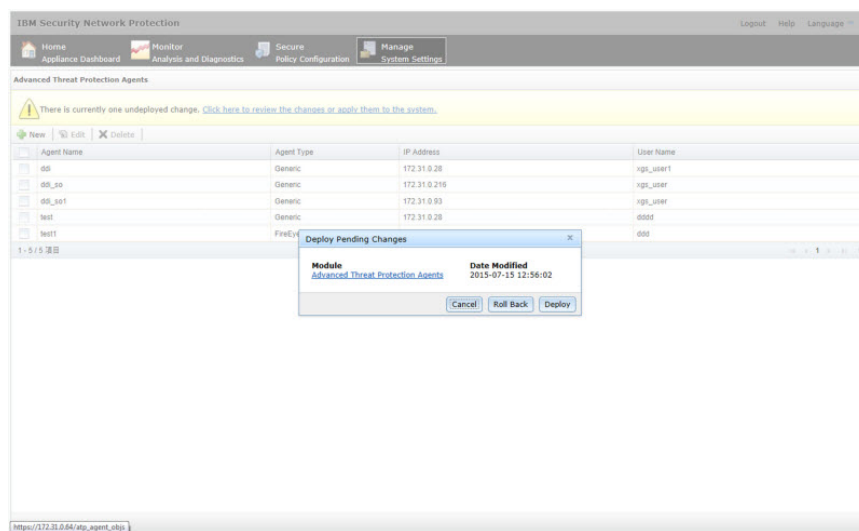
|                | USER NAME     | PASSWORD      |
|----------------|---------------|---------------|
| Minimum length | 1 character   | 1 character   |
| Maximum length | 15 characters | 15 characters |



2. Click **Save Confirmation**.

The **Deploy Pending Changes** window opens.

3. To apply changes to IBM XGS, click **Deploy**.



The new agent appears in the **Advanced Threat Protection Agents** list.

4. On the Deep Discovery Email Inspector management console, go to **Administration > Integrated Products/Services > Auxiliary Products/Services**.
5. Select **Configuring IBM Security Network Protection (XGS)**.
6. Under **Object Distribution**, select **Enable**.
7. Under **Server Settings**, provide the following information:
  - Server name



**Note**

The server name must be the FQDN or IPv4 address of the auxiliary product.

- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-21. Valid Character Sets**

|                | USER NAME     | PASSWORD      |
|----------------|---------------|---------------|
| Minimum length | 1 character   | 1 character   |
| Maximum length | 15 characters | 15 characters |

8. (Optional) Click **Test Connection**.
9. To send object information from Deep Discovery Email Inspector to this product/service, configure the following criteria:
  - Object type:
    - Suspicious Object
      - IPv4 address
      - URL

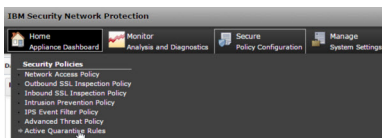
**Note**

You must select at least one object.

- Risk level:
  - High only
  - High and medium
  - High, medium, and low

10. Click **Save**.

11. (Optional) On the IBM XGS console, go to **Secure Policy Configuration > Security Policies > Active Quarantine Rules** to view suspicious objects and C&C callback addresses sent by Deep Discovery Email Inspector to IBM XGS.

**Note**

Suspicious objects with a low risk level do not appear in the IBM XGS **Active Quarantine Rules**. To view all suspicious objects sent by Deep Discovery Email Inspector, go to **Security Policy Configuration > Advanced Threat Policy** and specify the following settings:

- **Agent Type: Generic**
- **Alert Type: Reputation**
- **Alert Severity: Low**

Suspicious objects and C&C callback addresses distributed by Deep Discovery Email Inspector are displayed.

## Palo Alto Panorama or Firewalls

Palo Alto Networks® firewalls identify and control applications, regardless of port, protocol, encryption (SSL or SSH) or evasive characteristics.

Panorama™ is a centralized policy and device management system that allows administrators to control Palo Alto Networks firewalls.

Deep Discovery Email Inspector can send IPv4, domain, and URL suspicious objects to the URL category of Palo Alto Firewall or Palo Alto Panorama™ as match criteria allow for exception-based behavior.

Use URL categories in policies as follows:

- Identify and allow exceptions to general security policies for users who belong to multiple groups within Active Directory

Example: Deny access to malware and hacking sites for all users, while allowing access to users that belong to the security group.

- Allow access to streaming media category, but apply quality of service policies to control bandwidth consumption
- Prevent file download and upload for URL categories that represent higher risks

Example: Allow access to unknown sites, but prevent upload and download of executable files from unknown sites to limit malware propagation.

- Apply SSL decryption policies that allow encrypted access to finance and shopping categories, but decrypt and inspect traffic to all other URL categories.

## Configuring Palo Alto Panorama and Firewalls

---

### Procedure

1. On the Deep Discovery Email Inspector management console, go to **Administration > Integrated Products/Services > Auxiliary Products/Services**.

2. Select **Palo Alto Panorama or Firewalls**.
3. Under **Object Distribution**, select **Enable**.
4. Under **Server Settings**, provide the following information:
  - Server name

**Note**

The server name must be the FQDN or IPv4 address of the auxiliary product.

---

- Server type
- User name: Existing authentication credential
- Password: Existing authentication credential

**TABLE 8-22. Valid Character Sets**

|                | USER NAME     | PASSWORD      |
|----------------|---------------|---------------|
| Minimum length | 1 character   | 1 character   |
| Maximum length | 15 characters | 15 characters |

5. (Optional) Click **Test Connection**.
6. To send object information from Deep Discovery Email Inspector to this product/service, configure the following criteria:
  - Object type:
    - Suspicious Object
      - URL
      - IPv4 address
      - Domain

**Note**

You must select at least one object.

---

- Risk level:
  - High only
  - High and medium
  - High, medium, and low
- 7. (Optional) Under **Advanced Settings**, customize URL category names:

URL category names must include a minimum of one character and a maximum of 31 characters, and may include the following characters:

  - Uppercase (A-Z)
  - Lowercase (a-z)
  - Numeric (0-9)
  - Special characters: - \_
  - Space
- 8. Click **Save**.
- 9. (Optional) To view suspicious objects sent by Deep Discovery Email Inspector on the Palo Alto product console, go to **Objects > Custom URL Category** (or **Objects > Custom Objects > URL Category**).



Suspicious objects distributed by Deep Discovery Email Inspector are displayed.

---

## LDAP

Deep Discovery Email Inspector integrates with an LDAP server for user-group definition and administrator privileges.

Deep Discovery Email Inspector supports the following types of directory servers:

- Microsoft Active Directory on Windows Server 2016 and 2019
- Microsoft AD Global Catalog on Windows Server 2016 and 2019
- IBM Domino V9 and V10
- OpenLDAP

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

| TASK                              | DESCRIPTION  |
|-----------------------------------|--|
| Add an LDAP server                | Click <b>Add</b> to add a new directory server.<br><br>Deep Discovery Email Inspector supports up to ten directory servers.<br><br>For more information, see <a href="#">Configuring an LDAP Server on page 8-166</a> .                      |
| Edit an LDAP server               | Click a server name to edit the settings.<br><br>For more information, see <a href="#">Configuring an LDAP Server on page 8-166</a> .  |
| Enable or disable an LDAP server  | Toggle the button in the <b>Status</b> column to: <ul style="list-style-type: none"><li>• Enable the LDAP server that you selected to enable on the configuration screen</li><li>• Disable both primary and secondary LDAP servers</li></ul> |
| Synchronize directory information | Click <b>Sync All</b> to synchronize directory information with all the LDAP servers.  |
| Delete a directory server         | Click <b>Delete</b> to remove one or more selected entries.  |

## Configuring an LDAP Server

---

### Procedure

1. Obtain the information required to configure LDAP integration from the server administrator.
2. Go to **Administration > Integrated Products/Services > LDAP**.
3. Do one of the following:
  - Click **Add** to add a new entry.
  - Click a name to change the server settings.
4. Select a server type.
5. Select to enable one or both primary and secondary servers.
6. Configure the server settings (server address, access protocol, and port number).



### Note

Trend Micro recommends using the following default ports:

- For Microsoft Active Directory, Domino, or OpenLDAP:
  - **SSL:** 636
  - **STARTTLS:** 389
- For Microsoft AD Global Catalog:
  - **SSL:** 3269
  - **STARTTLS:** 3268

- 
7. Configure administrative settings for the LDAP server.

The following table provides the configuration recommendations for each supported LDAP server type.

| LDAP SERVER TYPE                   | USER ACCOUNT<br>(EXAMPLE)       | BASE<br>DISTINGUISHED<br>NAME (EXAMPLE)   | AUTHENTICATION<br>METHOD   |
|------------------------------------|---------------------------------|---|--|
| Active Directory                   | user1@domain.com<br>(UPN)       | dc=domain, dc=com   | <ul style="list-style-type: none"> <li>• Simple</li> <li>• Advanced (with Kerberos)</li> </ul> |
| Active Directory<br>Global Catalog | user1@domain.com<br>(UPN)       | dc=domain, dc=com<br>dc=domain1, dc=com<br>(if multiple<br>unique domains<br>exist) | <ul style="list-style-type: none"> <li>• Simple</li> <li>• Advanced (with Kerberos)</li> </ul> |
| OpenLDAP                           | cn=manager,<br>dc=test1, dc=com | dc=test1, dc=com  | Simple   |
| IBM Domino                         | user1/domain                    | Not applicable  | Simple   |

- a. Type the base distinguished name.
  - b. Select an email address attribute option to apply policy settings based on the address information.
  - c. Type the user name.
  - d. Type the password.
  - e. (Optional) If your organization uses a CA certificate, select **Use CA certificate** and click **Select** to locate the CA certificate file.
  - f. In the Authentication Method section, select **Simple** or **Advanced**.  
For Active Directory, select **Advanced** and configure the required settings.
8. (Optional) Click **Test Connection** to verify that a connection to the LDAP server can be established using the specified information.
  9. Click **Save**.

## SAML Integration

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

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

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

- Microsoft Active Directory Federation Services (AD FS) 4.0 or 5.0
- Okta
- To connect Deep Discovery Email Inspector to your organization environment for single-sign-on, complete the following:
  1. Access the Deep Discovery Email Inspector management console to obtain the service provider metadata file.

For more information, see [Service Provider Metadata and Certificate on page 8-169](#).
  2. In your identity provider:
    - a. Configure the required settings for single sign-on.
    - b. Obtain the federation metadata file.

For more information, see [Configuring Active Directory Federation Services on page 8-173](#) and [Configuring Okta on page 8-170](#).

### 3. In Deep Discovery Email Inspector:

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

For more information, see [Configuring Identity Provider Settings on page 8-170](#).

- b. Create SAML user groups.

For more information, see [SAML Groups on page 8-215](#).

## Service Provider Metadata and Certificate

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

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

- **Entity ID:** Identifies the service provider application
- **Single Sign On URL:** The endpoint URL responsible for receiving and parsing a SAML assertion (also referred to as "Assertion Consumer Service")
- **Single Sign Off URL:** The endpoint URL responsible for initiating the SAML logout process
- **Certificate:** The encryption certificate (verification certificate) in X.509 format

You can click the following in the Service Provide section:

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

Deep Discovery Email Inspector supports certificates in X.509 PEM format.

## Configuring Identity Provider Settings

---



### Note

- Before you add an identity provider, obtain the federation metadata file from your identity provider.
  - You can add up to four identity providers in Deep Discovery Email Inspector, two for the management console and two for the EUQ console.
- 

### Procedure

1. Go to **Administration > Integrated Products/Services > SAML Authentication**.
2. In the Identity Provider section, do one of the following:
  - Click **Add** to add a new entry.
  - Click an identity provider name to change the settings.
3. Select a status option to enable or disable the identity provider settings.
4. Type a descriptive name for the identity provider.
5. Type a description.
6. Click **Select** and choose the federation metadata file obtained from your identity provider.

After importing the federation metadata file, the system displays the identity provider information.

7. Click **Save**.
- 

## Configuring Okta

Okta is a standards-compliant OAuth 2.0 authorization server that provides cloud identity solutions for your organization. Okta is a single sign-on

provider that allows you to manage user access to Deep Discovery Email Inspector.

This section describes how to configure Okta as a SAML (2.0) identity provider for Deep Discovery Email Inspector to use.

Before you begin configuring Okta, make sure that:

- You have a valid subscription with Okta that handles the sign-in process and that eventually provides the authentication credentials to the Deep Discovery Email Inspector management console.
- You are logged on to the management console as a Deep Discovery Email Inspector administrator.

---

## Procedure

1. Log in to your Okta organization as a user with administrative privileges.
2. Click **Admin** in the upper right, and then navigate to **Applications > Applications**.
3. Click **Add Application**, and then click **Create New App**.  
The **Create a New Application Integration** screen appears.
4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.
5. On the **General Settings** screen, type a name for Deep Discovery Email Inspector in **App name**, for example, "Deep Discovery Email Inspector", and click **Next**.
6. On the **Configure SAML** screen, specify the following:
  - a. Type the Deep Discovery Email Inspector address in the **Single sign on URL** field.
  - b. Select **Use this for Recipient URL and Destination URL**.
  - c. Specify the Audience URI in **Audience URI (SP Entity ID)** based on your serving site:

- d. For **Assertion Encryption**, select **Encrypted**.
- e. For **Encryption Certificate**, click **Browse files** to select the certificate file that you obtained from Deep Discovery Email Inspector.

For more information, see [Service Provider Metadata and Certificate on page 8-169](#).

- f. (Optional) In the **ATTRIBUTE STATEMENTS (OPTIONAL)** section, specify the following for EUQ console access on Deep Discovery Email Inspector:
  - **Name:** The value configured on Deep Discovery Email Inspector.

**Note**

Make sure you specify the same claim value for an email address in your identity provider and Deep Discovery Email Inspector.

---

- **Value:** The name of specified attribute
- g. In the **Group Attribute Statements (Optional)** section, specify the following:
    - **Name:** DDEI\_GROUP
    - **Filter:** Matches regex `^(.*)*$`
  - h. Click **Next**.

- 7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, select **This is an internal app that we have created**, and then click **Finish**.

The **Sign On** tab of your newly created Deep Discovery Email Inspector application appears.

- 8. Click **Identity Provider Metadata** to download the metadata file from Okta.

**Note**

Import this metadata file to Deep Discovery Email Inspector.

---

9. Assign the application to groups and add people to groups.

- a. Select **Directory > Groups**.
- b. Click the groups that you want to assign the application to, and then click **Manage Apps**.

The **Assign Applications** screen appears.

- c. Locate Deep Discovery Email Inspector you added and click **Assign**.
- d. Click **Manage People**.

The **Add People to Groups** screen appears.

- e. Locate the user you want to allow access to Deep Discovery Email Inspector and add the user to the Deep Discovery Email Inspector group.
- f. Confirm that the application is assigned to the user and group.

After assigning an application to a group, the system automatically assigns the application to all users in the group.

- g. Repeat the above steps to assign the application to more groups as necessary.

You are now ready to configure Okta for single sign-on and create the required SAML groups in the Deep Discovery Email Inspector management console.

---

## Configuring Active Directory Federation Services

This section describes how to configure a federation server using Active Directory Federation Services (AD FS) to work with Deep Discovery Email Inspector.

**Note**

Deep Discovery Email Inspector supports connecting to the federation server using AD FS 4.0 and 5.0.

---

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

Before you begin configuring AD FS, make sure that:

- You have a Windows Server installed with AD FS 4.0 or AD FS 5.0 to serve as a federation server.
  - You are logged on to the management console as a Deep Discovery Email Inspector administrator.
  - You have obtained the metadata file from Deep Discovery Email Inspector.
- 

**Procedure**

1. Go to **Start > All Programs > Administrative Tools** to open the AD FS management console.
2. Click **AD FS** in the left navigation, and under the **Action** area on the right, click **Add Relying Party Trust...**
3. Complete settings on each tab of the **Add Relying Party Trust Wizard** screen.
  - a. On the **Welcome** tab, select **Claims aware** and click **Start**.
  - b. On the **Select Data Source** tab, select **Import data about the relying party from a file**, click **Browse** to select the metadata file you obtain from Deep Discovery Email Inspector; then, click **Next**.
  - c. On the **Specify Display Name** tab, specify a display name for Deep Discovery Email Inspector, for example, "Deep Discovery Email Inspector", and click **Next**.

- d. On the **Choose Access Control Policy** tab, select **Permit everyone** or **Permit specific group**. If you select **Permit specific group**, select one or more groups in **Policy**. Then, click **Next**.
- e. On the **Ready to Add Trust** tab, click **Next**.
- f. On the **Finish** tab, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** and click **Close**.

The **Edit Claim Rules** screen appears.

- 4. On the **Issuance Transform Rules** tab, click **Add Rule...**
- 5. Complete settings on each tab of the **Add Transform Claim Rule Wizard** screen to configure the claim rules for the LDAP attributes listed in the following table.
  - a. On the **Choose Rule Type** tab, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list, and click **Next**.
  - b. On the **Configure Claim Rule** tab, specify a claim rule name in the **Claim rule name** text box, and select **Active Directory** from the **Attribute store** drop-down list.
  - c. Select the **User-Principal-Name** LDAP attribute and specify **Name ID** as the outgoing claim type for the attribute.
  - d. Click **OK**.

**TABLE 8-23. LDAP attributes**

| WEB CONSOLE | LDAP ATTRIBUTE      | OUTGOING CLAIM TYPE | REQUIRED |
|-------------|---------------------|---------------------|----------|
| Management  | User-Principal-Name | Name ID             | Yes      |
| EUQ         | User-Principal-Name | Name ID             | Yes      |

| WEB CONSOLE | LDAP ATTRIBUTE   | OUTGOING CLAIM TYPE                                       | REQUIRED |
|-------------|------------------|---|----------|
| EUQ         | E-Mail-Addresses | <user-defined value><br><br>For example, EUQ_Email.       | No       |
| EUQ         | Proxy-Addresses  | <user-defined value><br><br>For example, EUQ_PROXY_Email. | No       |

6. Configure settings for each AD group that you permitted in step 3d and customize the settings based on your requirements.

**Note**

Make sure you set the outgoing claim type as `DDEI_GROUP`.

- a. Click **Add Rule....**


The **Add Transform Claim Rule Wizard** screen appears.

- b. On the **Choose Rule Type** tab, select **Send Group Membership as a Claim** from the **Claim rule template** drop-down list, and click **Next**.

The **Configure Claim Rule** tab appears.

- c. For **Claim rule name**, type the name of the AD group.
- d. For **User's group**, click **Browse** and then select the AD group.
- e. For **Outgoing claim type**, type "`DDEI_GROUP`".
- f. For **Outgoing claim value**, type the name of the AD group.
- g. Click **Apply** and then click **OK**.

TABLE 8-24. Group membership rules

| CLAIM RULE NAME          | USER GROUP                | OUTGOING CLAIM TYPE | OUTGOING CLAIM VALUE   |
|--------------------------|---------------------------|---------------------|--|
| <user-defined rule name> | <user group name in ADFS> | DDEI_GROUP          | <user-defined value> <div><b>Note</b><br/>This value must be the same as the SAML group name you configure on Deep Discovery Email Inspector.</div> |

7. Click **Apply** and then **OK**.

Configuring Endpoints for Single Sign-on through AD FS

Before endpoints can access Deep Discovery Email Inspector using single sign-on through Active Directory Federation Services (AD FS), configure the web browser settings on each endpoint to trust both Deep Discovery Email Inspector and the federation server.

You can configure the web browser settings on endpoints manually or through group policies.

The following provides the procedure for endpoints running Windows 10. Steps may vary depending on the Windows version.

---

## Procedure

1. On an endpoint, open the **Control Panel** from the Start menu.
  2. Click **Network and Internet > Internet Options**.  
The Internet Properties screen appears.
  3. Click the **Security** tab.
  4. Select **Local intranet** and click **Sites**.
  5. Click **Advanced**.
  6. In the **Add this website to the zone** field, type FQDN or IP address of the account federation server and click **Add**.
  7. Repeat Step 6 to add the FQDN or IP address of Deep Discovery Email Inspector to the Websites list.
  8. Click **Close**.
  9. Click **OK**.
  10. Click **OK**.
- 

## Log Settings

Deep Discovery Email Inspector maintains system logs that provide summaries of system events, including component updates and appliance restarts. Go to **Administration > Integrated Products/Services > Syslog** to configure Deep Discovery Email Inspector to send logs to a syslog server.

Deep Discovery Email Inspector can send logs to up to three syslog servers after saving the logs to its database. Only logs saved after enabling a syslog server will be sent to that server. Previous logs are excluded.

The following table describes the tasks you can perform on the **Log Settings** screen.

| TASK                            | DESCRIPTION   |
|---------------------------------|---|
| Add server profile              | Click <b>Add</b> to Create a new syslog server profile.<br>For more information, see <a href="#">Adding a Syslog Server on page 8-179</a> .             |
| Edit existing server profiles   | Click a server profile name to view or modify the settings.<br>For more information, see <a href="#">Editing Syslog Server Profiles on page 8-180</a> . |
| Delete existing server profiles | Select one or more server profiles and click <b>Delete</b> to remove the selected entries from the table.   |

## Adding a Syslog Server

### Procedure

1. Go to **Administration > Integrated Products/Services > Syslog**.  
The **Log Settings** screen appears.
2. Click **Add**.  
The **Add Syslog Server Profile** settings appear.
3. Type a profile name for the syslog server.
4. Type the host name or IP address of the syslog server.
5. Type the port number.
6. Select the protocol to be used when transporting log content to the syslog server.
  - TCP
  - UDP
  - SSL
7. 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.
  - **Trend Micro Event Format (TMEF):** Trend Micro Event Format (TMEF) is a customized event format developed by Trend Micro and is used by Trend Micro products for reporting event information.
8. Select the scope of the data that will be logged.
- **Detections**
  - **Alerts**
  - **Virtual Analyzer analysis logs**
  - **System events**
  - **Message tracking**
  - **Sender Filtering/Authentication**
  - **MTA events**
  - **Time-of-click protection**
9. Click **Save**.
- 

## Editing Syslog Server Profiles

---

### Procedure

1. Go to **Administration > Integrated Products/Services > Syslog**.  
The **Log Settings** screen appears.
  2. Click a syslog server profile hyperlink.  
The **Edit Syslog Server Profile** screen appears.
  3. Make the required changes.
  4. Click **Save**.
-

## SFTP

You can configure Deep Discovery Email Inspector to send Virtual Analyzer detection information to a secure FTP (SFTP) server.

---

### Procedure

1. Go to **Administration > Integrated Products/Services > SFTP**.
2. Select **Send detection information to SFTP server**.
3. Configure the following settings.

| FIELD                 | DESCRIPTION   |
|-----------------------|---|
| Authentication method | Select an option from the drop-down list.                         |
| IP address / Domain   | Type the server IP address or domain name.                        |
| Port                  | Type the port number.   |
| User name             | Type the user name to access the SFTP server.                     |
| Password              | Type the password for the user account to access the SFTP server. |
| Path                  | Specify the directory on the SFTP server to upload files.         |
| Encryption            | Type the password to encrypt the ZIP file for upload.             |
| Certificate           | Click <b>Select</b> to locate and upload a certificate.           |
| Passphrase            | Type a passphrase to protect the certificate.                     |

4. Under **Criteria**, select to send the following detection information to the SFTP server:
    - Investigation packages for safe email messages
    - Data type (threat sample, original email message, or report)
  5. Click **Save**.
-

## Email Encryption

With Email Encryption, Deep Discovery Email Inspector encrypts messages using Trend Micro Identity-Based Encryption (IBE). For example, when the domain **a.com** is registered with Trend Micro for encryption and decryption and **user1@a.com** sends a message with private information to **user2@b.com**, Deep Discovery Email Inspector encrypts the message sent to **user2@b.com**. You can configure a policy rule to encrypt messages containing private information.



### Tip

Before using Email Encryption, Trend Micro recommends you configure Deep Discovery Email Inspector to synchronize the system time with an NTP server to ensure standard time and date data.

---



### Note

When Deep Discovery Email Inspector is registered to Deep Discovery Director 5.1 (or later), Deep Discovery Director provides central management of the Email Encryption settings. After registration is successful, Deep Discovery Email Inspector obtains Email Encryption settings (including the registered email domains) from Deep Discovery Director and prevents manual configuration of the settings on the management console.

---

**Important**

When Email Encryption is enabled, the number of email messages that Deep Discovery Email Inspector encrypts and decrypts may affect system performance. If there is a high volume of email messages in your organization, Trend Micro recommends the following:

- Configure policies with content filtering rules to encrypt specific outgoing email messages
- Set up a dedicated Deep Discovery Email Inspector appliance to perform email encryption and decryption

For assistance with performance sizing, contact Trend Micro Technical Support.

To configure Email Encryption settings in Deep Discovery Email Inspector, do the following:

1. Register one or more domains to the Trend Micro Email Encryption server.

For more information, see [Registering Domains for Email Encryption on page 8-184](#).

2. Configure default sender address for message signing.

For more information, see [Configure Default Email Identity for Message Signing on page 8-186](#).

3. (Optional) Configure Email Encryption exceptions.

For more information, see [Configuring Email Encryption Exceptions on page 5-91](#).

4. Configure content filtering or Data Loss Prevention (DLP) rules with the **Encrypt message** action.

For more information, see [Configuring a Content Filtering Rule on page 5-38](#) and [Configuring a DLP Rule on page 5-44](#).

## Registering Domains for Email Encryption

For email encryption to work, you must register one or more domains to the Trend Micro Email Encryption Server.



### Note

- If the produce license for Gateway Module is expired, Deep Discovery Email Inspector prevents you from configuring settings on the **Email Encryption** screen and removes the specified domain owner email addresses from the Trend Micro Email Encryption Server.
  - When you register a domain to the Trend Micro Email Encryption Server for the first time, Deep Discovery Email Inspector is also registered to the server.
  - You cannot re-register a domain that is already registered to the Trend Micro Email Encryption Server.
  - You can add and register up to 300 domains to the Trend Micro Email Encryption Server.
- 

## Procedure

1. Go to **Administration > Integrated Products/Services > Email Encryption**.
2. In the **Domain List** section, review the domain registration procedure information.
3. Click **Add**.
4. On the **Add Domain** screen, do the following:
  - a. If this is the first time you are adding a domain, specify the email address to receive domain ownership verification key files from Trend Micro.

**Note**

After the first domain is registered to the Trend Micro Email Encryption Server successfully, you can update the email address in the **Appliance Information** section.

- b. Select an input option and do one of the following to add a domain to the **Selected Domains** list:
  - Type a domain in the text field and press Enter.
  - Select a domain from the list.
- c. Click **Save**.

**Note**

- You can add up to 10 domains at a time.
- Domains and their sub-domains are treated as unique entries. Sub-domains must be added separately to the domain list.
- Wildcards cannot be used to include sub-domains.
- LDAP groups (entries starting with "LDAP") cannot be added to the domain list.

5. If you are the registered owner of a domain in the domain list, reply to the confirmation message from Trend Micro.

Trend Micro sends the message to the following email addresses to verify ownership of the domain:

- postmaster@<domain>
  - webmaster@<domain>
  - The email address returned from a WHOIS lookup for the domain
6. When your domain is approved, Trend Micro sends the key file to the specified email address. To upload the key file, do the following:
    - a. In the **Domain List** section, click **Import Key File**.

- b. Click **Select File** and select the key file.
- c. Click **Import**.

**Note**

Trend Micro sends a key file for each added domain to the specified email address. If you do not receive a message with the key file for a domain within three working days, contact your sales representative.

---

**Tip**

After you have registered a domain, you can click **Delete** to remove a domain from the list. To add the delete domain to the list, you must perform the domain registration steps again.

---

- 7. If this is the first time you are registering a domain to the Trend Micro Email Encryption Server, check that the gateway ID information displays under **Appliance Information**.
- 

## Configure Default Email Identity for Message Signing

The default sender address is used when Deep Discovery Email Inspector tries to encrypt a message sent from a sender domain that is not in the Domain List. Deep Discovery Email Inspector signs these messages with the default sender address.

---

### Procedure

- 1. Go to **Administration > Integrated Products/Services > Email Encryption**.
  - 2. Under **Default Email Identify for Message Signing**, type the default sender address.
  - 3. Click **Save**.
-

## System Settings

Topics include:

- [Network Settings on page 8-187](#)
- [Configuring NIC Teaming on page 8-189](#)
- [Operation Modes on page 8-190](#)
- [Configuring Proxy Settings on page 8-193](#)
- [Configuring the Notification SMTP Server on page 8-194](#)
- [Configuring System Time on page 8-197](#)
- [SNMP on page 8-197](#)
- [Certificate Management on page 8-202](#)

## Network Settings

Use this screen to configure the host name, the IPv4 and IPv6 addresses of the Deep Discovery Email Inspector appliance, and other network settings.


### Configuring Network Settings

Perform initial network configurations with the Command Line Interface (CLI). Use the management console to make changes to the network interface settings.

---

#### Procedure

1. Go to **Administration > System Settings > Network**.
2. Specify the host name.
3. Specify the network settings.

| OPTION                                     | DESCRIPTION  |
|--|--|
| IP address and Subnet mask / prefix length | <p>Specify the network interface IP settings for the management network, custom network, and mail network.</p> <ul style="list-style-type: none"> <li>• <b>Management network:</b> The management network handles the management console, SSH connections, and Trend Micro updates. Mail traffic can pass through the management network and by default it is the only network that routes mail. Use only the management port (eth0).</li> <li>• <b>Custom network:</b> The custom network handles sandbox analysis. This network should be an isolated network without connection restrictions so that malicious samples do not affect other networks. Use any available network interface (eth1, eth2, or eth3) that is not configured for the mail network.</li> <li>• <b>Mail network:</b> The mail network handles mail routing and monitoring. Use a network interface that is not configured for the custom network. <ul style="list-style-type: none"> <li>• (Optional) For BCC or MTA mode, use any available network interface (eth1, eth2, or eth3).</li> <li>• For SPAN/TAP mode, use the eth2 or eth3 network interface.</li> </ul> </li> </ul> <hr/> <p> <b>Note</b><br/>For information on operation mode configuration, see <a href="#">Operation Modes on page 8-190</a>.</p> <hr/> |
| Gateway / DNS                              | Specify the general network settings that affect all interfaces, including the gateway and DNS settings.   |

#### 4. Click **Save**.

## Configuring NIC Teaming

A network interface card (NIC) team is a software-based virtual network interface that provides fault tolerance in the event of a network interface card failure. On Deep Discovery Email Inspector, you can group one or more network interface cards in a NIC team.



### Note

- Deep Discovery Email Inspector supports NIC teaming for active/backup mode only.
  - The management port is always bind to the eth0 interface. When grouped with the eth0 interface, the other network interface acts as a backup interface.
  - To function in SPAN/TAP mode, Deep Discovery Email Inspector requires at least three network interface cards that are not selected for NIC teaming.
- 

## Procedure

1. Go to **Administration > System Settings > NIC Teaming**.
2. Under the NIC Teaming section, do the following:
  - a. Toggle the status button to enable a NIC team.
  - b. Select one or more network interface cards to add to the NIC team.



### Note

- You can group up to two network interface cards in a NIC team.
  - A network interface card can only belong to one NIC team.
- 

3. Click **Save**.

The system automatically restarts. This may take some time. Wait for the process to complete before you can access the management console again.

---

## Operation Modes

Deep Discovery Email Inspector can act as a Mail Transfer Agent (MTA mode), or as an out-of-band appliance (BCC mode or SPAN/TAP mode).

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

To configure the operation mode, go to **Administration > System Settings > Operation Mode**.

---



### Note


The internal Postfix server cannot be used to send email notifications in BCC or SPAN/TAP mode.

For more information on specifying an external SMTP server, see [Configuring the Notification SMTP Server on page 8-194](#).

---

**TABLE 8-25. Operation Modes**

| MODE                  | DESCRIPTION   |
|-----------------------|---|
| MTA mode<br>(Default) | As an inline MTA, Deep Discovery Email Inspector protects your network from harm by blocking malicious email messages in the mail traffic flow. Deep Discovery Email Inspector delivers safe email messages to recipients.                    |
| BCC mode              | As an out-of-band appliance, Deep Discovery Email Inspector receives mirrored traffic from an upstream MTA to monitor your network for cyber threats. Deep Discovery Email Inspector discards all replicated email messages without delivery. |

| MODE          | DESCRIPTION   |
|---------------|---|
| SPAN/TAP mode | <p>As an out-of-band appliance, Deep Discovery Email Inspector receives mirrored traffic from a SPAN/TAP device to monitor your network for cyber threats. Deep Discovery Email Inspector discards all replicated email messages without delivery.</p> <p>If you select <b>SPAN/TAP mode</b>, you must add at least one monitoring rule. For more information, see <a href="#">Monitoring Rules for SPAN/TAP Mode on page 8-192</a>.</p> <hr/> <div>  <b>Note</b><br/>           Deep Discovery Email Inspector virtual appliances installed in Microsoft Hyper-V do not support SPAN/TAP mode.         </div> <hr/> |

The following table lists the availability of the features in each operating mode.

| FEATURE/SERVICE  | MTA MODE | BCC MODE | SPAN/TAP MODE                       |
|--|----------|----------|-------------------------------------|
| Message modification (tag, stamp, strip, clean up, rewrite URL, add X-headers, sanitize file, encrypt message, etc.) | Yes      | No       | No                                  |
| Message notification   | Yes      | No       | Yes (using an external SMTP server) |
| Message delivery   | Yes      | No       | No                                  |
| Message quarantine   | Yes      | No       | No                                  |
| Message archiving  | Yes      | No       | No                                  |
| DKIM signing   | Yes      | No       | No                                  |
| End-User Quarantine  | Yes      | No       | No                                  |
| Sender authentication (SPF, DKIM, DMARC)   | Yes      | No       | No                                  |

| FEATURE/SERVICE                     | MTA MODE | BCC MODE                            | SPAN/TAP MODE                       |
|-------------------------------------|----------|-------------------------------------|-------------------------------------|
| Email Reputation Services (ERS)     | Yes      | No                                  | No                                  |
| Sender filtering                    | Yes      | No                                  | No                                  |
| Alerts                              | Yes      | Yes                                 | Yes                                 |
| Alert notification and reports      | Yes      | Yes (using an external SMTP server) | Yes (using an external SMTP server) |
| Queue management                    | Yes      | Yes                                 | Yes                                 |
| Deep Discovery Director integration | Yes      | Yes                                 | Yes                                 |

## Monitoring Rules for SPAN/TAP Mode

When SPAN/TAP mode is selected, you can add a maximum of 10 monitoring rules. The monitoring rules specify the SMTP traffic that Deep Discovery Email Inspector monitors for cyber threats.

### Adding a Monitoring Rule

#### Procedure

1. Go to **Administration > System Settings > Operation Mode**.
2. Click **Add Rule**.

The **Add SPAN/TAP Mode Rule** window appears.

3. Type the **Source IP address**, **Destination IP address**, and **SMTP port** to monitor.



#### Note

If a field is empty, all SMTP traffic for that option is monitored.

For example, when **Source IP address** is empty, SMTP traffic from all sources is monitored.

4. Click **Add**.
- 

## Editing a Monitoring Rule

---

### Procedure

1. Go to **Administration > System Settings > Operation Mode**.
  2. Select a monitoring rule and click **Edit**.  
The **Edit SPAN/TAP Mode Rule** window appears.
  3. Make the changes.
  4. Click **Edit**.
- 

## Deleting a Monitoring Rule

---

### Procedure

1. Go to **Administration > System Settings > Operation Mode**.
  2. Select a monitoring rule and click **Delete**.
- 

## 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

- Time-of-Click protection
- Predictive Machine Learning Engine

---

## Procedure

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

The **Proxy** screen appears.

2. Specify the proxy server settings.

| OPTION         | DESCRIPTION   |
|----------------|---|
| Check box      | Select <b>Use a proxy server to connect to the Internet</b> .   |
| Type           | Select the proxy protocol: <ul style="list-style-type: none"><li>• HTTP</li><li>• SOCKS4</li><li>• SOCKS5</li></ul> |
| Server address | Specify the proxy server host name or IP address.   |
| Port           | Specify the port that the proxy server uses to connect to the Internet.   |
| User name      | Optional: Specify the user name for administrative access to the proxy server.                                      |
| Password       | Optional: Specify the corresponding password.   |

3. Click **Save**.
- 

## Configuring the Notification SMTP Server


Deep Discovery Email Inspector uses the SMTP server settings to send alert notifications and reports.




For details about processing SMTP traffic, see [Mail Settings on page 8-94](#).

---

## Procedure

1. Go to **Administration > System Settings > SMTP**.
2. Type the **Sender email address**.
3. Specify the SMTP server settings.

| OPTION                  | DESCRIPTION  |
|-------------------------|--|
| Internal postfix server | <p>Select this option to use the postfix server embedded in Deep Discovery Email Inspector as an SMTP server.</p> <hr/> <div> <b>Note</b><br/>Internal postfix is not available when operating in BCC mode and SPAN/TAP mode.</div> <hr/> |
| External SMTP server    | Select this option to specify a standalone SMTP server, such as Microsoft Exchange.  |
| Server address          | Type the external SMTP server host name, IPv4 address or IPv6 address.   |
| Port                    | Type the external SMTP server port number.   |
| Connection security     | Select a security protocol if required for the connection.   |

| OPTION                              | DESCRIPTION   |
|-------------------------------------|---|
| SMTP server requires authentication | <p>Select this option if connection to the SMTP server requires authentication.</p> <hr/> <div data-bbox="475 354 532 402"></div> <div data-bbox="548 354 596 375"><b>Note</b></div> <ul style="list-style-type: none"> <li>• Make sure that you configure the user name and password correctly. An external SMTP server may refuse connection from Deep Discovery Email Inspector after the maximum number of unsuccessful authentication attempts has been reached.</li> <li>• Clicking <b>Test Connection</b> checks the connection from Deep Discovery Email Inspector to the external SMTP server, but does not verify SMTP server authentication.</li> </ul> |
| User name                           | <p>Type the user name used for authentication.</p> <hr/> <div data-bbox="475 850 532 899"></div> <div data-bbox="548 850 596 872"><b>Note</b></div> <p>This option is only available if <b>SMTP server requires authentication</b> is selected.</p>  |
| Password                            | <p>Type the password used for authentication.</p> <hr/> <div data-bbox="475 1055 532 1104"></div> <div data-bbox="548 1055 596 1076"><b>Note</b></div> <p>This option is only available if <b>SMTP server requires authentication</b> is selected.</p>   |

4. Click **Save**.
5. (Optional) To test the connection to the external SMTP server, do the following:
  - a. Click **Test Connection**.

- b. Type the recipient email address.
- c. Click **OK**.

**Note**

Deep Discovery Email Inspector does not send a test email message to the recipient.

---

## Configuring System Time

Network Time Protocol (NTP) synchronizes computer system clocks across the Internet. Configure NTP settings to synchronize the server clock with an NTP server, or manually set the system time.

---

### 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 or select the time zone.
    - To display the date and time in another format, select the format from the **Date and time format** drop-down list.
  3. Click **Save**.
- 

## 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 Email 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 8-198](#).
- Configure the appliance to listen for manager requests  
For details, see [Configuring Manager Requests on page 8-200](#).

## Configuring Trap Messages




A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.


---

### Procedure

1. Go to **Administration > System Settings > SNMP**.
2. Under **Trap Messages**, select **Send SNMP trap messages**.
3. Specify the trap message settings.

| OPTION                 | DESCRIPTION                         |
|------------------------|-------------------------------------|
| Manager server address | Specify the manager server address. |

| OPTION         | DESCRIPTION  |
|----------------|--|
| SNMP version   | <p>Select the SNMP version:</p> <ul style="list-style-type: none"> <li>• SNMPv1/SNMPv2c</li> <li>• SNMPv3</li> </ul> <p>If you use SNMPv3, configure the SNMP server as follows:</p> <ul style="list-style-type: none"> <li>• Context Name: "" (default context)</li> <li>• Context Engine ID: &lt;Auto&gt;</li> <li>• (Optional) MD5 Authentication protocol: HMAC-MD5</li> <li>• (Optional) DES Privacy protocol: CBC-DES</li> </ul> |
| Community name | Specify a community name.  |
| Security model | <hr/> <div>  <b>Note</b><br/> This field is only available for SNMPv3. </div> <hr/> <p>Select the security model:</p> <ul style="list-style-type: none"> <li>• No authentication or privacy</li> <li>• Authenticated</li> <li>• Authenticated with privacy</li> </ul>   |
| User name      | <hr/> <div>  <b>Note</b><br/> This field is only available for SNMPv3. </div> <hr/> <p>Specify the user name.</p>  |
| Password       | <hr/> <div>  <b>Note</b><br/> This field is only available for SNMPv3. </div> <hr/> <p>Specify the password.</p>  |

| OPTION             | DESCRIPTION  |
|--------------------|--|
| Privacy passphrase | <div> <b>Note</b><br/>This field is only available for SNMPv3.</div> <div>Specify the privacy passphrase.</div> |

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 Email Inspector supported SNMP object identifiers (OID), see [SNMP Object Identifiers on page D-1](#).
- 

## Configuring Manager Requests




SNMP managers can use SNMP protocol commands to request Deep Discovery Email 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.

| OPTION                | DESCRIPTION  |
|-----------------------|--|
| Device location       | Specify the location of this appliance.              |
| Administrator contact | Specify the administrator contact of this appliance. |

| OPTION                  | DESCRIPTION  |
|-------------------------|--|
| SNMP version            | <p>Select the SNMP version:</p> <ul style="list-style-type: none"> <li>• SNMPv1/SNMPv2c</li> <li>• SNMPv3</li> </ul> <p>If you use SNMPv3, configure the SNMP server as follows:</p> <ul style="list-style-type: none"> <li>• Context Name: "" (default context)</li> <li>• Context Engine ID: &lt;Auto&gt;</li> <li>• (Optional) MD5 Authentication protocol: HMAC-MD5</li> <li>• (Optional) DES Privacy protocol: CBC-DES</li> </ul> |
| Allowed community names | Specify a maximum of 5 community names.  |
| Security model          | <hr/> <p> <b>Note</b><br/>This field is only available for SNMPv3.</p> <hr/> <p>Select the security model:</p> <ul style="list-style-type: none"> <li>• No authentication or privacy</li> <li>• Authenticated</li> <li>• Authenticated with privacy</li> </ul>  |
| User name               | <hr/> <p> <b>Note</b><br/>This field is only available for SNMPv3.</p> <hr/> <p>Specify the user name.</p>   |
| Password                | <hr/> <p> <b>Note</b><br/>This field is only available for SNMPv3.</p> <hr/> <p>Specify the password.</p>   |

| OPTION                           | DESCRIPTION   |
|----------------------------------|---|
| Privacy passphrase               |  <b>Note</b><br>This field is only available for SNMPv3. |
|                                  | Specify the privacy passphrase.   |
| Trusted manager server addresses | Specify a maximum of 5 trusted manager server addresses.  |

4. Click **Save**.
  5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.
    - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.
    - For a list of Deep Discovery Email Inspector supported SNMP object identifiers (OID), see [SNMP Object Identifiers on page D-1](#).
- 

## Configuring Session Timeout Setting

Deep Discovery Email Inspector automatically logs you out of the management console after a period of inactivity. The default session timeout period is 30 minutes.

To configure the session timeout, go to **Administration > System Settings > Session Timeout** and select an option from the drop-down list.

## Certificate Management

Digital certificates are electronic documents that are used to create secure connections between clients and servers or websites. A valid and trusted certificate ensures clients that they are connecting to a trusted server or website, and helps protect against man-in-the-middle attacks.

Certificates become trusted by going through a validation process of a Certificate Authority (CA). Certificate Authorities themselves are usually

third-party companies that are trusted by both the client and server or website.

You can manage certificates in Deep Discovery Email Inspector to enable secure console access and SMTP communication in Transport Layer Security (TLS) environments.

For more information about TLS, see [Transport Layer Security \(TLS\) on page 8-112](#).

## SMTP and HTTPS Certificates

SMTP and HTTPS certificates identify Deep Discovery Email Inspector to other entities, for example, message transfer agents (MTAs). Along with the SMTP or HTTPS certificate, a private key is stored in Deep Discovery Email Inspector to prove its authenticity.

You can manage certificates in Deep Discovery Email Inspector to enable secure connections for the following services:

- SMTP client communication
- SMTP server communication
- EUQ console access
- Management console access

The following table describes the tasks you can perform on the **SMTP and HTTPS Certificates** screen.

| TASK                                 | DESCRIPTION   |
|--------------------------------------|---|
| Create a self-signed certificate     | Click <b>Add</b> .<br>For more information, see <a href="#">Configuring a Certificate Signing Request on page 8-204</a> |
| Create a certificate signing request | Click <b>Add</b> .<br>For more information, see <a href="#">Configuring a Self-signed Certificate on page 8-205</a>     |

| TASK  | DESCRIPTION  |
|---|--|
| Change the certificate name and view detailed information | Click an IP address or domain.<br>For more information, see <a href="#">Configuring a Certificate Signing Request on page 8-204</a> or <a href="#">Configuring a Self-signed Certificate on page 8-205</a> . |
| Import a certificate                                      | Click <b>Import</b> .<br>For more information, see <a href="#">Importing a Certificate on page 8-206</a> .   |
| Export a certificate                                      | Select a certificate and click <b>Export</b> .<br>For more information, see <a href="#">Exporting a Certificate on page 8-207</a> .  |
| Assign a certificate                                      | Select a certificate and click <b>Assign</b> .<br>For more information, see <a href="#">Assigning a Certificate on page 8-207</a> .  |
| Delete certificates                                       | Select one or more certificates and click <b>Delete</b> , and then click <b>Yes</b> to confirm deletion.   |

## Configuring a Certificate Signing Request

---

### Procedure

1. Go to **Administration > System Settings > Certificate Management**.  
The **SMTP and HTTPS Certificates** screen appears.
2. Do one of the following:
  - Click **Add** to create a new entry.
  - Click a name to view detailed information and change the name only.
3. Type the certificate name.
4. In the **Subject alternative names** field, type one or more domain names to associate with the generated certificate.
5. From the **Type** drop-down list, select **Certificate signing request**.
6. Configure the required fields.

| FIELD             | DESCRIPTION   |
|-------------------|---|
| Key length        | Select the certificate key size.                        |
| Country code      | Select the country where your company is located.       |
| State             | Type the state or region where your company is located. |
| Locality          | Type the city where your company is located.            |
| Organization      | Type your company name.                                 |
| Organization unit | Type the name of your department within your company.   |
| Common name       | Type a common name (for example, the server FQDN).      |
| Email address     | Type your email address.                                |

7. Click **Add**.
8. Copy and save the content of your certificate signing request so that you can send the request to a certificate authority (CA).
9. Click **Close**.

---

## Configuring a Self-signed Certificate

---

### Procedure

1. Go to **Administration > System Settings > Certificate Management**.  
The **SMTP and HTTPS Certificates** screen appears.
2. Do one of the following:
  - Click **Add** to create a new entry.
  - Click a name to view detailed information and change the name only.
3. Type the certificate name.
4. In the **Subject alternative names** field, type one or more domain names to associate with the generated certificate.

5. From the **Type** drop-down list, select **Self-signed certificate**.
6. Configure the required fields.

| FIELD             | DESCRIPTION   |
|-------------------|---|
| Key length        | Select the certificate key size.                        |
| Country code      | Select the country where your company is located.       |
| State             | Type the state or region where your company is located. |
| Locality          | Type the city where your company is located.            |
| Organization      | Type your company name.                                 |
| Organization unit | Type the name of your department within your company.   |
| Common name       | Type a common name (for example, the server FQDN).      |
| Email address     | Type your email address.                                |
| Valid days        | Type the number of days the certificate will be valid.  |

7. Click **Add**.
- 

## Importing a Certificate

Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.

---

### Procedure

1. Go to **Administration > System Settings > Certificate Management**.  
The **SMTP and HTTPS Certificates** screen appears.
2. Click **Import**.
3. Select the certificate file.
4. (Optional) Select the private key file and type the password.

5. Click **Import**.
- 

## Exporting a Certificate

---

### Procedure

1. Go to **Administration > System Settings > Certificate Management**.  
The **SMTP and HTTPS Certificates** screen appears.
  2. Select a certificate and click **Export**.
  3. (Optional) Select **Export the private key file** and type the password.
  4. Click **Export**.
- 

## Assigning a Certificate

After importing a certificate or creating a self-signed certificate, assign the certificate to a service to use it.

---

### Procedure


1. Go to **Administration > System Settings > Certificate Management**.  
The **SMTP and HTTPS Certificates** screen appears.
  2. Select a certificate and click **Assign**.
  3. Move one or more selected services from the **Available Services** list to the **Selected Services** list.
  4. Click **Assign**.
- 

## Trusted CA Certificates

Trusted certificate authority (CA) certificates verify remote certificates that are presented to Deep Discovery Email Inspector. CA certificates have a dependency relationship that forms a Certificate Trust List (CTL) hierarchy.

This hierarchy connects a certificate with its root CA and verifies its authenticity.

The following table describes the tasks you can perform on the **Trusted CA Certificates** screen.

| TASK                         | DESCRIPTION  |
|------------------------------|--|
| View certificate information | Click a name.  |
| Import certificates          | Click <b>Import</b> .<br>For more information, see <a href="#">Importing Certificates on page 8-208</a> .  |
| Export certificates          | Select one or more certificates and click <b>Export</b> .<br><br> <b>Note</b><br>If you select more than one certificate to export, Deep Discovery Email Inspector exports the selected certificate in the same certificate file. |
| Delete certificates          | Select one or more certificates and click <b>Delete</b> , and then click <b>Yes</b> to confirm deletion.   |

## Importing Certificates

Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.



### Note

If you want to import multiple CA certificates at the same time, save them into the same file and then import the file.

## Procedure

1. Go to **Administration > System Settings > Certificate Management**.
2. Click **Trusted CA Certificates**.

3. Click **Import**.
4. Select the certificate file.

Deep Discovery Email Inspector imports the file.

---

## Configuring Connection Security Settings

You can select the security protocols that Deep Discovery Email Inspector uses for web console and SMTP connections.

---

### Procedure

1. Go to **Administration > System Settings > Connection Security**.
2. Select the security protocols for the connection types (**Web console** and **SMTP**).



#### Note

For the SMTP connection type, you can configure the Transport Layer Security (TLS) settings for inbound and outbound messages on the **TLS** screen.

For more information, see [Configuring TLS Settings on page 8-113](#).

---

3. Click **Save**.
- 

## Accounts / Contacts

Deep Discovery Email 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 only the tools and permissions necessary to perform specific tasks.

To enhance account security for management console access, Deep Discovery Email Inspector automatically locks an account after five unsuccessful logon attempts. To use the account again to log onto the management console, the user can wait for 10 minutes or request an administrator to unlock the account.

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 Email Inspector has a default administrator account (“admin”) that has full administrative access.

The default administrator account can perform the following tasks:

- Add new administrator accounts
- Lock or unlock an account

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 Email Inspector administration.

Administrator accounts can additionally edit or delete existing accounts.

## Account Role Classifications

| ROLE          | DESCRIPTION   |
|---------------|---|
| Administrator | <p>Users have complete access to the features and settings contained in the menu items.</p> <ul style="list-style-type: none"><li>• <b>Dashboard</b></li><li>• <b>Detections</b></li><li>• <b>Policies</b></li><li>• <b>Alerts / Reports</b></li><li>• <b>Logs</b></li><li>• <b>Administration</b></li><li>• <b>Help</b></li></ul>  |
| Investigator  | <p>Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.</p> <ul style="list-style-type: none"><li>• <b>Dashboard</b></li><li>• <b>Detections</b></li><li>• <b>Alerts / Reports &gt; Reports &gt; Generated Reports</b></li><li>• <b>Alerts / Reports &gt; Alerts &gt; Triggered Alerts</b></li><li>• <b>Logs</b></li><li>• <b>Help</b></li></ul>                             |
| Operator      | <p>Users can view certain features and settings contained in the menu items, but cannot make any administrative modifications.</p> <ul style="list-style-type: none"><li>• <b>Dashboard</b></li><li>• <b>Detections</b> (no access to message body)</li><li>• <b>Alerts / Reports &gt; Reports &gt; Generated Reports</b></li><li>• <b>Alerts / Reports &gt; Alerts &gt; Triggered Alerts</b></li><li>• <b>Logs</b></li><li>• <b>Help</b></li></ul> |

## Adding a Local User Account

---

### Procedure

1. Go to **Administration > Accounts / Contacts > Accounts**.
2. Click **Add**.  
The **Add Account** screen appears.
3. Toggle the **Status** of this account.
4. Select **Local user** from the **Type** drop-down list.
5. Specify the account user name and password.
6. Select a **Role** for this account. The role determines the level of access this account has.

See [Account Role Classifications on page 8-211](#).

7. Click **Save**.  
The new account is added to the **Accounts** list.
- 

## Adding an Active Directory User Account or Group

---



### Note

Microsoft Active Directory settings have to be configured before an Active Directory user account or group can be added.

For details, see [LDAP on page 8-165](#).

---

### Procedure

1. Go to **Administration > Accounts / Contacts > Accounts**.
2. Click **Add**.

The **Add Account** screen appears.

3. Toggle the **Status** of this account.
4. Select **LDAP user or group** as the **Type** for this account.
5. Type a user or group name and click **Search** to search the LDAP server for matching user accounts or groups.

Matching user accounts and groups are displayed in the results table.

**Note**

User accounts are not displayed in the results table if:

- The user account's User Principal Name (UPN) is not specified on the LDAP server
- The user account is disabled on the LDAP server

- 
6. Select the LDAP user account or group to add.
  7. Select a **Role** for this account. The role determines the level of access this account has.  
See [Account Role Classifications on page 8-211](#).
  8. Click **Save**.

The new account is added to the **Accounts** list.

---

## Editing Accounts

Change account permissions to adjust settings for a role revision or other 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 Email 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**.
- 

## Unlocking a Locked Account

Deep Discovery Email Inspector automatically locks an account after five unsuccessful logon attempts. You can use ad administrator account to manually unlock the account.



### Note

If an account is locked, the user can log in again after 10 minutes and Deep Discovery Email Inspector will unlock the account. The account remains locked if the user does not try to log in again after 10 minutes.

---

## Procedure

1. Go to **Administration > Accounts / Contacts > Accounts**.

2. Select a locked account.
  3. Click **Unlock**.
- 

## Changing Your Password

---



### Note

You cannot use the management console to change the password for the following:

- Microsoft Active Directory accounts
  - Trend Micro Apex Central single sign-on (SSO) accounts
  - SAML SSO accounts
- 

### Procedure

---

1. On the management console banner, click your account name.  
The **Change Password** screen appears.
  2. Specify password settings.
    - **Old password**
    - **New password**
    - **Confirm password**
  3. Click **Save**.
- 

## SAML Groups

Once Deep Discovery Email Inspector and the identity provider have established a trust relationship, Deep Discovery Email Inspector can access the user identities on the identity provider's directory server. However, before Deep Discovery Email Inspector can actually perform user authentication and authorization using the user identity information, you need to configure account types and SAML groups using groups, roles and claims.

The following provides a configuration overview to map a SAML account from identity provider to a user role in Deep Discovery Email Inspector:

1. Create user accounts.
  - a. Create user accounts.
  - b. Create user groups and assign user accounts to the groups.

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

2. In Deep Discovery Email Inspector, create SAML groups with the specified roles and claims.

For more information, see [Configuring SAML Groups on page 8-216](#).

## Configuring SAML Groups

Configure SAML groups in Deep Discovery Email Inspector to map to user groups in your identity provider.

---

### Procedure

1. Go to **Administration > Accounts / Contacts > SAML**.
2. Do one of the following:
  - Click **Add** to create a SAML group.
  - Click the name of a SAML group to configure the settings.
3. Select a status option to enable or disable the SAML group.
4. Type a claim value.



#### Important

A claim value identifies the role of a user in the response sent by the identity provider. Make sure you specify the same claim value for a user group in your identity provider and Deep Discovery Email Inspector.

---

5. (Optional) Type a description for the SAML group.

6. Select the role and associated permissions of the SAML group.
    - **Administrator:** Users have full access to submitted objects, analysis results, and product settings
    - **Investigator:** Users have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects
    - **Operator:** Users have read-only access to submitted objects, analysis results, and product settings
    - **EUQ:** Users have full access to the EUQ console only
  7. Click **Save**.
- 

## Managing Contacts

Type the email addresses of notification contacts that are sent alert notifications and reports.

For details, see [Scheduling Reports on page 6-28](#) and [Configuring Alert Notifications on page 6-5](#).

## System Maintenance

Go to the **System Maintenance** screen to perform the following operations:

- [Backing Up or Restoring a Configuration on page 8-217](#)
- [Configuring Storage Maintenance on page 8-224](#)
- [Debug Logs on page 8-226](#)
- [Testing Network Connections on page 8-227](#)

## Backing Up or Restoring a Configuration

Export settings from the management console to back up the Deep Discovery Email Inspector configuration. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

**Important**

Deep Discovery Email Inspector only supports restoring configurations from other Deep Discovery Email Inspector servers with a compatible license status and with the same firmware version, hardware model, and locale. For example, you cannot restore a server running version 5.1 with a configuration file backed up from a server running version 3.2 or earlier versions.

For more information on compatible licenses, see [License Compatibility on page 8-218](#).

---

**Note**

When exporting/importing your settings, the database will be locked. Therefore, all Deep Discovery Email 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 Email Inspector is idle. Importing and exporting affects Deep Discovery Email Inspector performance.

Back up settings to create a copy of Deep Discovery Email Inspector appliance configuration to restore the configuration in another Deep Discovery Email Inspector appliance or to revert to the backup settings at a later time. Replicate a configuration across several Deep Discovery Email Inspector appliances by restoring the same configuration file into each appliance.

## License Compatibility

The following table indicates compatible product licenses. You can only restore configuration files backed up from other Deep Discovery Email Inspector servers with a compatible license, and with the same firmware version, hardware model, and locale.

**TABLE 8-26. License compatibility**

| <b>LICENSE ACTIVATION</b>                          | <b>ADVANCED THREAT PROTECTION + GATEWAY MODULE</b> | <b>GATEWAY MODULE ONLY</b> | <b>ADVANCED THREAT PROTECTION ONLY</b> |
|--|--|----------------------------|--|
| <b>ADVANCED THREAT PROTECTION + GATEWAY MODULE</b> | Compatible   | Compatible                 | Compatible                             |
| <b>GATEWAY MODULE ONLY</b>                         | Not compatible                                     | Compatible                 | Not compatible                         |
| <b>ADVANCED THREAT PROTECTION ONLY</b>             | Not compatible                                     | Not compatible             | Compatible                             |

## Backup Recommendations

Trend Micro recommends exporting your settings to:

- Keep a backup

If Deep Discovery Email Inspector cannot recover from a critical problem, import your configuration backup after restoring the device to automatically implement the pre-failure configuration.

- Replicate settings across several devices

If you have several devices on your network, you do not need to separately configure most settings.

## Backing 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

You can back up settings from the screens and tabs listed in the following table.

**TABLE 8-27. Backed up configuration settings**

| SCREEN                                       | TAB   |
|--|---|
| <b>Dashboard</b>                             | Settings for all widgets only                 |
| <b>Policies &gt; Policy Management</b>       | <b>Policy List</b>                            |
|  | <b>Content Filtering Rules</b>                |
|  | <b>DLP Rules</b>                              |
|  | <b>Antispam Rules</b>                         |
|  | <b>Threat Protection Rules</b>                |
| <b>Policies &gt; Policy Objects</b>          | <b>Notifications</b>                          |
|  | <b>Replacement File</b>                       |
|  | <b>Redirect Pages</b>                         |
|  | <b>Archive Servers</b>                        |
|  | <b>Data Identifiers</b>                       |
|  | <b>DLP Templates</b>                          |
| <b>Policies &gt; Exceptions</b>              | <b>Messages</b>                               |
|  | <b>Objects</b> (local object exceptions only) |
|  | <b>URL Keywords</b>                           |
|  | <b>Graymail Exceptions</b>                    |
|  | <b>Email Encryption Exceptions</b>            |
| <b>Alerts / Reports &gt; Alerts</b>          | <b>Rules</b>                                  |
| <b>Alerts / Reports &gt; Reports</b>         | <b>Schedules</b>                              |
| <b>Administration &gt; Component Updates</b> | <b>Schedule</b>                               |

| SCREEN   | TAB  |
|--|--|
|  | <b>Source</b>  |
| <b>Administration &gt; System Settings</b>               | <b>Operation Mode</b>  |
|  | <b>Proxy</b>   |
|  | <b>SMTP</b>  |
|  | <b>Time</b> (date and time format and NTP server settings only)                                    |
|  | <b>SNMP</b>  |
|  | <b>Session Timeout</b>   |
|  | <b>Certificate Management</b>  |
|  | <b>Connection Security</b>   |
| <b>Administration &gt; Mail Settings</b>                 | <b>Connections</b>   |
|  | <b>Message Delivery</b>  |
|  | <b>Limits and Exceptions</b>   |
|  | <b>SMTP Greeting</b>   |
|  | <b>Edge MTA Relay Servers</b>  |
|  | <b>Internal Domains</b>  |
| <b>Administration &gt; Integrated Products/ Services</b> | <b>Syslog</b>  |
|  | <b>LDAP</b>  |
|  | <b>SFTP</b>  |
| <b>Administration &gt; Scanning / Analysis</b>           | <b>Settings</b> (Submission Filters , URL Submission Filtering, and Timeout Setting sections only) |
|  | <b>File Passwords</b>  |
|  | <b>Smart Protection</b>  |

| SCREEN   | TAB                                  |
|--|--------------------------------------|
|  | Smart Feedback                       |
|  | YARA Rules                           |
|  | Time-of-Click Protection             |
|  | Business Email Compromise Protection |
|  | URL Scanning                         |
| Administration > Sender Filtering/<br>Authentication | Approved Senders                     |
|  | Blocked Senders                      |
|  | DHA Protection                       |
|  | Email Reputation                     |
|  | Bounce Attack Protection             |
|  | SMTP Traffic Throttling              |
|  | SPF                                  |
|  | DKIM Authentication                  |
|  | DKIM Signatures                      |
|  | DMARC                                |
| Administration > End-User Quarantine                 | User Quarantine Access               |
|  | EUQ Digest                           |
| Administration > System Maintenance                  | Storage Maintenance                  |
| Administration > Accounts / Contacts                 | Accounts                             |
|  | Contacts                             |

---

## Procedure

1. Go to **Administration > System Maintenance > Back Up / Restore**.

2. Next to **Configuration Settings Backup**, click **Export**.  
A **File Download** window appears.
  3. Click **Save** to save the configuration file to local storage.
- 

## Restoring a Configuration

Restoring Deep Discovery Email Inspector settings replaces the original settings and rules, such as message delivery settings, with the imported configuration.

During import, 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 [Backing Up a Configuration on page 8-219](#).

---

## Procedure

1. Go to **Administration > System Maintenance > Back Up / Restore**.
2. Next to **Restore Configuration Settings**, click **Choose File** or **Browse** and locate the file.
3. Click **Restore**.

All services restart. Depending on the settings and rules to restore, this may take some time.

---

## Configuring Storage Maintenance

Storage Maintenance allows you to control the size of your quarantine folders and the amount of log data that the system saves. You can also view the current usage information for the quarantined folders.

---

### Procedure

1. Go to **Administration > System Maintenance > Storage Maintenance**.
2. Specify the global quarantine settings.
  - **Global quarantine folder size:** Specify the size of the global quarantine folder in GB



#### Note

Depending on your version of the Deep Discovery Email Inspector appliance, configure the global quarantine folder size as follows:

- Deep Discovery Email Inspector 7100/7200/7300: The quarantine folder size must be a value between 1 and 100
- Deep Discovery Email Inspector 9100/9200: The quarantine folder size must be a value between 1 and 400

- 
- **Delete message attachments, links, and analysis reports when the free global quarantine space is equal to or lower than:** Specify the quarantine space threshold for automatic file deletion



#### Note

The threshold value must be between 10 and 50.

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

---

3. Specify the End-User Quarantine (EUQ) settings.
  - **Remove all data (including messages and approved senders):**  
Click **Remove** to delete all data in the EUQ database

- **End-User Quarantine folder size:** Specify the size of the quarantine folder in GB
- **Delete message attachments, links, and analysis reports when the free End-User Quarantine space is equal to or lower than:** Specify the EUQ space threshold for automatic file deletion

**Note**

The threshold value must be between 10 and 50.

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

- 
- **Maximum quarantined message age:** Specify the number of days to keep quarantined spam messages

**Note**

The specified value must be between 1 and 60.

#### 4. Specify the log settings.

- **Delete logs older than:** Specify the number of days to keep logs

**Note**

The specified value must be between 3 and 366.

- 
- **Delete logs when the total free disk space is equal to or lower than:** Specify the disk space threshold for automatic log deletion

**Note**

The threshold value must be between 10 and 50.

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

---



### Important

Integration with Deep Discovery Director for Virtual Analyzer image deployment requires additional disk space. After registering Deep Discovery Email Inspector to Deep Discovery Director 5.0 (or later), configure Deep Discovery Email Inspector to delete logs when the total free disk space is less than 20%.

---

5. Click **Save**.
- 

## Powering Off or Restarting Deep Discovery Email Inspector

The **Power Off / Restart** screen provides options to power off or restart the Deep Discovery Email Inspector appliance and its associated services.

---

### Procedure

1. Go to **Administration > System Maintenance > Power Off / Restart**.
  2. Do one of the following:
    - To shut down the Deep Discovery Email Inspector appliance, click **Power Off**.
    - To restart Deep Discovery Email Inspector, click **Restart**.
  3. Click **OK** to confirm.
- 

## Debug Logs

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

### Exporting Debugging Files

Export your debugging file to provide information to Trend Micro Support for troubleshooting a problem.

---

### Procedure

1. Go to **Administration > System Maintenance > Debug Logs** .
  2. Select the number of days to export.
  3. Click **Export**.
  4. Wait for the export to complete. The time required depends on the amount of data to export.
- 

## Configuring Log Level

Configure the log level to save information that you can provide to Trend Micro Support for troubleshooting a problem.

---

### Procedure

1. Go to **Administration > System Maintenance > Debug Logs** .
  2. Select the log level.
    - Debug
    - Error
  3. Click **Save**.
- 

## Testing Network Connections

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.

---

### Procedure

1. Go to **Administration > System Maintenance > Network Services Diagnostics**.
2. Select one or more enabled services and click **Test**.

**Note**

You can enable the **Smart Protection Server** option by configuring settings on the **Smart Protection** screen.

For more information, see [Configuring Smart Protection Settings on page 8-39](#).

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.

## Licenses

The **License** screen displays license information and accepts valid Activation Codes for the feature sets in Deep Discovery Email Inspector.

- **Advanced Threat Protection**
- **Gateway Module**

The following table lists the features or services available for each feature set.

| FEATURE/SERVICE                         | ADVANCED THREAT PROTECTION | GATEWAY MODULE |
|---|----------------------------|----------------|
| Auxiliary products/services integration | Yes                        | Yes            |
| Community File Reputation               | Yes                        | Yes            |
| File password analyzer                  | Yes                        | No             |
| Internal Virtual Analyzer               | Yes                        | No             |
| Office macro scanning                   | Yes                        | Yes            |
| Predictive Machine Learning             | Yes                        | Yes            |
| Time-of-Click protection                | Yes                        | Yes            |

| FEATURE/SERVICE                 | ADVANCED THREAT PROTECTION | GATEWAY MODULE |
|---------------------------------|----------------------------|----------------|
| Threat intelligence sharing     | Yes                        | Yes            |
| Web service API                 | Yes                        | Yes            |
| YARA rules                      | Yes                        | No             |
| Antispam/graymail protection    | No                         | Yes            |
| Content filtering               | No                         | Yes            |
| Data loss prevention (DLP)      | No                         | Yes            |
| DKIM signatures                 | No                         | Yes            |
| Email Encryption                | No                         | Yes            |
| Email Reputation Services (ERS) | No                         | Yes            |
| End-User Quarantine             | No                         | Yes            |
| Sender filtering                | No                         | Yes            |

**Note**

Other features (for example, ActiveUpdate, suspicious object detections, and Social Engineering Attack Protection, etc.) not listed in the table are available in both feature sets.

## 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://clp.trendmicro.com/fullregistration?T=TM>

## 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://clp.trendmicro.com/fullregistration?T=TM>

A Registration Key has 22 characters (including the hyphens) and appears as follows:


XX-XXXX-XXXX-XXXX-XXXX

After registration, your Activation Code is sent via email.

## Product License Status

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        | DESCRIPTION   |
|---------------|---|
| Evaluation    | Deep Discovery Email Inspector has full product functionality for a limited trial period. The trial period is based on the Maintenance Agreement.                                 |
| Not Activated | Technical support and component updates are not available. Deep Discovery Email Inspector passes all email messages without investigation until the product license is activated. |

| STATUS    | DESCRIPTION   |
|-----------|---|
| Activated | Deep Discovery Email Inspector has full product functionality and component updates for the license period. Technical Support is available based on the Maintenance Agreement.  |
| Expired   | <p>The license is no longer valid. After the grace period lapses, product functionality is limited.</p> <ul style="list-style-type: none"> <li>For evaluation licenses, component updates and scanning are not available.</li> <li>For full licenses, technical support and component updates are not available. Scanning is maintained with outdated components.</li> </ul> <hr/> <div>  <b>WARNING!</b><br/> Outdated components significantly reduce product detection capabilities. </div> <hr/> |

## Viewing Your Product License

Monitor the status of your product licenses on the **License** screen.

### Procedure

#### 1. Go to **Administration > License**.

The following table describes the license information.

| FIELD           | DESCRIPTION   |
|-----------------|---|
| Status          | The current state of your product license. For information about the product license statuses, see <a href="#">Product License Status on page 8-230</a> . |
| Type            | The license type includes full and trial licenses. The Maintenance Agreement defines the available license type.  |
| Expiration date | The date that the license expires.  |

| FIELD           | DESCRIPTION   |
|-----------------|---|
| Activation Code | The Activation Code has 37 characters (including the hyphens) and appears as follows:<br><br>XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX<br><br>For details, see <a href="#">Activation Codes on page 8-230</a> . |

**2. Under **License Details**:**

- Click **View details** to display the Trend Micro Online Registration website.
  - Click **Refresh** to manually synchronize the license expiration date.
- 

## Activating or Renewing 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. If you are activating the license for the first time, 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 Email Inspector component activates.

6. View your product license.

See [Viewing Your Product License on page 8-231](#).

---

## About Deep Discovery Email Inspector

Use the **About** screen in **Help** → **About** to view the firmware version, API key, and other product details.



### Note

For hardware model 7300, download and install Hotfix 1394 to display the correct hardware model information on the management console.

For more information, go to [https://success.trendmicro.com/dcx/s/solution/000290725?language=en\\_US](https://success.trendmicro.com/dcx/s/solution/000290725?language=en_US).

---



## Chapter 9

### Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 9-2*
- *Contacting Trend Micro on page 9-3*
- *Sending Suspicious Content to Trend Micro on page 9-4*
- *Other Resources on page 9-5*

## Troubleshooting Resources

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

### Using the Support Portal

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

---

#### Procedure

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



#### Tip

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

<https://success.trendmicro.com/smb-new-request>

---

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

---

### Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware> to learn more about:

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

## Contacting Trend Micro

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

|               |  |
|---------------|--|
| Address       | Trend Micro, Incorporated<br>225 E. John Carpenter Freeway, Suite 1500<br>Irving, Texas 75062 U.S.A. |
| Phone         | Phone: +1 (817) 569-8900<br>Toll-free: (888) 762-8736  |
| Website       | <a href="https://www.trendmicro.com">https://www.trendmicro.com</a>                                  |
| Email address | <a href="mailto:support@trendmicro.com">support@trendmicro.com</a>                                   |

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

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

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

## **Sending Suspicious Content to Trend Micro**

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

### **Email Reputation Services**

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

<https://servicecentral.trendmicro.com/en-us/ers/>

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

<https://success.trendmicro.com/solution/1112106>

### **File Reputation Services**

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

<https://success.trendmicro.com/solution/1059565>

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

## Other Resources

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

## Download Center

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

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

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

## Documentation Feedback

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

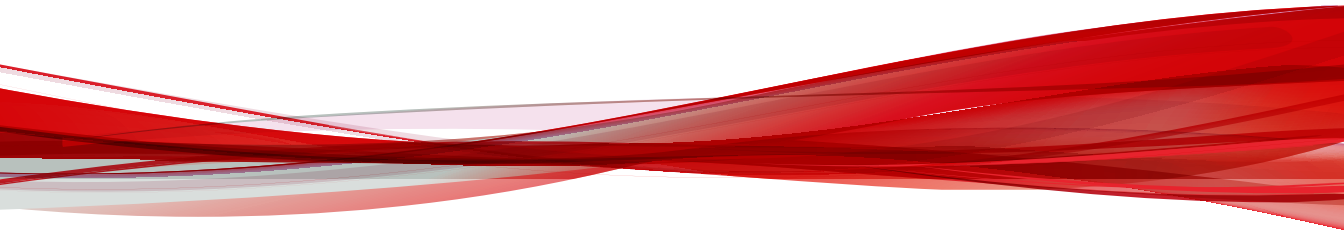
<https://docs.trendmicro.com/en-us/survey.aspx>



# Appendices

## Appendices

---





# Appendix A

## Using the Command Line Interface

Topics include:

- *Using the CLI on page A-2*
- *Entering the CLI on page A-2*
- *Command Line Interface Commands on page A-3*

## Using the CLI

Use the Command Line Interface (CLI) perform the following tasks:

- Configure initial settings, such as the device IP address and host name
- Restart the device
- View device status
- Debug and troubleshoot the device



### Note

Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

---

## Entering the CLI

To log on to the CLI, either connect directly to the server or connect using SSH.

---

### Procedure

- To connect directly to the server:
  - a. Connect a monitor and keyboard to the server.
  - b. Log on to the CLI.



### Note

The default credentials are:

- User name: `admin`
- Password: `ddei`

- 
- If the SSH service is enabled, do the following to connect using SSH:
    - a. Verify the computer you are using can ping Deep Discovery Email Inspector's IP address.

- b. Use an SSH client to connect to Deep Discovery Email Inspector's IP address and TCP port 22.

**Note**

The default IP address / subnet mask is 192.168.252.1 / 255.255.0.0.

## Command Line Interface Commands

The Deep Discovery Email 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**

CLI commands require privileged mode. For details, see [Entering Privileged Mode on page A-3](#).


## configure product management-port

**TABLE A-1. configure product management-port**

|  |  |
|--|--|
| Set the management port IP address   |  |
| <b>Syntax:</b><br><br>configure product management-port [ipv4   ipv6] <ip> <mask>                                  |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>ipv4:</b> Configure IPv4 settings<br><b>ipv6:</b> Configure IPv6 settings<br><b>&lt;ip&gt;:</b> IP address for the interface<br><b>&lt;mask&gt;:</b> Network mask for the NIC |
| <b>Example:</b>  |  |
| To set the management port IPv4 address:<br><br>configure product management-port ipv4 192.168.10.21 255.255.255.0 |  |

## configure product operation-mode

**TABLE A-2. configure product operation-mode**

|  |  |
|--|--|
| Set the Deep Discovery Email Inspector operation mode  |  |
| <div> <b>Note</b></div> <div>Deep Discovery Email Inspector virtual appliances installed in Microsoft Hyper-V do not support SPAN/TAP mode.</div> |  |
| <b>Syntax:</b><br><br>configure product operation-mode [BCC   MTA   TAP]   |  |

|  |   |
|--|---|
| <b>View</b>  | Privileged  |
| <b>Parameters</b>  | <b>BCC:</b> Deploy in BCC mode<br><b>MTA:</b> Deploy in MTA mode<br><b>TAP:</b> Deploy in SPAN/TAP mode |
| <b>Example:</b>  |   |
| To deploy in BCC mode:<br><br>configure product operation-mode BCC |   |

configure network basic

TABLE A-3. configure network basic

|  |            |
|--|------------|
| Configures basic network settings, including host name, IP address, subnet mask, gateway, and DNS. |            |
| <b>Syntax:</b><br><br>configure network basic  |            |
| <b>View</b>  | Privileged |
| <b>Parameters</b>  | None       |
| <b>Examples:</b>   |            |

```
***Network Configuration***

Specify value for each item and press ENTER. Settings apply to the
management port (Eth0) and require a restart.

Host name: mail.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

IPv6 address:

Prefix length:

IPv6 gateway:

Preferred IPv6 DNS:


Alternate IPv6 DNS:

Confirm changes and restart (Y/N):
```

configure network dns

TABLE A-4. configure network dns

|   |            |
|---|------------|
| Configures DNS settings for the Deep Discovery Email Inspector device.  |            |
| <b>Syntax:</b><br><br>configure network dns [ipv4   ipv6] <dns1> <dns2> |            |
| <b>View</b>   | Privileged |

|   |   |
|---|---|
| <b>Parameters</b>   | <p><b>ipv4:</b> Configure IPv4 settings</p> <p><b>ipv6:</b> Configure IPv6 settings</p> <p><b>&lt;dns1&gt;:</b> Primary DNS server</p> <p><b>&lt;dns2&gt;:</b> Secondary DNS server</p> <div> <b>Note</b><br/>Use a space to separate the primary and secondary DNS value.</div> |
| <b>Examples:</b>  |   |
| To configure the primary DNS with an IP address of 192.168.10.21:<br><code>configure network dns ipv4 192.168.10.21</code>  |   |
| To configure the primary and secondary DNS with the following values: <ul style="list-style-type: none"><li>• Primary DNS: 192.168.10.21</li><li>• Secondary DNS: 192.168.10.22</li></ul> <code>configure network dns ipv4 192.168.10.21 192.168.10.22</code> |   |

## configure network hostname

**TABLE A-5. configure network hostname**

|  |  |
|--|--|
| Configures the host name for the Deep Discovery Email Inspector device.  |  |
| <b>Syntax:</b><br><code>configure network hostname &lt;hostname&gt;</code>   |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>&lt;hostname&gt;:</b> The host name or fully qualified domain name (FQDN) for the Deep Discovery Email Inspector device |
| <b>Examples:</b>   |  |
| To change the host name of the Deep Discovery Email Inspector device to test.host.com:<br><code>configure network hostname test.example.com</code> |  |

## configure network interface

**TABLE A-6. configure network interface**

|  |  |
|--|--|
| Configures the IP address for the network interface card (NIC).  |  |
| <b>Syntax:</b><br><code>configure network interface [ipv4   ipv6] &lt;interface&gt; &lt;ip&gt; &lt;mask&gt;</code>   |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>ipv4:</b> Configure IPv4 settings<br><b>ipv6:</b> Configure IPv6 settings<br><b>&lt;interface&gt;:</b> NIC name<br><b>&lt;ip&gt;:</b> IP address for the interface<br><b>&lt;mask&gt;:</b> Network mask for the NIC |
| <b>Example:</b><br>To configure an NIC with the following values: <ul style="list-style-type: none"> <li>Interface: eth0</li> <li>IPv4 address: 192.168.10.10</li> <li>IPv4 subnet mask: 255.255.255.0</li> </ul> <code>configure network interface ipv4 eth0 192.168.10.10 255.255.255.0</code> |  |

## configure network teaming reinit

**TABLE A-7. configure network teaming reinit**

|   |            |
|---|------------|
| Disables network interface card (NIC) teaming and restores network card configuration |            |
| <b>Syntax:</b><br><code>configure network teaming reinit</code>                       |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Example:</b>   |            |

To disable NIC teaming:  
`configure network teaming reinit`

## configure network route add

TABLE A-8. configure network route add

|   |   |
|---|---|
| Adds a new route entry  |   |
| <b>Syntax:</b><br><code>configure network route add [ipv4   ipv6] &lt;ip_prefixlen&gt; &lt;via&gt; &lt;dev&gt;</code> |   |
| <b>View</b>   | Privileged  |
| <b>Parameters</b>   | <b>ipv4:</b> Configure IPv4 settings<br><b>ipv6:</b> Configure IPv6 settings<br><b>&lt;ip_prefixlen&gt;:</b> Destination network ID with format IP_Address/Prefixlen<br><b>&lt;via&gt;:</b> IP address of the next hop<br><b>&lt;dev&gt;:</b> Device name |
| <b>Example:</b>   |   |
| To add a new route entry:<br><code>configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1</code>           |   |

## configure network route default

TABLE A-9. configure network route default

|  |            |
|--|------------|
| Sets the default route   |            |
| <b>Syntax:</b><br><code>configure network route default [ipv4   ipv6] &lt;gateway&gt;</code> |            |
| <b>View</b>  | Privileged |

|   |  |
|---|--|
| <b>Parameter</b>  | <b>ipv4</b> : Configure IPv4 settings<br><b>ipv6</b> : Configure IPv6 settings<br><b>&lt;gateway&gt;</b> : IP address of default gateway |
| <b>Example:</b>   |  |
| To set the default route for the Deep Discovery Email Inspector appliance:<br><br>configure network route default ipv4 192.168.10.1 |  |

## configure network route del

**TABLE A-10. configure network route del**

|  |  |
|--|--|
| Deletes a route  |  |
| <b>Syntax:</b><br><br>configure network route del [ipv4   ipv6] <ip_prefixlen> <via> <dev>   |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>ipv4</b> : Configure IPv4 settings<br><b>ipv6</b> : Configure IPv6 settings<br><b>&lt;ip_prefixlen&gt;</b> : Destination network ID with format IP_Address/Prefixlen<br><b>&lt;via&gt;</b> : IPv4 address of the next hop<br><b>&lt;dev&gt;</b> : Device name |
| <b>Example:</b>  |  |
| To delete a route for the Deep Discovery Email Inspector appliance:<br><br>configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1 |  |

## configure network route del default/default ipv6

**TABLE A-11. configure network route del default/default ipv6**

|                                  |
|----------------------------------|
| Deletes the default IPv6 gateway |
|----------------------------------|

|   |  |
|---|--|
| <b>Syntax:</b><br>configure network route del default ipv6 <gateway> <device>   |  |
| <b>View</b>   | Privileged   |
| <b>Parameters</b>   | gateway: IPv6 Address of the default gateway<br>device: Link local to IPv6 default gateway |
| <b>Example:</b><br><br>To delete the default IPv6 gateway fe80::20c:29ff:fe75:b579 on device eth0: configure network route del default ipv6 fe80::20c:29ff:fe75:b579 eth0 |  |

configure service nscd disable

TABLE A-12. configure service nscd disable

|  |            |
|--|------------|
| Disables the name service cache daemon (nscd) at system startup.   |            |
| <b>Syntax:</b><br>configure service nscd disable   |            |
| <b>View</b>  | Privileged |
| <b>Parameters</b>  | None       |
| <b>Example:</b><br><br>To disable the name service cache daemon at system startup:<br><br>configure service nscd disable |            |

configure service nscd enable

TABLE A-13. configure service nscd enable

|   |            |
|---|------------|
| Enables the name service cache daemon (nscd) at system startup. |            |
| <b>Syntax:</b><br>configure service nscd enable                 |            |
| <b>View</b>   | Privileged |

|  |      |
|--|------|
| <b>Parameters</b>  | None |
| <b>Example:</b>  |      |
| To enable the name service cache daemon at system startup:<br><code>configure service nscd enable</code> |      |

## configure service ssh disable

**TABLE A-14. configure service ssh disable**

|   |            |
|---|------------|
| Disables SSH on all network interface cards (NIC).                        |            |
| <b>Syntax:</b><br><code>configure service ssh disable</code>              |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Examples:</b>  |            |
| To disable SSH on all NICs:<br><code>configure service ssh disable</code> |            |

## configure service ssh enable

**TABLE A-15. configure service ssh enable**

|   |            |
|---|------------|
| Enables SSH on one specific network interface card (NIC).   |            |
| <b>Syntax:</b><br><code>configure service ssh enable</code> |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Examples:</b>  |            |

To enable SSH:

```
configure service ssh enable
```

### configure service ssh port

TABLE A-16. configure service ssh port

|   |   |
|---|---|
| Change SSH service port.  |   |
| <b>Syntax:</b><br><code>configure service ssh port &lt;port&gt;</code>  |   |
| <b>View</b>   | Privileged  |
| <b>Parameters</b>   | port: configure the SSH service port<br><br><port>: SSH service port number |
| <b>Example:</b><br><br>To change the SSH service port to 56743: <code>configure service ssh port 56743</code> |   |

### configure service ntp

TABLE A-17. configure service ntp

|  |   |
|--|---|
| Synchronize the Deep Discovery Email Inspector system time with an NTP server.                           |   |
| <b>Syntax:</b><br><code>configure service ntp [enable   disable   server-address &lt;address&gt;]</code> |   |
| <b>View</b>  | Privileged  |
| <b>Parameters</b>  | <b>enable:</b> Enable NTP<br><br><b>disable:</b> Disable NTP<br><br><b>server-address:</b> Configure the NTP server address<br><br><b>&lt;address&gt;:</b> Specify the FQDN or IP address of the NTP server |
| <b>Examples:</b>   |   |

To configure the NTP server address as 192.168.10.21:

```
configure service ntp server-address 192.168.10.21
```

To enable synchronization with the NTP server:

```
configure service ntp enable
```

## configure system date

**TABLE A-18. configure system date**

|  |   |
|--|---|
| Configures the time and date and saves the data in CMOS.   |   |
| <b>Syntax:</b><br><pre>configure system date &lt;date&gt; &lt;time&gt;</pre>   |   |
| <b>View</b>  | Privileged  |
| <b>Parameters</b>  | <b>&lt;date&gt;:</b> Set the date using the following format: <b>yyyy-mm-dd</b><br><b>&lt;time&gt;:</b> Set the time with the following format: <b>hh:mm:ss</b> |
| <b>Example:</b><br>To set the date to August 12, 2010 and the time to 3:40 PM:<br><pre>configure system date 2010-08-12 15:40:00</pre> |   |

## configure system password enable

**TABLE A-19. configure system password enable**

|   |            |
|---|------------|
| To change the password required to enter Privileged mode.     |            |
| <b>Syntax:</b><br><pre>configure system password enable</pre> |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Examples:</b>  |            |

To change the password required to enter Privileged mode:

```
configure system password enable
```

configure system timezone

TABLE A-20. configure system timezone

|   |  |
|---|--|
| Configures the time zone used by Deep Discovery Email Inspector.  |  |
| <b>Syntax:</b><br><br>configure system timezone <region> <city>   |  |
| <b>View</b>   | Privileged                                     |
| <b>Parameters</b>   | <region>: Region name<br><br><city>: City name |
| <b>Example:</b>   |  |
| To configure the Deep Discovery Email Inspector appliance to use the time zone for the following location:<br><br>Region: America<br><br>City: New York<br><br>configure system timezone America New_York |  |

TABLE A-21. Time Zone Setting Examples

| REGION/COUNTRY | CITY         |
|----------------|--------------|
| Africa         | Cairo        |
|                | Harare       |
|                | Nairobi      |
| America        | Anchorage    |
|                | Bogota       |
|                | Buenos_Aires |

| REGION/COUNTRY | CITY        |
|----------------|-------------|
|                | Caracas     |
|                | Chicago     |
|                | Chihuahua   |
|                | Denver      |
|                | Godthab     |
|                | Lima        |
|                | Los_Angeles |
|                | Mexico_City |
|                | New_York    |
|                | Noronha     |
|                | Phoenix     |
|                | Santiago    |
|                | St_Johns    |
|                | Tegucigalpa |
| Asia           | Almaty      |
|                | Baghdad     |
|                | Baku        |
|                | Bangkok     |
|                | Calcutta    |
|                | Colombo     |
|                | Dhaka       |
|                | Hong_Kong   |
|                | Irkutsk     |

| REGION/COUNTRY   | CITY         |
|------------------|--------------|
|                  | Jerusalem    |
|                  | Kabul        |
|                  | Karachi      |
|                  | Katmandu     |
|                  | Krasnoyarsk  |
|                  | Kuala_Lumpur |
|                  | Kuwait       |
|                  | Magadan      |
|                  | Manila       |
|                  | Muscat       |
|                  | Rangoon      |
|                  | Seoul        |
|                  | Shanghai     |
| Asia (Continued) | Singapore    |
|                  | Taipei       |
|                  | Tehran       |
|                  | Tokyo        |
|                  | Yakutsk      |
| Atlantic         | Azores       |
| Australia        | Adelaide     |
|                  | Brisbane     |
|                  | Darwin       |
|                  | Hobart       |

| REGION/COUNTRY | CITY         |
|----------------|--------------|
|                | Melbourne    |
|                | Perth        |
| Europe         | Amsterdam    |
|                | Athens       |
|                | Belgrade     |
|                | Berlin       |
|                | Brussels     |
|                | Bucharest    |
|                | Dublin       |
|                | Moscow       |
|                | Paris        |
| Pacific        | Auckland     |
|                | Fiji         |
|                | Guam         |
|                | Honolulu     |
|                | Kwajalein    |
|                | Midway       |
| US             | Alaska       |
|                | Arizona      |
|                | Central      |
|                | East-Indiana |
|                | Eastern      |
|                | Hawaii       |

| REGION/COUNTRY | CITY     |
|----------------|----------|
|                | Mountain |
|                | Pacific  |

enable

TABLE A-22. enable

|  |        |
|--|--------|
| Enters privileged mode so privileged commands can be provided. |        |
| <b>Syntax:</b><br><br>enable                                   |        |
| <b>View</b>  | Normal |
| <b>Parameters</b>  | None   |
| <b>Example:</b><br><br>To enter privileged mode:<br><br>enable |        |

exit

TABLE A-23. exit

|   |        |
|---|--------|
| Exits privileged mode.<br><br>Exits the session for those not in privileged mode. |        |
| <b>Syntax:</b><br><br>exit  |        |
| <b>View</b>   | Normal |
| <b>Parameters</b>   | None   |
| <b>Example:</b>   |        |

To exit privileged mode or to exit the session when not in privileged mode:

```
exit
```

## help

**TABLE A-24. help**

|  |        |
|--|--------|
| Displays the CLI help information.               |        |
| <b>Syntax:</b><br><br>help                       |        |
| <b>View</b>                                      | Normal |
| <b>Parameters</b>                                | None   |
| <b>Example:</b>                                  |        |
| To display the CLI help information:<br><br>help |        |

## history

**TABLE A-25. history**

|  |  |
|--|--|
| Displays the current session's command line history.                       |  |
| <b>Syntax:</b><br><br>history [limit]                                      |  |
| <b>View</b>  | Normal   |
| <b>Parameters</b>  | <b>[limit]:</b> Specifies the size of the history list for the current session<br><br>Specifying "0" retains all commands for the session. |
| <b>Example:</b>  |  |
| To specify six commands for the size of the history list:<br><br>history 6 |  |

## logout

**TABLE A-26. logout**

|   |        |
|---|--------|
| Logs out of the current CLI session.              |        |
| <b>Syntax:</b><br><br>logout                      |        |
| <b>View</b>                                       | Normal |
| <b>Parameters</b>                                 | None   |
| <b>Example:</b>                                   |        |
| To logout from the current session:<br><br>logout |        |

## ping

**TABLE A-27. ping**

|  |  |
|--|--|
| Pings a specified host.  |  |
| <b>Syntax:</b><br><br>ping [-c num_echos] [-i interval] <dest> |  |
| <b>View</b>  | Normal   |
| <b>Parameters</b>  | <p><b>[-c num_echos]:</b> Specifies the number of echo requests to be sent. Default value is 5.</p> <p><b>[-i interval]:</b> Specifies the delay interval in seconds between each packet. Default value is 1 second.</p> <p><b>&lt;dest&gt;:</b> Specifies the destination host name or IP address</p> |
| <b>Examples:</b>   |  |
| To ping the IP address 192.168.1.1:<br><br>ping 192.168.1.1    |  |

To ping the host remote.host.com:

```
ping remote.host.com
```

## ping6

**TABLE A-28. ping6**

|   |  |
|---|--|
| Pings a specified IPv6 host through interface eth0.   |  |
| <b>Syntax:</b><br><pre>ping6 [-c num_echos] [-i interval] &lt;dest&gt;</pre>                    |  |
| <b>View</b>   | Normal   |
| <b>Parameters</b>   | <p><b>[-c num_echos]:</b> Specifies the number of echo requests to be sent. Default value is 5.</p> <p><b>[-i interval]:</b> Specifies the delay interval in seconds between each packet. Default value is 1 second.</p> <p><b>&lt;dest&gt;:</b> Specifies the destination host name or IP address</p> |
| <b>Examples:</b>  |  |
| To ping the IPv6 address fe80::21a:a5ff:fec1:1060:<br><pre>ping6 fe80::21a:a5ff:fec1:1060</pre> |  |
| To ping the host remote.host.com:<br><pre>ping6 remote.host.com</pre>                           |  |

## start task postfix drop

**TABLE A-29. start task postfix drop**

|  |            |
|--|------------|
| Deletes a specified message or all messages in the email message queue.        |            |
| <b>Syntax:</b><br><pre>start task postfix drop { &lt;mail_id&gt;   all }</pre> |            |
| <b>View</b>  | Privileged |

|   |  |
|---|--|
| <b>Parameters</b>   | <b>&lt;mail_id&gt;</b> : Specifies the message ID in the postfix queue to delete |
| <b>Examples:</b>  |  |
| To delete email message D10D4478A5 from the email message queue:<br><code>start task postfix drop D10D4478A5</code> |  |
| To delete all email messages from the email message queue:<br><code>start task postfix drop all</code>              |  |

### start task postfix flush

**TABLE A-30. start task postfix flush**

|  |            |
|--|------------|
| Attempts to deliver all queued email messages.                                 |            |
| <b>Syntax:</b><br><code>start task postfix flush</code>                        |            |
| <b>View</b>  | Privileged |
| <b>Parameters</b>  | None       |
| <b>Example:</b>  |            |
| To deliver all queued email messages:<br><code>start task postfix flush</code> |            |

### start task postfix queue

**TABLE A-31. start task postfix queue**

|   |            |
|---|------------|
| Displays all email messages queued in Postfix.          |            |
| <b>Syntax:</b><br><code>start task postfix queue</code> |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>                                       | None       |

**Example:**

To display all Postfix queued email messages:

```
start task postfix queue
```

## start service nscd

**TABLE A-32. start service nscd**

Starts the name service cache daemon (nscd).

**Syntax:**

```
start service nscd
```

**View**

Privileged

**Parameters**

None

**Example:**

To start the name service cache daemon:

```
start service nscd
```

## start service postfix

**TABLE A-33. start service postfix**

Starts the Postfix mail system

**Syntax:**

```
start service postfix
```

**View**

Privileged

**Parameters**

None

**Example:**

To start the Postfix mail system:

```
start service postfix
```

## start service product

**TABLE A-34. start service product**

|   |            |
|---|------------|
| Starts the Product service system.                                |            |
| <b>Syntax:</b><br><br>start service product                       |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Example:</b>   |            |
| To start the Product service system:<br><br>start service product |            |

## start service ssh

**TABLE A-35. start service ssh**

|   |            |
|---|------------|
| Starts the ssh service system.                            |            |
| <b>Syntax:</b><br><br>start service ssh                   |            |
| <b>View</b>   | Privileged |
| <b>Parameters</b>   | None       |
| <b>Example:</b>   |            |
| To start the ssh service system:<br><br>start ssh service |            |

## stop process core

**TABLE A-36. stop process core**

|  |
|--|
| Stops a running process and generates a core file. |
|--|

|  |                                     |
|--|-------------------------------------|
| <b>Syntax:</b><br><code>stop process core &lt;pid&gt;</code>       |                                     |
| <b>View</b>  | Privileged                          |
| <b>Parameters</b>  | <b>&lt;pid&gt;</b> : The process ID |
| <b>Example:</b>  |                                     |
| To stop a process with ID 33:<br><code>stop process core 33</code> |                                     |

## stop service nscd

**TABLE A-37. stop service nscd**

|  |            |
|--|------------|
| Stops the name service cache daemon (nscd).                              |            |
| <b>Syntax:</b><br><code>stop service nscd</code>                         |            |
| <b>View</b>  | Privileged |
| <b>Parameters</b>  | None       |
| <b>Example:</b>  |            |
| To stop the name service cache daemon:<br><code>stop service nscd</code> |            |

## stop service postfix

**TABLE A-38. stop service postfix**

|   |            |
|---|------------|
| Stops the Postfix mail system.                      |            |
| <b>Syntax:</b><br><code>stop service postfix</code> |            |
| <b>View</b>   | Privileged |

|   |      |
|---|------|
| <b>Parameters</b>   | None |
| <b>Example:</b>   |      |
| To stop the Postfix mail system:<br><code>stop service postfix</code> |      |

## stop service product

**TABLE A-39. stop service product**

|  |            |
|--|------------|
| Stops the Product service system.  |            |
| <b>Syntax:</b><br><code>stop service product</code>                      |            |
| <b>View</b>  | Privileged |
| <b>Parameters</b>  | None       |
| <b>Example:</b>  |            |
| To stop the Product service system:<br><code>stop service product</code> |            |

## stop service ssh

**TABLE A-40. stop service ssh**

|   |            |
|---|------------|
| Stops the ssh service system.                   |            |
| <b>Syntax:</b><br><code>stop service ssh</code> |            |
| <b>View</b>                                     | Privileged |
| <b>Parameters</b>                               | None       |
| <b>Example:</b>                                 |            |

To stop the ssh service system:

```
stop ssh service
```

## reboot

**TABLE A-41. reboot**

|  |  |
|--|--|
| Reboots the Deep Discovery Email Inspector appliance immediately or after a specified delay.     |  |
| <b>Syntax:</b><br><code>reboot [time]</code>   |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>[time]:</b> Specifies the delay, in minutes, to reboot the Deep Discovery Email Inspector appliance |
| <b>Examples:</b>   |  |
| To reboot the Deep Discovery Email Inspector appliance immediately:<br><code>reboot</code>       |  |
| To reboot the Deep Discovery Email Inspector appliance after 5 minutes:<br><code>reboot 5</code> |  |

## resolve

**TABLE A-42. resolve**

|   |   |
|---|---|
| Resolves an IPv4 address from a host name or resolves a host name from an IPv4 address. |   |
| <b>Syntax:</b><br><code>resolve &lt;dest&gt;</code>                                     |   |
| <b>View</b>   | Privileged  |
| <b>Parameter</b>  | <b>&lt;dest&gt;:</b> Specifies the IPv4 address or host name to resolve |
| <b>Examples:</b>  |   |

|   |
|---|
| To resolve the host name from IP address 192.168.10.1:    |
| <code>resolve 192.168.10.1</code>                         |
| To resolve the IP address from host name parent.host.com: |
| <code>resolve parent.host.com</code>                      |

show storage statistic

TABLE A-43. show storage statistic

|   |  |
|---|--|
| Displays the file system disk space usage.  |  |
| <b>Syntax:</b><br><code>show storage statistic [partition]</code>   |  |
| <b>View</b>   | Normal   |
| <b>Parameters</b>   | <b>[partition]:</b> Specify a partition. This is optional. |
| <b>Example:</b>   |  |
| To display the file system disk space usage of the Deep Discovery Email Inspector appliance:<br><code>show storage statistic</code> |  |

show network

TABLE A-44. show network

|  |        |
|--|--------|
| Displays various Deep Discovery Email Inspector network configurations.  |        |
| <b>Syntax:</b><br><code>show network [arp &lt;address&gt;   connections   dns   dns ipv6   hostname   interface   route   route ipv4   route default ipv4   route default ipv6]</code> |        |
| <b>View</b>  | Normal |

|   |   |
|---|---|
| <b>Parameters</b>   | <p><b>arp:</b> Displays the value returned by the Address Resolution Protocol (ARP) for the given address.</p> <p><b>&lt;address&gt;:</b> FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP).</p> <p><b>connections:</b> Displays the current network connections of the Deep Discovery Email Inspector appliance.</p> <p><b>dns:</b> Displays the DNS IP address of the Deep Discovery Email Inspector appliance.</p> <p><b>dns ipv6:</b> Displays system DNS configuration for IPv6.</p> <p><b>hostname:</b> Displays the host name of the Deep Discovery Email Inspector appliance.</p> <p><b>interface:</b> Displays the network interface card (NIC) status and configuration.</p> <p><b>route:</b> Displays IP address route table.</p> <p><b>route ipv4:</b> Displays system IPv4 route table.</p> <p><b>route default ipv4:</b> Displays default IPv4 route table.</p> <p><b>route default ipv6:</b> Display default IPv6 route table.</p> |
| <b>Examples:</b>  |   |
| To display the ARP information for the address 10.2.23.41:                                  |   |
| <pre>show network arp 10.2.23.41</pre>  |   |
| To display the current network connections of the Deep Discovery Email Inspector appliance: |   |
| <pre>show network connections</pre>   |   |
| To display the DNS configuration:   |   |
| <pre>show network dns</pre>   |   |
| To display system DNS configuration for IPv6:   |   |
| <pre>show network dns ipv6</pre>  |   |
| To display the host name of the Deep Discovery Email Inspector appliance:                   |   |
| <pre>show network hostname</pre>  |   |

|  |
|--|
| To display the NIC status and configuration: |
| <code>show network interface</code>          |
| To display the IP address route table:       |
| <code>show network route</code>              |
| To display system IPv4 route table:          |
| <code>show network route ipv4</code>         |
| To display system default IPv4 gateway:      |
| <code>show network route default ipv4</code> |
| To display system default IPv6 gateway:      |
| <code>show network route default ipv6</code> |

show kernel

TABLE A-45. show kernel

|   |   |
|---|---|
| Displays the OS kernel information of the Deep Discovery Email Inspector appliance.   |   |
| <b>Syntax:</b><br><code>show kernel {messages   modules   parameters   iostat}</code> |   |
| <b>View</b>   | Normal  |
| <b>Parameters</b>   | <b>messages:</b> Displays kernel messages.<br><b>modules:</b> Displays kernel modules.<br><b>parameters:</b> Displays kernel parameters.<br><b>iostat:</b> Displays CPU statistics and I/O statistics for devices and partitions. |
| <b>Examples:</b>  |   |
| To display the OS kernel's messages:<br><code>show kernel messages</code>             |   |

To display the OS kernel's modules:

```
show kernel modules
```

To display the OS kernel's parameters:

```
show kernel parameters
```

To display the CPU statistics and I/O statistics:

```
show kernel iostat
```

## show service

**TABLE A-46. show service**

|   |   |
|---|---|
| Displays the Deep Discovery Email Inspector service status.                                   |   |
| <b>Syntax:</b><br><pre>show service [ntp &lt;enabled   server-address&gt;   ssh   nscd]</pre> |   |
| <b>View</b>   | Normal  |
| <b>Parameters</b>   | <p><b>nscd:</b> Displays the status of the name service cache daemon.</p> <p><b>ntp enabled:</b> Displays the system NTP service status.</p> <p><b>ntp server-address:</b> Displays the system NTP service server address.</p> <p><b>ssh:</b> Displays the status of SSH.</p> |
| <b>Examples:</b>  |   |
| To display the name service cache daemon status:<br><pre>show service nscd</pre>              |   |
| To display the NTP service status:<br><pre>show service ntp</pre>                             |   |
| To display the SSH status:<br><pre>show service ssh</pre>                                     |   |

## show memory

TABLE A-47. show memory

|   |  |
|---|--|
| Displays the system memory information.                               |  |
| <b>Syntax:</b><br><br>show memory [vm   statistic]                    |  |
| <b>View</b>   | Normal   |
| <b>Parameters</b>   | <b>vm:</b> Displays virtual memory statistics<br><br><b>statistic:</b> Displays system memory statistics |
| <b>Examples:</b>  |  |
| To display the virtual memory statistics:<br><br>show memory vm       |  |
| To display the system memory statistics:<br><br>show memory statistic |  |

## show process

TABLE A-48. showprocess

|   |  |
|---|--|
| Displays the status of the processes that are currently running.        |  |
| <b>Syntax:</b><br><br>show process [top   stack   itrace   trace] [pid] |  |
| <b>View</b>   | Normal   |
| <b>Parameters</b>   | <b>top:</b> Displays the status of the processes that are currently running and system related processes<br><br><b>stack:</b> Print a stack trace of a running process<br><br><b>itrace:</b> Trace the library call<br><br><b>trace:</b> Trace system calls and signals<br><br><b>pid:</b> The process id number |

**Examples:**

To display the status of the processes that are currently running:

```
show process
```

To display the stack trace of process 1233:

```
show process stack 1233
```

To display the system call of process 1233:

```
show process trace 1233
```

To display the library call of process 1233:

```
show process itrace 1233
```

## show product-info

**TABLE A-49. show product-info**

|  |  |
|--|--|
| Displays the product information.  |  |
| <b>Syntax:</b><br><pre>show product-info [management-port   operation-mode   service-status   version]</pre> |  |
| <b>View</b>  | Normal   |
| <b>Parameters</b>  | <p><b>management-port:</b> Displays the management port's IP address and subnet mask</p> <p><b>operation-mode:</b> Displays the operation mode of Deep Discovery Email Inspector</p> <p><b>service-status:</b> Displays the status of services</p> <p><b>version:</b> Displays the product version</p> |
| <b>Examples:</b>   |  |

To display the management port's IP address and mask: `show product-info management-port`

To display the operation mode: `show product-info operation-mode`

To display the status of the service: `show-product-info service-status`

To display the build version of Deep Discovery Email Inspector: `show product-info version`

show system

TABLE A-50. show system

|  |  |
|--|--|
| Displays various system settings.  |  |
| <b>Syntax:</b><br><br>show system [date   timezone [continent   city   country]] uptime   version]               |  |
| <b>View</b>  | Normal   |
| <b>Parameters</b>  | <p><b>date:</b> Displays the current time and date.</p> <p><b>timezone:</b> Displays the timezone settings. You can optionally specify the timezone information to view:</p> <ul style="list-style-type: none"><li>• <b>continent:</b> Displays the system continent</li><li>• <b>city:</b> Displays the system city</li><li>• <b>country:</b> Displays the system country</li></ul> <p><b>uptime:</b> Displays how long the Deep Discovery Email Inspector appliance has been running.</p> <p><b>version:</b> Displays version number for the Deep Discovery Email Inspector appliance.</p> |
| <b>Examples:</b>   |  |
| <p>To display the current time and date of the Deep Discovery Email Inspector appliance:</p><br>show system date |  |

|   |
|---|
| To display the timezone settings:   |
| <code>show system timezone</code>   |
| To display the continent of the Deep Discovery Email Inspector appliance:           |
| <code>show system timezone continent</code>   |
| To display the city of the Deep Discovery Email Inspector appliance: device's city: |
| <code>show system timezone city</code>  |
| To display the country of the Deep Discovery Email Inspector appliance:             |
| <code>show system timezone country</code>   |
| To display how long Deep Discovery Email Inspector has been running:                |
| <code>show system uptime</code>   |
| To display the version number of the Deep Discovery Email Inspector appliance:      |
| <code>show system version</code>  |

## shutdown

**TABLE A-51. shutdown**

|  |  |
|--|--|
| Specifies shutting down the Deep Discovery Email Inspector appliance immediately or after a specified delay. |  |
| <b>Syntax:</b><br><code>shutdown [time]</code>   |  |
| <b>View</b>  | Privileged   |
| <b>Parameters</b>  | <b>[time]:</b> Shuts down the Deep Discovery Email Inspector appliance after a specified delay in minutes. |
| <b>Examples:</b>   |  |
| To shut down the Deep Discovery Email Inspector appliance immediately:<br><code>shutdown</code>              |  |

To shut down the Deep Discovery Email Inspector appliance after a 5 minute delay:

```
shutdown 5
```

traceroute

TABLE A-52. traceroute

|   |  |
|---|--|
| Displays the tracking route to a specified destination.   |  |
| <b>Syntax:</b><br><br>traceroute [-h hops] <dest>   |  |
| <b>View</b>   | Normal   |
| <b>Parameters</b>   | <b>[-h hops]:</b> Specifies the maximum number of hops to the destination. The minimum number is 6.<br><br><b>&lt;dest&gt;:</b> Specifies the remote system to trace |
| <b>Examples:</b>  |  |
| To display the route to IP address 172.10.10.1 with a maximum of 6 hops:<br><br>traceroute 172.10.10.1        |  |
| To display the route to IP address 172.10.10.1 with a maximum of 30 hops:<br><br>traceroute -h 30 172.10.10.1 |  |



# Appendix B

## Notification Message Tokens

Add message tokens to customize email message notifications.

Topics include:

- *[Recipient Notification Message Tokens on page B-2](#)*
- *[Alert Notification Message Tokens on page B-3](#)*

## Recipient Notification Message Tokens

Deep Discovery Email Inspector sends recipient notifications to inform recipients that an email message contained a detected threat. After acting upon an email message, Deep Discovery Email Inspector sends recipient notifications based on the detected risk level. Use the following table to customize your recipient notifications with message tokens.

**Note**

For information about configuring recipient notifications, see [Configuring Recipient Notification on page 5-54](#).

**TABLE B-1. Message Tokens**

| TOKEN             | DESCRIPTION  | EXAMPLE  |
|-------------------|--|--|
| %Action%          | The action that Deep Discovery Email Inspector took on the processed message | <ul style="list-style-type: none"><li>• Block and quarantine</li><li>• Strip attachments, redirect links to blocking page, and tag</li><li>• Strip attachments, redirect links to warning page, and tag</li><li>• Pass and tag</li><li>• Pass with no action</li></ul> |
| %AttachmentNames% | The top ten detected attachments   | important.doc  |
| %ConsoleURL%      | The Deep Discovery Email Inspector management console URL.                   | https://192.168.252.1/loginPage.ddei   |
| %DateTime%        | The date and time that the alert was triggered                               | 2014-03-21 03:34:09  |
| %DeviceIP%        | The IP address of the Deep Discovery Email Inspector appliance               | 123.123.123.123  |
| %DeviceName%      | The host name of the Deep Discovery Email Inspector appliance                | example.com  |

| TOKEN         | DESCRIPTION                      | EXAMPLE   |
|---------------|----------------------------------|---|
| %Risk%        | The email message's risk level   | <ul style="list-style-type: none"><li>• High</li><li>• Medium</li><li>• Low</li><li>• Unavailable</li></ul> |
| %Sender%      | The sending email address        | senderemail@example.com   |
| %Subject%     | The subject of the email message | Your dream job!   |
| %ThreatNames% | The top ten detected threats     | Spam/Graymail   |

## Alert Notification Message Tokens

The following table explains the tokens available for alert notifications. Use the table to customize your alert notifications with message tokens.



**Note**

Not every alert notification can accept every message token. Review the alert's parameter specifications before using a message token. For details, see [Alert Notification Parameters on page 6-7](#).

**TABLE B-2. Message Tokens**

| TOKEN     | DESCRIPTION  | NOTES  |
|-----------|--|--|
| %Account% | The user name of the account that Deep Discovery Email Inspector locks | Where allowed: <ul style="list-style-type: none"><li>• System: Account Locked</li></ul> Examples: <ul style="list-style-type: none"><li>• JohnDoe</li><li>• Test</li></ul> |

| TOKEN            | DESCRIPTION   | NOTES   |
|------------------|---|---|
| %Action%         | The action that Deep Discovery Email Inspector took on the processed message        | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>Policy: Recipient Notifications</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>Policy: Recipient Notifications</li> <li>Pass and tag</li> </ul>  |
| %AveSandboxProc% | The average time in minutes it takes to queue and analyze messages in the past hour | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>System: Long Virtual Analyzer Processing Time</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>3</li> <li>2</li> </ul>   |
| %ComponentList%  | The list of components.   | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>System: Component Update/Rollback Successful</li> <li>System: Component Update/Rollback Unsuccessful</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>Network Content Inspection Engine/ 0x48000204/ 9.862.1107</li> <li>Network Content Inspection Engine/ 0x48000204/ Unknown</li> </ul> |
| %ConsoleURL%     | The Deep Discovery Email Inspector management console URL.                          | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>All</li> </ul> <p>Example:</p> <ul style="list-style-type: none"> <li><a href="https://192.168.252.1/loginPage.ddei">https://192.168.252.1/loginPage.ddei</a></li> </ul>   |

| TOKEN                     | DESCRIPTION   | NOTES   |
|---------------------------|---|---|
| %CPUThreshold%            | The maximum CPU usage as a percentage allowed before Deep Discovery Email Inspector sends an alert notification | Where allowed: <ul style="list-style-type: none"> <li>• System: High CPU Usage</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 95</li> <li>• 85</li> </ul>                |
| %CPUUsage%                | The total CPU utilization as a percentage   | Where allowed: <ul style="list-style-type: none"> <li>• System: High CPU Usage</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 80</li> <li>• 65</li> </ul>                |
| %DateTime%                | The date and time that the Deep Discovery Email Inspector received the email message                            | Where allowed: <ul style="list-style-type: none"> <li>• All</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 2014-03-21 03:34:09</li> <li>• 2014-06-15 11:31:22</li> </ul> |
| %DaysBeforeExpirationATD% | The number of days before the product license for Advanced Threat Protection expires                            | Where allowed: <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 4</li> <li>• 123</li> </ul>            |
| %DaysBeforeExpirationSEG% | The number of days before the product license for Gateway Module expires  | Where allowed: <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> Examples: <ul style="list-style-type: none"> <li>• 4</li> <li>• 123</li> </ul>            |

| TOKEN                | DESCRIPTION  | NOTES   |
|----------------------|--|---|
| %DeferredQueue%      | The number of email messages in the deferred queue waiting for Deep Discovery Email Inspector to process.                                    | Where allowed: <ul style="list-style-type: none"> <li>System: Long Message Deferred Queue</li> </ul> Example: <ul style="list-style-type: none"> <li>100</li> </ul>               |
| %DeliveryQueue%      | The number of email messages in the delivery queue waiting for Deep Discovery Email Inspector to process.                                    | Where allowed: <ul style="list-style-type: none"> <li>System: Long Message Delivery Queue</li> </ul> Examples: <ul style="list-style-type: none"> <li>100</li> <li>600</li> </ul> |
| %DetectionCount%     | The number of messages detected with suspicious characteristics during the specified period of time  | Where allowed: <ul style="list-style-type: none"> <li>System: Detection Surge</li> </ul> Examples: <ul style="list-style-type: none"> <li>50</li> <li>200</li> </ul>              |
| %DetectionThreshold% | The maximum number of messages detected to have suspicious characteristics before Deep Discovery Email Inspector sends an alert notification | Where allowed: <ul style="list-style-type: none"> <li>System: Detection Surge</li> </ul> Examples: <ul style="list-style-type: none"> <li>50</li> <li>40</li> </ul>               |
| %DeviceIP%           | The IP address of the Deep Discovery Email Inspector appliance   | Where allowed: <ul style="list-style-type: none"> <li>All</li> </ul> Example: <ul style="list-style-type: none"> <li>123.123.123.123</li> </ul>                                   |

| TOKEN               | DESCRIPTION  | NOTES  |
|---------------------|--|--|
| %DeviceName%        | The host name of the Deep Discovery Email Inspector appliance  | Where allowed: <ul style="list-style-type: none"> <li>All</li> </ul> Example: <ul style="list-style-type: none"> <li>example.com</li> </ul>  |
| %DiagnosisTip%      | Recommendations on how to resolve the issue  | Where allowed: <ul style="list-style-type: none"> <li>System: Connection Issue</li> </ul>  |
| %DiskSpace%         | The lowest amount of disk space in GB before Deep Discovery Email Inspector send an alert notification | Where allowed: <ul style="list-style-type: none"> <li>System: Low Free Disk Space</li> <li>System: Low Free Quarantine Disk Space</li> </ul> Examples: <ul style="list-style-type: none"> <li>2</li> <li>30</li> </ul> |
| %ExpirationDateATD% | The day the product license for Advanced Threat Protection expires                                     | Where allowed: <ul style="list-style-type: none"> <li>System: License Expiration</li> </ul> Examples: <ul style="list-style-type: none"> <li>2014-03-21 03:34:09</li> <li>2014-06-15 11:31:22</li> </ul>               |
| %ExpirationDateSEG% | The day the product license for Gateway Module expires   | Where allowed: <ul style="list-style-type: none"> <li>System: License Expiration</li> </ul> Examples: <ul style="list-style-type: none"> <li>2014-03-21 03:34:09</li> <li>2014-06-15 11:31:22</li> </ul>               |
| %Interval%          | The frequency that Deep Discovery Email Inspector checks the message processing volume in minutes      | Where allowed: <ul style="list-style-type: none"> <li>System: Detection Surge</li> <li>System: Processing Surge</li> </ul>   |

| TOKEN              | DESCRIPTION  | NOTES   |
|--------------------|--|---|
|                    |  | <p>Examples:</p> <ul style="list-style-type: none"> <li>• 15</li> <li>• 10</li> </ul>   |
| %LicenseStatusATD% | The current status of the product license for Advanced Threat Protection | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Evaluation</li> <li>• Not Activated</li> <li>• Activated</li> <li>• Expired</li> <li>• Grace Period</li> </ul> <p>For details, see <a href="#">Product License Status on page 8-230</a>.</p> |
| %LicenseStatusSEG% | The current status of the product license for Gateway Module             | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Evaluation</li> <li>• Not Activated</li> <li>• Activated</li> <li>• Expired</li> <li>• Grace Period</li> </ul> <p>For details, see <a href="#">Product License Status on page 8-230</a>.</p> |
| %LicenseTypeATD%   | The Advanced Threat Protection product license type                      | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Full</li> </ul>  |

| TOKEN             | DESCRIPTION   | NOTES   |
|-------------------|---|---|
|                   |   | <ul style="list-style-type: none"> <li>• Trial</li> </ul>   |
| %LicenseTypeSEG%  | The Gateway Module product license type   | Where allowed: <ul style="list-style-type: none"> <li>• System: License Expiration</li> </ul> Examples: <ul style="list-style-type: none"> <li>• Full</li> <li>• Trial</li> </ul>   |
| %MemoryThreshold% | The maximum memory usage as a percentage allowed before Deep Discovery Email Inspector sends an alert notification.   | Where allowed: <ul style="list-style-type: none"> <li>• System: High Memory Usage</li> </ul> Example: 90  |
| %MemoryUsage%     | The total memory utilization as a percentage.   | Where allowed: <ul style="list-style-type: none"> <li>• System: High Memory Usage</li> </ul> Example: 90  |
| %MessageList%     | <p>The list of detected messages, which includes the risk level, threat name, action taken, message ID, recipients, sender, recipient, subject, top three most risky attachment details, and when the message was received.</p> <p>This token also provides the names of detected threats for the following alert notifications:</p> <ul style="list-style-type: none"> <li>• Security: Suspicious Message Identified</li> <li>• Security: Watchlisted Recipients at Risk</li> <li>• System: Quarantined Messages</li> <li>• Security: Data Loss Prevention Incident</li> </ul> | Where allowed: <ul style="list-style-type: none"> <li>• Security: Suspicious Message Identified</li> <li>• Security: Watchlisted Recipients at Risk</li> <li>• System: Quarantined Messages</li> <li>• Security: Data Loss Prevention Incident</li> </ul> Examples: <pre>===== Risk: High (Suspicious File) Action: Action set to 'pass' Threat Name: EMERGING-THREAT_GENERIC.ERS VAN</pre> |

| TOKEN | DESCRIPTION | NOTES  |
|-------|-------------|--|
|       |             | <p>_DROPPER.UMXX<br/>Message ID: &lt;E1fk6FQ-00073X-Ns@funimo.com&gt;<br/>Recipients: relay@njrelay.itlab.trendmicro.com<br/>Sender: aliconwamonic@yahoo.com<br/>Subject: Our Order#6501732<br/>Attachment: 65017832.xls (Excel 95 or 97 spreads heet), Company Profile.ZIP(ZIP archive)<br/>Detected: 2018-07-30 19:41:23<br/>=====</p> <p>=====<br/>Risk: Medium (Malicious URL)<br/>Action: Quarantined<br/>Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS<br/>Message ID: &lt;20180903210849.3B4D93A06C9@ddei155.localdomain<br/>Recipients: bvt@ddei.com<br/>Sender: test@test.com<br/>Subject: Te_%*s'&lt;&gt;? \@~\$%^&amp;\$!'~(=-+&lt;&gt;;..){[]}(')+=-_t"ddd, Attachment: (Link only)<br/>Detected: 2018-09-03 21:08:51<br/>=====</p> |

| TOKEN                 | DESCRIPTION  | NOTES   |
|-----------------------|--|---|
|                       |  | <pre> ===== Message ID: &lt;5C32BC03. 9090201@test.com&gt; Recipients: test@test. com;test@test1.com Sender: test@test.com Subject: 1033 Attachment: (Link only) DLP templates (Data id entifiers): templateName (China: M obile Phone Number ) Detected: 2019-02-25 01: 07:42 ===== </pre> |
| %MTAList%             | The list of unreachable MTAs. Each MTA appears as an IP address and the port number.   | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>System: Relay MTAs Inaccessible</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>[1.1.1.1]:99</li> <li>[7.7.7.7]:77</li> </ul>   |
| %ProcessingCount%     | The total number of processed messages over the specified period of time   | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>System: Processing Surge</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>50</li> <li>200</li> </ul>   |
| %ProcessingThreshold% | The maximum number of processed messages during the specified time frame before Deep Discovery Email Inspector sends an alert notification | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>System: Processing Surge</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>100</li> </ul>   |

| TOKEN                   | DESCRIPTION   | NOTES   |
|-------------------------|---|---|
|                         |   | <ul style="list-style-type: none"> <li>• 40</li> </ul>  |
| %QueueThreshold%        | The maximum number of messages in the delivery queue before Deep Discovery Email Inspector sends an alert notification                | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: Long Message Delivery Queue</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 100</li> <li>• 40</li> </ul>            |
| %SandboxProcThreshold%  | The maximum amount of time allocated for average sandbox processing before Deep Discovery Email Inspector sends an alert notification | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: Long Virtual Analyzer Processing Time</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 15</li> <li>• 30</li> </ul>   |
| %SandboxQueue%          | The email message count in the sandbox queue waiting to be analyzed by Virtual Analyzer   | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: Long Virtual Analyzer Submission Queue</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 30</li> <li>• 75</li> </ul>  |
| %SandboxQueueThreshold% | The maximum number of messages in the sandbox queue before Deep Discovery Email Inspector sends an alert notification                 | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: Long Virtual Analyzer Submission Queue</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• 100</li> <li>• 75</li> </ul> |
| %ServiceList%           | The list of services affected by the connection issue   | <p>Where allowed:</p> <ul style="list-style-type: none"> <li>• System: Connection Issue</li> </ul> <p>Example:</p>  |

| TOKEN           | DESCRIPTION   | NOTES   |
|-----------------|---|---|
|                 |   | <ul style="list-style-type: none"><li>Internal Virtual Analyzer network (eth1, No proxy)</li></ul>  |
| %ServiceName%   | <p>The stopped Deep Discovery Email Inspector service</p> <p>Where allowed:</p> <ul style="list-style-type: none"><li>System: Service Stopped</li></ul> | <p>Where allowed:</p> <ul style="list-style-type: none"><li>System: Service Stopped</li></ul> <p>Example:</p> <ul style="list-style-type: none"><li>scanner</li></ul>                 |
| %TotalMessages% | <p>The total number of messages with unsuccessful DKIM signing</p>  | <p>Where allowed:</p> <ul style="list-style-type: none"><li>System: Unsuccessful DKIM Signing</li></ul> <p>Example:</p> <ul style="list-style-type: none"><li>10</li><li>25</li></ul> |



# Appendix C

## Connections and Ports

## Service Addresses and Ports

Deep Discovery Email Inspector accesses several Trend Micro services to obtain information about emerging threats and to manage your existing Trend Micro products. The following table describes each service and provides the required address and port information accessible to the product version in your region.

**TABLE C-1. Service Addresses and Ports**

| SERVICE                                | DESCRIPTION  | ADDRESS AND PORT   |
|--|--|--|
| ActiveUpdate Server                    | Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.  | http://ddei50-p.activeupdate.trendmicro.com/activeupdate:80<br><br>https://ddei50-p.activeupdate.trendmicro.com/activeupdate:443 |
| Certified Safe Software Service (CSSS) | Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources.   | https://grid-global.trendmicro.com:443/ws/level-0/files:443  |
| Community File Reputation              | Determines the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time.                                    | ddei510-en-census.trendmicro.com:80  |
| Community Domain/IP Reputation Service | Determines the prevalence of detected domains and IP addresses. Prevalence is a statistical concept referring to the number of times a domain or IP address was detected by Trend Micro sensors at a given time. | ddei510-en-domaincensus.trendmicro.com:80  |
| Customer Licensing Portal              | Manages your customer information, subscriptions, and product or service license.  | licenseupdate.trendmicro.com:80<br><br>cpl.trendmicro.com:443  |

| SERVICE                            | DESCRIPTION   | ADDRESS AND PORT  |
|------------------------------------|---|---|
| Dynamic URL Scanning               | Performs real-time analysis of URLs to detect zero-day attacks.   | ddei5-0-en.url.trendmicro.com:80  |
| Email Encryption                   | Encrypts and decrypts email messages with registered domains using Identity-Based Encryption (IBE) for secure private information delivery.   | http://root.ibe-ta.com:80<br>http://public.ibe-ta.com:80<br>http://ppconfig.ibe-ta.com:80 |
| Predictive Machine Learning engine | Through use of malware modeling, Predictive Machine Learning compares samples to the malware models, assigns a probability score, and determines the probable malware type that a file contains.  | ddei51-en-f.trx.trendmicro.com:443  |
| Smart Feedback                     | Shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains. | ddei500-en.fbs25.trendmicro.com:443   |
| Time-of-Click Protection           | Detects unknown URLs in email messages by rewriting and analyzing URLs at the time of user clicks to protect users against link-based malware and phishing attacks.   | ddei5-0-ctp.trendmicro.com:443  |

| SERVICE                 | DESCRIPTION  | ADDRESS AND PORT  |
|-------------------------|--|---|
| Threat Connect          | Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.  | ddei5-threatconnect.trendmicro.com:443  |
| Web Inspection Service  | <p>Web Inspection Service is an auxiliary service of Web Reputation Services, providing granular levels of threat results and comprehensive threat names to users.</p> <p>The threat name and severity can be used as filtering criteria for proactive actions and further intensive scanning.</p> | ddei5-0-en-wis.trendmicro.com:443   |
| Web Reputation Services | Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis.   | <p>ddei5-0-en-url.trendmicro.com:80</p> <p>ddei5-0-en-backup.url.trendmicro.com:80</p> <p>ddei5-0-usbx-en.url.trendmicro.com:80 (for use by internal Virtual Analyzer)</p> <p>ddei5-0-usbx-en-backup.url.trendmicro.com:80 (for use by internal Virtual Analyzer)</p> |

## Ports Used by the Appliance

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

**TABLE C-2. Ports used by Deep Discovery Email Inspector**

| PORT | PROTOCOL | FUNCTION               | PURPOSE   |
|------|----------|------------------------|---|
| 22   | TCP      | Listening              | Endpoints connect to Deep Discovery Email Inspector through SSH.  |
| 25   | TCP      | Listening              | MTAs and mail servers connect to Deep Discovery Email Inspector through SMTP.   |
| 53   | TCP/UDP  | Outbound               | Deep Discovery Email Inspector uses this port for: <ul style="list-style-type: none"> <li>• DNS resolution</li> <li>• Sender authentication (SPF, DKIM, DMARC) query</li> </ul>   |
| 80   | TCP      | Listening and outbound | Deep Discovery Email Inspector connects to other computers and integrated Trend Micro products and hosted services through this port. <ul style="list-style-type: none"> <li>• Connect to the Customer Licensing Portal to manage the product licenses</li> <li>• Query Community File Reputation Services</li> <li>• Query Community Domain/IP Reputation Services</li> <li>• Query Web Reputation Services through the Smart Protection Network</li> <li>• Upload virtual analyzer images to Deep Discovery Email Inspector using the image import tool</li> <li>• Communicate with Trend Micro Apex Central if Deep Discovery Email Inspector is registered over HTTP</li> </ul> |

| PORT | PROTOCOL | FUNCTION  | PURPOSE  |
|------|----------|-----------|--|
| 123  | UDP      | Outbound  | Deep Discovery Email Inspector connects to the NTP server to synchronize time.           |
| 161  | UDP      | Listening | Deep Discovery Email Inspector uses this port to listen for requests from SNMP managers. |
| 162  | UDP      | Outbound  | Deep Discovery Email Inspector connects to SNMP managers to send SNMP trap messages.     |

| PORT | PROTOCOL | FUNCTION               | PURPOSE   |
|------|----------|------------------------|---|
| 443  | TCP      | Listening and outbound | <p>Deep Discovery Email Inspector uses this port to:</p> <ul style="list-style-type: none"><li>• Query Predictive Machine Learning engine</li><li>• Query Web Inspection Service</li><li>• Access the management console with a computer through HTTPS</li><li>• Communicate with Trend Micro Apex Central</li><li>• Connect to the Smart Protection Network and query Web Reputation Services</li><li>• Connect to Trend Micro Threat Connect</li><li>• Send protected threat information to Smart Feedback</li><li>• Update components by connecting to the ActiveUpdate server</li><li>• Send product usage information to Trend Micro feedback servers</li><li>• Verify the safety of files through the Certified Safe Software Service</li><li>• Communicate with Deep Discovery Director - On-premises version</li><li>• Share threat intelligence information and exception list with other products</li></ul> |
| 4459 | TCP      | Listening and outbound | <p>Endpoints connect to the End-User Quarantine console on Deep Discovery Email Inspector through this port.</p>  |

| PORT         | PROTOCOL | FUNCTION | PURPOSE   |
|--------------|----------|----------|---|
| 5274         | TCP      | Outbound | Deep Discovery Email Inspector uses this port as the default port to connect to the Smart Protection Server for web reputation services.  |
| User-defined | N/A      | Outbound | Deep Discovery Email Inspector uses specified ports to: <ul style="list-style-type: none"><li>• Send logs to syslog servers</li><li>• Share threat intelligence with integrated products/services</li><li>• Upload detection logs to SFTP servers</li><li>• Communicate with and Check Point Open Platform for Security (OPSEC)</li><li>• Connect to an LDAP server for third-party authentication and LDAP query</li></ul> |

# Appendix D

## SNMP Object Identifiers

Topics include:

- *SNMP Query Objects on page D-2*
- *SNMP Traps on page D-17*
- *Registration Objects on page D-30*

## SNMP Query Objects

**TABLE D-1. memTotalSwap**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.3                                    |
| <b>Object name</b> | memTotalSwap   |
| <b>Description</b> | The total amount of swap space configured for this host. |

**TABLE D-2. memAvailSwap**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.4                                   |
| <b>Object name</b> | memAvailSwap  |
| <b>Description</b> | The amount of swap space currently unused or available. |

**TABLE D-3. memTotalReal**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.5  |
| <b>Object name</b> | memTotalReal   |
| <b>Description</b> | The total amount of real/physical memory installed on this host. |

**TABLE D-4. memAvailReal**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.6   |
| <b>Object name</b> | memAvailReal  |
| <b>Description</b> | The amount of real/physical memory currently unused or available. |

**TABLE D-5. memTotalFree**

| ITEM       | DESCRIPTION            |
|------------|------------------------|
| <b>OID</b> | .1.3.6.1.4.1.2021.4.11 |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Object name</b> | memTotalFree  |
| <b>Description</b> | The total amount of memory free or available for use on this host. This value typically covers both real memory and swap space or virtual memory. |

**TABLE D-6. memMinimumSwap**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.12   |
| <b>Object name</b> | memMinimumSwap   |
| <b>Description</b> | The minimum amount of swap space expected to be kept free or available during normal operation of this host. If this value (as reported by 'memAvailSwap(4)') falls below the specified level, then 'memSwapError(100)' will be set to 1 and an error message made available via 'memSwapErrorMsg(101)'. |

**TABLE D-7. memShared**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.13   |
| <b>Object name</b> | memShared  |
| <b>Description</b> | The total amount of real or virtual memory currently allocated for use as shared memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose. |

**TABLE D-8. memBuffer**

| ITEM               | DESCRIPTION            |
|--------------------|------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.14 |
| <b>Object name</b> | memBuffer              |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | The total amount of real or virtual memory currently allocated for use as memory buffers. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose. |

**TABLE D-9. memCached**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.15  |
| <b>Object name</b> | memCached   |
| <b>Description</b> | The total amount of real or virtual memory currently allocated for use as cached memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as reserved for this purpose. |

**TABLE D-10. memSwapError**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.100   |
| <b>Object name</b> | memSwapError  |
| <b>Description</b> | Indicates whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)'). |

**TABLE D-11. memSwapErrorMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.4.101   |
| <b>Object name</b> | memSwapErrorMsg   |
| <b>Description</b> | Describes whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)'). |

**TABLE D-12. dskIndex**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.1                                 |
| <b>Object name</b> | dskIndex  |
| <b>Description</b> | Integer reference number (row number) for the disk mib. |

**TABLE D-13. dskPath**

| ITEM               | DESCRIPTION                     |
|--------------------|---------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.2         |
| <b>Object name</b> | dskPath                         |
| <b>Description</b> | Path where the disk is mounted. |

**TABLE D-14. dskDevice**

| ITEM               | DESCRIPTION                           |
|--------------------|---------------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.3               |
| <b>Object name</b> | dskDevice                             |
| <b>Description</b> | Path of the device for the partition. |

**TABLE D-15. dskMinimum**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.4   |
| <b>Object name</b> | dskMinimum  |
| <b>Description</b> | Minimum space required on the disk (in kBytes) before the errors are triggered. Either this or dskMinPercent is configured via the agent's snmpd.conf file. |

**TABLE D-16. dskMinPercent**

| ITEM       | DESCRIPTION             |
|------------|-------------------------|
| <b>OID</b> | .1.3.6.1.4.1.2021.9.1.5 |

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>Object name</b> | dskMinPercent  |
| <b>Description</b> | Percentage of minimum space required on the disk before the errors are triggered. Either this or dskMinimum is configured via the agent's snmpd.conf file. |

**TABLE D-17. dskTotal**

| ITEM               | DESCRIPTION                                |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.6                    |
| <b>Object name</b> | dskTotal                                   |
| <b>Description</b> | Total size of the disk/partition (kBytes). |

**TABLE D-18. dskAvail**

| ITEM               | DESCRIPTION             |
|--------------------|-------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.7 |
| <b>Object name</b> | dskAvail                |
| <b>Description</b> | Available disk space.   |

**TABLE D-19. dskUsed**

| ITEM               | DESCRIPTION             |
|--------------------|-------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.8 |
| <b>Object name</b> | dskUsed                 |
| <b>Description</b> | Disk space used.        |

**TABLE D-20. dskPercent**

| ITEM               | DESCRIPTION             |
|--------------------|-------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.9 |
| <b>Object name</b> | dskPercent              |

| ITEM               | DESCRIPTION                       |
|--------------------|-----------------------------------|
| <b>Description</b> | Percentage of space used on disk. |

**TABLE D-21. dskPercentNode**

| ITEM               | DESCRIPTION                        |
|--------------------|------------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.10           |
| <b>Object name</b> | dskPercentNode                     |
| <b>Description</b> | Percentage of inodes used on disk. |

**TABLE D-22. dskErrorFlag**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.100   |
| <b>Object name</b> | dskErrorFlag  |
| <b>Description</b> | Error flag indicating that the disk or partition is under the minimum required space configured for it. |

**TABLE D-23. dskErrorMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.9.1.101  |
| <b>Object name</b> | dskErrorMsg  |
| <b>Description</b> | A text description providing a warning and the space left on the disk. |

**TABLE D-24. ssSwapIn**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.3  |
| <b>Object name</b> | ssSwapIn  |
| <b>Description</b> | The average amount of memory swapped in from disk, calculated over the last minute. |

**TABLE D-25. ssSwapOut**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.4   |
| <b>Object name</b> | ssSwapOut  |
| <b>Description</b> | The average amount of memory swapped out to disk, calculated over the last minute. |

**TABLE D-26. sslOSent**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.5  |
| <b>Object name</b> | sslOSent  |
| <b>Description</b> | The average amount of data written to disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'sslORawSent(57)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-27. sslOReceive**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.6   |
| <b>Object name</b> | sslOReceive  |
| <b>Description</b> | The average amount of data read from disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'sslORawReceived(58)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-28. ssSysInterrupts**

| ITEM               | DESCRIPTION            |
|--------------------|------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.7 |
| <b>Object name</b> | ssSysInterrupts        |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | The average rate of interrupts processed (including the clock) calculated over the last minute. This object has been deprecated in favour of 'ssRawInterrupts(59)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-29. ssSysContext**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.8  |
| <b>Object name</b> | ssSysContext  |
| <b>Description</b> | The average rate of context switches, calculated over the last minute. This object has been deprecated in favour of 'ssRawContext(60)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-30. ssCpuUser**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.9   |
| <b>Object name</b> | ssCpuUser  |
| <b>Description</b> | The percentage of CPU time spent processing user-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawUser(50)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-31. ssCpuSystem**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.10  |
| <b>Object name</b> | ssCpuSystem  |
| <b>Description</b> | The percentage of CPU time spent processing system-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawSystem(52)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-32. ssCpuIdle**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.11  |
| <b>Object name</b> | ssCpuIdle  |
| <b>Description</b> | The percentage of processor time spent idle, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawIdle(53)', which can be used to calculate the same metric, but over any desired time period. |

**TABLE D-33. ssCpuRawUser**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.50   |
| <b>Object name</b> | ssCpuRawUser  |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing user-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). |

**TABLE D-34. ssCpuRawNice**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.51   |
| <b>Object name</b> | ssCpuRawNice  |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing reduced-priority code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). |

**TABLE D-35. ssCpuRawSystem**

| ITEM       | DESCRIPTION             |
|------------|-------------------------|
| <b>OID</b> | .1.3.6.1.4.1.2021.11.52 |

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>Object name</b> | ssCpuRawSystem   |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing system-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be $N \times 100$ (for $N$ processors). This object may sometimes be implemented as the combination of the 'ssCpuRawWait(54)' and 'ssCpuRawKernel(55)' counters, so care must be taken when summing the overall raw counters. |

**TABLE D-36. ssCpuRawIdle**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.53  |
| <b>Object name</b> | ssCpuRawIdle   |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent idle. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be $N \times 100$ (for $N$ processors). |

**TABLE D-37. ssCpuRawWait**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.54  |
| <b>Object name</b> | ssCpuRawWait   |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent waiting for IO. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be $N \times 100$ (for $N$ processors). |

**TABLE D-38. ssCpuRawKernel**

| ITEM       | DESCRIPTION             |
|------------|-------------------------|
| <b>OID</b> | .1.3.6.1.4.1.2021.11.55 |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Object name</b> | ssCpuRawKernel  |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing kernel-level code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). |

**TABLE D-39. ssCpuRawInterrupt**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.56   |
| <b>Object name</b> | ssCpuRawInterrupt   |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing hardware interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). |

**TABLE D-40. sslORawSent**

| ITEM               | DESCRIPTION                              |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.57                  |
| <b>Object name</b> | sslORawSent                              |
| <b>Description</b> | Number of blocks sent to a block device. |

**TABLE D-41. sslORawReceived**

| ITEM               | DESCRIPTION                                    |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.58                        |
| <b>Object name</b> | sslORawReceived                                |
| <b>Description</b> | Number of blocks received from a block device. |

**TABLE D-42. ssRawInterrupts**

| ITEM               | DESCRIPTION                     |
|--------------------|---------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.59         |
| <b>Object name</b> | ssRawInterrupts                 |
| <b>Description</b> | Number of interrupts processed. |

**TABLE D-43. ssRawContexts**

| ITEM               | DESCRIPTION                 |
|--------------------|-----------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.60     |
| <b>Object name</b> | ssRawContexts               |
| <b>Description</b> | Number of context switches. |

**TABLE D-44. ssCpuRawSoftIRQ**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.61   |
| <b>Object name</b> | ssCpuRawSoftIRQ   |
| <b>Description</b> | The number of 'ticks' (typically 1/100s) spent processing software interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). |

**TABLE D-45. ssRawSwapIn**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.62      |
| <b>Object name</b> | ssRawSwapIn                  |
| <b>Description</b> | Number of blocks swapped in. |

**TABLE D-46. ssRawSwapOut**

| ITEM               | DESCRIPTION                   |
|--------------------|-------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.2021.11.63       |
| <b>Object name</b> | ssRawSwapOut                  |
| <b>Description</b> | Number of blocks swapped out. |

**TABLE D-47. productVersion**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.1.1                          |
| <b>Object name</b> | productVersion                                      |
| <b>Description</b> | Returns the Deep Discovery Email Inspector version. |

**TABLE D-48. productBuild**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.1.2                               |
| <b>Object name</b> | productBuild   |
| <b>Description</b> | Returns the Deep Discovery Email Inspector build number. |

**TABLE D-49. productHotfix**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.1.3                                |
| <b>Object name</b> | productHotfix   |
| <b>Description</b> | Returns the Deep Discovery Email Inspector hotfix number. |

**TABLE D-50. patternIndex**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.2.1.1 |
| <b>Object name</b> | patternIndex                 |

| ITEM               | DESCRIPTION                |
|--------------------|----------------------------|
| <b>Description</b> | Returns the pattern index. |

**TABLE D-51. patternID**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.2.1.2 |
| <b>Object name</b> | patternID                    |
| <b>Description</b> | Returns the pattern ID.      |

**TABLE D-52. patternName**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.2.1.3 |
| <b>Object name</b> | patternName                  |
| <b>Description</b> | Returns the pattern name.    |

**TABLE D-53. patternVersion**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.2.1.4 |
| <b>Object name</b> | patternVersion               |
| <b>Description</b> | Returns the pattern version. |

**TABLE D-54. deliveryQueue**

| ITEM               | DESCRIPTION                        |
|--------------------|------------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.3.1         |
| <b>Object name</b> | deliveryQueue                      |
| <b>Description</b> | Returns the delivery queue number. |

**TABLE D-55. virtualAnalyzerQueue**

| ITEM               | DESCRIPTION                                |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.3.2                 |
| <b>Object name</b> | virtualAnalyzerQueue                       |
| <b>Description</b> | Returns the Virtual Analyzer queue number. |

**TABLE D-56. deferredQueue**

| ITEM               | DESCRIPTION                        |
|--------------------|------------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.3.3         |
| <b>Object name</b> | deferredQueue                      |
| <b>Description</b> | Returns the deferred queue number. |

**TABLE D-57. ifIndex**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.4.1.1 |
| <b>Object name</b> | ifIndex                      |
| <b>Description</b> | Returns the interface index. |

**TABLE D-58. ifDescr**

| ITEM               | DESCRIPTION                        |
|--------------------|------------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.4.1.2       |
| <b>Object name</b> | ifDescr                            |
| <b>Description</b> | Returns the interface description. |

**TABLE D-59. ifReceiveThroughput**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.4.1.3 |
| <b>Object name</b> | ifReceiveThroughput          |

| ITEM               | DESCRIPTION                                 |
|--------------------|---|
| <b>Description</b> | Returns the interface receiving throughput. |

**TABLE D-60. ifTransmitThroughput**

| ITEM               | DESCRIPTION                                    |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.4.1.4                   |
| <b>Object name</b> | ifTransmitThroughput                           |
| <b>Description</b> | Returns the interface transmitting throughput. |

## SNMP Traps

**TABLE D-61. coldStart**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.6.3.1.1.5.1.0  |
| <b>Object name</b> | coldStart   |
| <b>Description</b> | A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered. |

**TABLE D-62. linkDown**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.6.3.1.1.5.3.0   |
| <b>Object name</b> | linkDown   |
| <b>Description</b> | A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. |

**TABLE D-63. linkUp**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.6.3.1.1.5.4.0   |
| <b>Object name</b> | linkUp   |
| <b>Description</b> | A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. |

**TABLE D-64. nsNotifyShutdown**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.8072.4.0.2  |
| <b>Object name</b> | nsNotifyShutdown   |
| <b>Description</b> | An indication that the agent is in the process of being shut down. |

**TABLE D-65. vaStoppedNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.1                                     |
| <b>Object name</b> | vaStoppedNotification  |
| <b>Description</b> | Notification to indicate that Virtual Analyzer is not available. |

**TABLE D-66. serviceStoppedNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.2   |
| <b>Object name</b> | serviceStoppedNotification   |
| <b>Description</b> | Notification to indicate that a service has stopped and cannot be restarted. |

**TABLE D-67. unreachableMTANotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.3   |
| <b>Object name</b> | unreachableMTANotification   |
| <b>Description</b> | Notification to indicate that relay MTAs for a domain cannot be reached. |

**TABLE D-68. suspiciousMsgNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.4  |
| <b>Object name</b> | suspiciousMsgNotification   |
| <b>Description</b> | Notification to indicate that one or more email messages are detected with threats. |

**TABLE D-69. watchlistNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.5   |
| <b>Object name</b> | watchlistNotification  |
| <b>Description</b> | Notification to indicate that one or more email messages detected with threats are sent to watchlist recipients. |

**TABLE D-70. deliveryQueueNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.6  |
| <b>Object name</b> | deliveryQueueNotification   |
| <b>Description</b> | Notification to indicate that the number of email messages on the delivery queue has reached the maximum threshold. |

**TABLE D-71. cpuUsageNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.7   |
| <b>Object name</b> | cpuUsageNotification   |
| <b>Description</b> | Notification to indicate that the CPU usage level has reached the maximum threshold. |

**TABLE D-72. vaQueueNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.8  |
| <b>Object name</b> | vaQueueNotification   |
| <b>Description</b> | Notification to indicate that the number of email messages on the Virtual Analyzer queue has reached the maximum threshold. |

**TABLE D-73. vaProcessTimeNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.9  |
| <b>Object name</b> | vaProcessTimeNotification   |
| <b>Description</b> | Notification to indicate that the average Virtual Analyzer processing time is greater than the maximum threshold. |

**TABLE D-74. diskSpaceNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.10  |
| <b>Object name</b> | diskSpaceNotification  |
| <b>Description</b> | Notification to indicate that the available disk space is less than the minimum threshold. |

**TABLE D-75. updateFailedNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.11                                      |
| <b>Object name</b> | updateFailedNotification   |
| <b>Description</b> | Notification to indicate that a component update was unsuccessful. |

**TABLE D-76. updateSuccessNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.12                                    |
| <b>Object name</b> | updateSuccessNotification  |
| <b>Description</b> | Notification to indicate that a component update was successful. |

**TABLE D-77. ntpFailedNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.13  |
| <b>Object name</b> | ntpFailedNotification  |
| <b>Description</b> | Notification to indicate that time synchronization with an NTP server is not successful. |

**TABLE D-78. vaProcessTimeoutNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.14  |
| <b>Object name</b> | vaProcessTimeoutNotification   |
| <b>Description</b> | Notification to indicate that an analysis process has timed out with no analysis result. |

**TABLE D-79. quarantineDiskSpaceNotification**

| ITEM       | DESCRIPTION                   |
|------------|-------------------------------|
| <b>OID</b> | .1.3.6.1.4.1.6101.3004.5.0.15 |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Object name</b> | quarantineDiskSpaceNotification   |
| <b>Description</b> | Notification to indicate that the available disk space for quarantined files has reached the minimum threshold. |

**TABLE D-80. msgQuarantinedNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.16   |
| <b>Object name</b> | msgQuarantinedNotification  |
| <b>Description</b> | Notification to indicate that one or more email messages are quarantined. |

**TABLE D-81. memUsageNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.17   |
| <b>Object name</b> | memUsageNotification  |
| <b>Description</b> | Notification to indicate that the memory usage level has reached the maximum threshold. |

**TABLE D-82. deferredQueueNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.18   |
| <b>Object name</b> | deferredQueueNotification   |
| <b>Description</b> | Notification to indicate that the number of email messages on the deferred queue has reached the maximum threshold. |

**TABLE D-83. spamQuarantineSpaceNotification**

| ITEM       | DESCRIPTION                   |
|------------|-------------------------------|
| <b>OID</b> | .1.3.6.1.4.1.6101.3004.5.0.19 |

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>Object name</b> | spamQuarantineSpaceNotification  |
| <b>Description</b> | Notification to indicate that the available disk space for spam quarantined files has reached the minimum threshold. |

**TABLE D-84. accountLockedNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.20                             |
| <b>Object name</b> | accountLockedNotification                                 |
| <b>Description</b> | Notification to indicate that an account has been locked. |

**TABLE D-85. failedDKIMSignNotification**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.21  |
| <b>Object name</b> | failedDKIMSignNotification   |
| <b>Description</b> | Notification to indicate that the number of messages with unsuccessful DKIM signing has reached the maximum threshold. |

**TABLE D-86. connectionIssueNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.22   |
| <b>Object name</b> | connectionIssueNotification   |
| <b>Description</b> | Notification to indicate that the appliance is unable to establish connection to a required resource. |

**TABLE D-87. dataLossPreventionNotification**

| ITEM               | DESCRIPTION                    |
|--------------------|--------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.23  |
| <b>Object name</b> | dataLossPreventionNotification |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | Notification to indicate that the number of messages with selected templates has reached the minimum threshold. |

**TABLE D-88. encryptionExceptionNotification**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.0.24   |
| <b>Object name</b> | encryptionExceptionNotification   |
| <b>Description</b> | Notification to indicate that the number of messages that Deep Discovery Email Inspector cannot encrypt or decrypt has reached the maximum threshold. |

**TABLE D-89. vaStoppedMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.1                                |
| <b>Object name</b> | vaStoppedMsg  |
| <b>Description</b> | Message to indicate that Virtual Analyzer is not available. |

**TABLE D-90. serviceStoppedMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.2  |
| <b>Object name</b> | serviceStoppedMsg   |
| <b>Description</b> | Message to indicate that a service has stopped and cannot be restarted. |

**TABLE D-91. unreachableMTAMsg**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.3 |
| <b>Object name</b> | unreachableMTAMsg            |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | Message to indicate that relay MTAs for a domain cannot be reached. |

**TABLE D-92. suspiciousMsgMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.4   |
| <b>Object name</b> | suspiciousMsgMsg   |
| <b>Description</b> | Message to indicate that one or more email messages are detected with threats. |

**TABLE D-93. watchlistMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.5  |
| <b>Object name</b> | watchlistMsg  |
| <b>Description</b> | Message to indicate that one or more email messages detected with threats are sent to watchlist recipients. |

**TABLE D-94. deliveryQueueMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.6   |
| <b>Object name</b> | deliveryQueueMsg   |
| <b>Description</b> | Message to indicate that the number of email messages on the delivery queue has reached the maximum threshold. |

**TABLE D-95. cpuUsageMsg**

| ITEM               | DESCRIPTION                  |
|--------------------|------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.7 |
| <b>Object name</b> | cpuUsageMsg                  |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | Message to indicate that the CPU usage level has reached the maximum threshold. |

**TABLE D-96. vaQueueMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.8   |
| <b>Object name</b> | vaQueueMsg   |
| <b>Description</b> | Message to indicate that the number of email messages on the Virtual Analyzer queue has reached the maximum threshold. |

**TABLE D-97. vaProcessTimeMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.9   |
| <b>Object name</b> | vaProcessTimeMsg   |
| <b>Description</b> | Message to indicate that the average Virtual Analyzer processing time is greater than the maximum threshold. |

**TABLE D-98. diskSpaceMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.10   |
| <b>Object name</b> | diskSpaceMsg  |
| <b>Description</b> | Message to indicate that the available disk space is less than the minimum threshold. |

**TABLE D-99. updateFailedMsg**

| ITEM               | DESCRIPTION                   |
|--------------------|-------------------------------|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.11 |
| <b>Object name</b> | updateFailedMsg               |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>Description</b> | Message to indicate that a component update was unsuccessful. |

**TABLE D-100. updateSuccessMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.12                               |
| <b>Object name</b> | updateSuccessMsg  |
| <b>Description</b> | Message to indicate that a component update was successful. |

**TABLE D-101. ntpFailedMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.13   |
| <b>Object name</b> | ntpFailedMsg  |
| <b>Description</b> | Message to indicate that time synchronization with an NTP server is not successful. |

**TABLE D-102. vaProcessTimeoutMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.14   |
| <b>Object name</b> | vaProcessTimeoutMsg   |
| <b>Description</b> | Message to indicate that an analysis process has timed out with no analysis result. |

**TABLE D-103. quarantineDiskSpaceMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.15  |
| <b>Object name</b> | quarantineDiskSpaceMsg   |
| <b>Description</b> | Message to indicate that the available disk space for quarantined files has reached the minimum threshold. |

**TABLE D-104. msgQuarantinedMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.16  |
| <b>Object name</b> | msgQuarantinedMsg  |
| <b>Description</b> | Message to indicate that one or more email messages are quarantined. |

**TABLE D-105. memUsageMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.17  |
| <b>Object name</b> | memUsageMsg  |
| <b>Description</b> | Message to indicate that the memory usage level has reached the maximum threshold. |

**TABLE D-106. deferredQueueMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.18  |
| <b>Object name</b> | deferredQueueMsg   |
| <b>Description</b> | Message to indicate that the number of email messages on the deferred queue has reached the maximum threshold. |

**TABLE D-107. spamQuarantineSpaceMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.19   |
| <b>Object name</b> | spamQuarantineSpaceMsg  |
| <b>Description</b> | Message to indicate that the available disk space for spam quarantined files has reached the minimum threshold. |

**TABLE D-108. accountLockedMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.20                        |
| <b>Object name</b> | accountLockedMsg                                     |
| <b>Description</b> | Message to indicate that an account has been locked. |

**TABLE D-109. failedDKIMSignMsg**

| ITEM               | DESCRIPTION   |
|--------------------|---|
| <b>OID</b>         | 1.3.6.1.4.1.6101.3004.5.1.21  |
| <b>Object name</b> | failedDKIMSignMsg   |
| <b>Description</b> | Message to indicate that the number of messages with unsuccessful DKIM signing has reached the maximum threshold. |

**TABLE D-110. connectionIssueMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.22  |
| <b>Object name</b> | connectionIssueMsg   |
| <b>Description</b> | Message to indicate that the appliance is unable to establish connection to a required resource. |

**TABLE D-111. dataLossPreventionMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.23  |
| <b>Object name</b> | dataLossPreventionMsg  |
| <b>Description</b> | Message to indicate that the number of messages with detected DLP incidents has reached the specified threshold. |

**TABLE D-112. encryptionExceptionMsg**

| ITEM               | DESCRIPTION  |
|--------------------|--|
| <b>OID</b>         | .1.3.6.1.4.1.6101.3004.5.1.24  |
| <b>Object name</b> | encryptionExceptionMsg   |
| <b>Description</b> | Message to indicate that the number of messages that Deep Discovery Email Inspector cannot encrypt or decrypt has reached the maximum threshold. |

## Registration Objects

| OID                    | DESCRIPTION                 |
|------------------------|-----------------------------|
| .1.3.6.1.4.1.2021      | UC Davis                    |
| .1.3.6.1.4.1.6101      | Trend Micro, Inc.           |
| .1.3.6.1.6.3.1.1.5.1   | SNMPv2-MIB MIB              |
| .1.3.6.1.4.1.8072      | NET-SNMP-AGENT-MIB          |
| .1.3.6.1.4.1.6101.999  | TMCN                        |
| .1.3.6.1.4.1.6101.3001 | TMTM                        |
| .1.3.6.1.4.1.6101.3004 | DeepDiscoveryEmailInspector |

# Appendix E

## IPv6 Support in Deep Discovery Email Inspector

This appendix is required reading for users who plan to deploy Deep Discovery Email Inspector in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in Deep Discovery Email Inspector.

Deep Discovery Email Inspector assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

IPv6 support for Deep Discovery Email Inspector started in version 2.1. Earlier Deep Discovery Email Inspector versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading Deep Discovery Email Inspector.

The following Deep Discovery Email Inspector features support IPv6:

- Email message processing (receiving and delivering)
- Management console and CLI access
- Notification SMTP
- SPAN/TAP mode
- Syslog server

- Sender filtering settings (Approved Senders, Email Reputation, DHA Protection, Bounce Attack Protection, SMTP Traffic Throttling)
- Sender authentication settings (SPF only)
- Edge relay MTA servers

## Configuring IPv6 Addresses

The CLI and management console allow you to configure an IPv6 address. The following are some configuration guidelines.

- Deep Discovery Email Inspector accepts standard IPv6 address presentations.

For example:

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```



### Note

Deep Discovery Email Inspector does not accept link-local IPv6 addresses.

---

- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).

## Configurable IPv6 Addresses

IPv6 addresses are configurable on the management console and CLI.

### Management Console IPv6 Addresses

IPv6 addresses are configurable on the following management console screens:

- **Administration > System Settings > Network**
- **Administration > System Settings > SMTP**
- **Administration > Mail Settings > Connections**
- **Administration > Mail Settings > Message Delivery**

- **Administration > Mail Settings > Limits and Exceptions**
- **Administration > Integrated Products/Services > Syslog**
- **Administration > System Settings > Operation Mode** (SPAN/TAP mode rules)
- **Administration > Sender Filtering/Authentication > Approved Senders**
- **Administration > Mail Settings > Edge MTA Relay Servers**

## CLI IPv6 Addresses

IPv6 addresses are configurable using the following CLI commands:

- *[configure product management-port on page A-4](#)*
- *[configure network basic on page A-5](#)*
- *[configure network dns on page A-6](#)*
- *[configure network interface on page A-8](#)*
- *[configure network route add on page A-9](#)*
- *[configure network route default on page A-9](#)*
- *[configure network route del on page A-10](#)*

# Appendix F

## System Event Logs

The following table lists the system event logs in Deep Discovery Email Inspector.

**TABLE F-1. System event logs**

| ID    | LOG TYPE      | MESSAGE   |
|-------|---------------|---|
| 11001 | Update events | Product Updates: {USER} installed hot fix {VERSION} from {IP}     |
| 11002 | Update events | Product Updates: {USER} rolled back hot fix {VERSION} from {IP}   |
| 11003 | Update events | Product Updates: Appliance firmware upgraded by {USER} from {IP}  |
| 12001 | Update events | Deep Discovery Director: Hotfix update successful                 |
| 12002 | Update events | Deep Discovery Director: Firmware update successful               |
| 12003 | Update events | Deep Discovery Director: Virtual Analyzer image import successful |
| 12004 | Update events | Deep Discovery Director: Configuration update successful          |

| ID    | LOG TYPE      | MESSAGE   |
|-------|---------------|---|
| 12005 | Update events | Deep Discovery Director: Unregistered by Deep Discovery Director administrator        |
| 12101 | Update events | Deep Discovery Director: Suspicious object synchronization with Apex Central disabled |
| 12201 | Update events | Deep Discovery Director: End-User Quarantine configuration disabled                   |
| 130xx | Update events | ActiveUpdate: {COMPONENT} downloaded manually by {USER} from {IP}                     |
| 131xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully downloaded manually by {USER} from {IP}      |
| 132xx | Update events | ActiveUpdate: {COMPONENT} downloaded by scheduled update                              |
| 133xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully downloaded by scheduled update               |
| 134xx | Update events | ActiveUpdate: {COMPONENT} rolled back to version {VERSION} by {USER} from {IP}        |
| 135xx | Update events | ActiveUpdate: {COMPONENT} unsuccessfully rolled back by {USER} from {IP}              |
| 136xx | Update events | ActiveUpdate Exception - Apply {COMPONENT} {VERSION} to local scanner failed          |
| 20101 | Audit log     | System started  |
| 20102 | Audit log     | System stopped  |
| 20201 | Audit log     | Service started   |
| 20202 | Audit log     | Service stopped   |
| 20301 | Audit log     | License: {NAME} license expired, grace period ends on {DATE}                          |
| 20302 | Audit log     | License: {NAME} license expired   |
| 20303 | Audit log     | License: {NAME} license updated   |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 20401 | Audit log | System Maintenance: Device powered off by {USER} from {IP}  |
| 20402 | Audit log | System Maintenance: Device restarted by {USER} from {IP}  |
| 20501 | Audit log | Logon: 'admin' logged on from {HOST} via SSH  |
| 20502 | Audit log | Logon: Attempted logon with user name ('admin') from {HOST} via SSH   |
| 20503 | Audit log | Logon: 'root' logged on from {HOST} with token {NAME} via SSH   |
| 20504 | Audit log | Logon: Attempted logon with user name ('root') from {HOST} via SSH  |
| 20505 | Audit log | Logon: 'admin' logged off from {HOST} via SSH   |
| 20506 | Audit log | Logon: 'root' logged off from {HOST} with token {NAME} via SSH  |
| 20507 | Audit log | Logon: Attempted logon with user name {USER} from {HOST} via SSH  |
| 30101 | Audit log | Active update source setting was changed  |
| 30102 | Audit log | Active update schedule setting was changed  |
| 30201 | Audit log | System Settings: Host name saved as {NAME} by {USER} from {IP}  |
| 30202 | Audit log | System Settings: {INTERFACE} IPv4 address and subnet mask were saved as {SUBNET} by {USER} from {IP}        |
| 30203 | Audit log | System Settings: {INTERFACE} IPv6 address and prefix length were saved as {IP}/{LENGTH} by {USER} from {IP} |
| 30204 | Audit log | System Settings: {INTERFACE} IPv4 gateway saved as {GATEWAY} by {USER} from {IP}                            |
| 30205 | Audit log | System Settings: {INTERFACE} IPv6 gateway saved as {GATEWAY} by {USER} from {IP}                            |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 30206 | Audit log | System Settings: {INTERFACE} primary IPv4 DNS server saved as {IP} and secondary IPv4 DNS server saved as {IP} by {USER} from {IP} |
| 30207 | Audit log | System Settings: {INTERFACE} primary IPv6 DNS server saved as {IP} and secondary IPv6 DNS server saved as {IP} by {USER} from {IP} |
| 30208 | Audit log | System Settings: {INTERFACE} IPv4 address and subnet mask deleted by {USER} from {IP}  |
| 30209 | Audit log | System Settings: NIC teaming settings changed by {USER} from {IP}  |
| 30301 | Audit log | System Settings: Operation mode saved as {MODE} by {USER} from {IP}  |
| 30401 | Audit log | System Settings: Proxy settings modified by {USER} from {IP}   |
| 30402 | Audit log | System Settings: Proxy settings unsuccessfully modified by {USER} from {IP}  |
| 30501 | Audit log | System Settings: SMTP server settings modified by {USER} from {IP}   |
| 30601 | Audit log | System Settings: System time zone saved as {ZONE} by {USER} from {IP}  |
| 30602 | Audit log | System Settings: NTP server synchronization enabled by {USER} from {IP}  |
| 30603 | Audit log | System Settings: NTP server synchronization disabled by {USER} from {IP}   |
| 30604 | Audit log | System Settings: System time saved as {TIME} by {USER} from {IP}   |
| 30605 | Audit log | System Settings: Database time zone saved as {ZONE} by {USER} from {IP}  |
| 30606 | Audit log | System Settings: NTP server saved as {NAME} by {USER} from {IP}  |
| 30701 | Audit log | System Settings: SNMP settings modified by {USER} from {IP}  |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 30702 | Audit log | System Settings: SNMP MIB files downloaded by {USER} from {IP}                   |
| 30703 | Audit log | System settings: Session timeout setting modified by {USER} from {IP}            |
| 30704 | Audit log | System Settings: SSL settings modified by {USER} from {IP}                       |
| 30705 | Audit log | System Settings: {USER} added certificate signing request {NAME} from {IP}       |
| 30706 | Audit log | System Settings: {USER} added self-signed certificate {NAME} from {IP}           |
| 30707 | Audit log | System Settings: {USER} deleted certificate {NAME} from {IP}                     |
| 30708 | Audit log | System Settings: {USER} imported certificate {NAME} from {IP}                    |
| 30709 | Audit log | System Settings: {USER} changed certificate name from {NAME} to {NAME} from {IP} |
| 30710 | Audit log | System Settings: {USER} assigned certificate {NAME} to {SERVICE} from {IP}       |
| 30711 | Audit log | System Settings: {USER} deleted trusted CA certificate {NAME} from {IP}          |
| 30712 | Audit log | System Settings: {USER} imported trusted CA certificate {NAME} from {IP}         |
| 30801 | Audit log | Mail Settings: SMTP Connection setting saved by {USER} from {IP}                 |
| 30802 | Audit log | Mail Settings: TLS certificate uploaded by {USER} from {IP}                      |
| 30803 | Audit log | Mail Settings: TLS certificate downloaded by {USER} from {IP}                    |
| 30901 | Audit log | Mail Settings: Delivery profiles exported by {USER} from {IP}                    |
| 30902 | Audit log | Mail Settings: Delivery profiles unsuccessfully exported by {USER} from {IP}     |
| 30903 | Audit log | Mail Settings: Delivery profiles imported by {USER} from {IP}                    |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 30904 | Audit log | Mail Settings: Mail Settings: Delivery profiles unsuccessfully imported due to maximum entries (256) exceeded |
| 30905 | Audit log | Mail Settings: Delivery profiles unsuccessfully imported by {USER} from {IP}                                  |
| 30906 | Audit log | Mail Settings: Delivery profile added by {USER} from {IP}   |
| 30907 | Audit log | Mail Settings: Delivery profile modified by {USER} from {IP}  |
| 30908 | Audit log | Mail Settings: Delivery profile deleted by {USER} from {IP}   |
| 31001 | Audit log | Mail Settings: Mail settings modified by {USER} from {IP}   |
| 31101 | Audit log | Mail Settings: SMTP server greeting saved by {USER} from {IP}   |
| 31102 | Audit log | Mail Settings: Internal domain settings modified by {USER} from {IP}  |
| 31103 | Audit log | Mail Settings: Internal domains imported by {USER} from {IP}  |
| 31103 | Audit log | Mail Settings: Internal domain {NAME} added through a policy by {USER} from {IP}                              |
| 31104 | Audit log | Mail Settings: Address Rewriting settings modified by by {USER} from {IP}                                     |
| 31105 | Audit log | Mail Settings: Domain Rewriting settings modified by {USER} from {IP}   |
| 31106 | Audit log | Mail Settings: {USER} added IP address or domain {NAME} from {IP} for incoming messages                       |
| 31107 | Audit log | Mail Settings: {USER} updated IP address or domain {NAME} from {IP} for incoming messages                     |
| 31108 | Audit log | Mail Settings: {USER} deleted one or more IP addresses or domains from {IP} for incoming messages             |
| 31109 | Audit log | Mail Settings: {USER} imported one or more IP addresses or domains from {IP} for incoming messages            |
| 31110 | Audit log | Mail Settings: {USER} enabled IP address or domain {NAME} from {IP} for incoming messages                     |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 31111 | Audit log | Mail Settings: {USER} disabled IP address or domain {NAME} from {IP} for incoming messages                                     |
| 31112 | Audit log | Mail Settings: {USER} added domain {NAME} from {IP} for outgoing messages  |
| 31113 | Audit log | Mail Settings: {USER} updated domain {NAME} from {IP} for outgoing messages  |
| 31114 | Audit log | Mail Settings: {USER} deleted one or more domains from {IP} for outgoing messages  |
| 31115 | Audit log | Mail Settings: {USER} imported one or more domains from {IP} for outgoing messages   |
| 31116 | Audit log | Mail Settings: {USER} enabled domain {NAME} from {IP} for outgoing messages  |
| 31117 | Audit log | Mail Settings: {USER} disabled domain {NAME} from {IP} for outgoing messages   |
| 31201 | Audit log | Log Settings: {NAME} syslog server profile created by {USER} from {IP}   |
| 31202 | Audit log | Log Settings: {NAME} syslog server profile deleted by {USER} from {IP}   |
| 31203 | Audit log | Log Settings: {NAME} syslog server profile modified by {USER} from {IP}  |
| 31204 | Audit log | Log Settings: {NAME} enabled by {USER} from {IP}   |
| 31205 | Audit log | Log Settings: {NAME} disabled by {USER} from {IP}  |
| 31206 | Audit log | Integrated Products/Services: {USER} synchronized data for all LDAP servers from {IP}  |
| 31207 | Audit log | Integrated Products/Services: {USER} enabled LDAP server {NAME} from {IP}<br>Log Settings: {NAME} disabled by {USER} from {IP} |
| 31208 | Audit log | Integrated Products/Services: {USER} disabled LDAP server {NAME} from {IP}   |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 31301 | Audit log | Integrated Products/Services: SFTP Upload settings modified by {USER} from {IP}                     |
| 31402 | Audit log | Integrated Products/Services: {USER} added LDAP server {NAME} from {IP}                             |
| 31403 | Audit log | Integrated Products/Services: {USER} modified LDAP server {NAME} from {IP}                          |
| 31404 | Audit log | Integrated Products/Services: {USER} deleted LDAP server {NAME} from {IP}                           |
| 31405 | Audit log | Integrated Products/Services: {USER} synchronized data for LDAP server {NAME} from {IP}             |
| 31406 | Audit log | Integrated Products/Services: {USER} synchronized data for all LDAP servers from {IP}               |
| 31407 | Audit log | Integrated Products/Services: {USER} enabled LDAP server {NAME} from {IP}                           |
| 31408 | Audit log | Integrated Products/Services: {USER} disabled LDAP server {NAME} from {IP}                          |
| 31501 | Audit log | Integrated Products/Services: Threat Intelligent Sharing settings modified by {USER} from {IP}      |
| 31502 | Audit log | Integrated Products/Services: {USER} generate suspicious objects list from {IP}                     |
| 31601 | Audit log | Integrated Products/Services: Auxiliary Products/Services settings modified by {USER} from {IP}     |
| 31602 | Audit log | Integrated Products/Services: {USER} clicked Auxiliary Products/Services > Distribute Now from {IP} |
| 31701 | Audit log | Systems Settings: Apex Central settings modified by {USER} from {IP}                                |
| 31702 | Audit log | System Settings: Suspicious object synchronization enabled by {USER} from {IP}                      |
| 31703 | Audit log | System Settings: Suspicious object synchronization disabled by {USER} from {IP}                     |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 31801 | Audit log | System Settings: Proxy settings for Deep Discovery Director modified by {USER} by {IP}                |
| 31802 | Audit log | System Settings: Registered to Deep Discovery Director by {USER} from {IP}                            |
| 31803 | Audit log | System Settings: Unregistered from Deep Discovery Director by {USER} from {IP}                        |
| 31804 | Audit log | System Settings: Deep Discovery Director fingerprint trusted by {USER} from {IP}                      |
| 31901 | Audit log | Scanning / Analysis: Image imported by {USER} from {IP}   |
| 31902 | Audit log | Scanning / Analysis: Image deleted by {USER} from {IP}  |
| 31903 | Audit log | Scanning / Analysis: Number of instances for each Virtual Analyzer image modified by {USER} from {IP} |
| 32001 | Audit log | Scanning / Analysis: Virtual Analyzer settings modified by {USER} from {IP}                           |
| 32101 | Audit log | Scanning / Analysis: {PRODUCT NAME} registered to the external Virtual Analyzer                       |
| 32102 | Audit log | Scanning / Analysis: Unable to register to the external Virtual Analyzer                              |
| 32103 | Audit log | Scanning / Analysis: {PRODUCT NAME} unregistered from the external Virtual Analyzer                   |
| 32104 | Audit log | Scanning / Analysis: Virtual Analyzer external integration settings modified by {USER} from "%s"      |
| 32201 | Audit log | Scanning / Analysis: File Passwords setting was modified by {USER} from {IP}                          |
| 32301 | Audit log | Scanning / Analysis: Smart Protection settings modified by {USER} from {IP}                           |
| 32401 | Audit log | Scanning / Analysis: Smart Feedback settings modified by {USER} from {IP}                             |
| 32501 | Audit log | Scanning / Analysis: {USER} added YARA rule {NAME} from {IP}  |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 32502 | Audit log | Scanning / Analysis: {USER} modified YARA rule {NAME} from {IP}               |
| 32503 | Audit log | Scanning / Analysis: {USER} deleted YARA rule {NAME} from {IP}                |
| 32504 | Audit log | Scanning / Analysis: {USER} modified status for YARA rule {NAME} from {IP}    |
| 32510 | Audit log | Scanning / Analysis: Time-of-Click settings modified by {USER} from {IP}      |
| 32520 | Audit log | Scanning / Analysis: High-Profile Users settings modified by {USER} from {IP} |
| 32521 | Audit log | Scanning / Analysis: Internal Domains settings modified by {USER} from {IP}   |
| 32522 | Audit log | Scanning / Analysis: Approved Senders settings modified by {USER} from {IP}   |
| 32523 | Audit log | Scanning / Analysis: Cousin Domains settings modified by {USER} from {IP}     |
| 32530 | Audit log | Scanning / Analysis: URL Scanning setting modified by {USER} from {IP}        |
| 32601 | Audit log | System Maintenance: Configuration imported by {USER} from {IP}                |
| 32602 | Audit log | System Maintenance: Configuration unsuccessfully imported by {USER} from {IP} |
| 32603 | Audit log | System Maintenance: Configuration exported by {USER} from {IP}                |
| 32604 | Audit log | System Maintenance: Configuration unsuccessfully exported by {USER} from {IP} |
| 32701 | Audit log | System Maintenance: Data purge started automatically                          |
| 32702 | Audit log | System Maintenance: Data purge completed ({MIN} min {SEC} s)                  |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 32703 | Audit log | System Maintenance: Storage maintenance setting modified by {USER} from {IP}         |
| 32801 | Audit log | System Maintenance: System log level setting modified by {USER} from {IP}            |
| 32901 | Audit log | Accounts / Contacts: {USER} created the account {NAME} from {IP}                     |
| 32902 | Audit log | Accounts / Contacts: {USER} deleted the account {NAME} from {IP}                     |
| 32903 | Audit log | Accounts / Contacts: {USER} modified the account {NAME} from {IP}                    |
| 32904 | Audit log | Accounts / Contacts: {USER} unlocked the account {NAME} from {IP}                    |
| 33001 | Audit log | Logon: {USER} logged on as {ROLE} role from {IP}                                     |
| 33002 | Audit log | Logon: {USER} logged off from {IP}   |
| 33003 | Audit log | Logon: Attempted logon with an invalid user name ({USER}) or password from {IP}      |
| 33004 | Audit log | Logon: Attempted logon with a disabled user name ({USER}) from {IP}                  |
| 33005 | Audit log | Logon: Attempted logon with a locked user name {NAME} from {IP}                      |
| 33006 | Audit log | Logon: Unlocked user name {NAME} from {IP}   |
| 33007 | Audit log | RDQA Logon: "{USER}" logged on as {NAME} role from {IP}                              |
| 33008 | Audit log | RDQA Logon: "{USER}" logged off  |
| 33009 | Audit log | RDQA Logon: Attempted logon with an invalid user name "{USER}" or password from {IP} |
| 33010 | Audit log | RDQA Logon: Attempted logon with a disabled user name "{USER}" from {IP}             |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 33011 | Audit log | RDQA Logon: Attempted logon with a locked user name "{USER}" from {IP}                             |
| 33012 | Audit log | RDQA Logon: Unlocked user name "{USER}" from {IP}  |
| 33101 | Audit log | Accounts / Contacts: Contacts for alert notifications and reports modified by {USER} from {IP}     |
| 33201 | Audit log | Accounts / Contacts: {USER} modified the password for {NAME} from {IP}                             |
| 33202 | Audit log | Accounts / Contacts: {USER} added SAML group {NAME} from {IP}                                      |
| 33203 | Audit log | Accounts / Contacts: {USER} modified SAML group {NAME} from {IP}                                   |
| 33204 | Audit log | Accounts / Contacts: {USER} deleted SAML group {NAME} from {IP}                                    |
| 33205 | Audit log | Accounts / Contacts: {USER} enabled SAML group {NAME} from {IP}                                    |
| 33206 | Audit log | Accounts / Contacts: {USER} disabled SAML group {NAME} from {IP}                                   |
| 33301 | Audit log | License: {NAME} license activated by {USER} from {IP}  |
| 33302 | Audit log | License: Attempted to activate {NAME} license using an invalid Activation Code by {USER} from {IP} |
| 33303 | Audit log | License: {NAME} license updated by {USER} from {IP}  |
| 33401 | Audit log | Policy: Policy setting changed by {USER} from {IP}   |
| 33402 | Audit log | Policy: {USER} added policy {NAME} from {IP}   |
| 33403 | Audit log | Policy: {USER} modified policy {NAME} from {IP}  |
| 33404 | Audit log | Policy: {USER} imported policies from {IP}   |
| 33405 | Audit log | Policy: {USER} deleted policy {NAME} from {IP}   |
| 33406 | Audit log | Policy: {USER} copied policy {NAME} from {IP}  |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 33407 | Audit log | Policy: {USER} enabled policy {NAME} from {IP}  |
| 33408 | Audit log | Policy: {USER} disabled policy {NAME} from {IP}   |
| 33409 | Audit log | Policy: {USER} modified priority setting of policy {NAME} from {PRIORITY} to {PRIORITY} from {IP} |
| 33410 | Audit log | Policy: {USER} added content filtering rule {NAME} from {IP}                                      |
| 33411 | Audit log | Policy: {USER} updated content filtering rule {NAME} from {IP}                                    |
| 33412 | Audit log | Policy: {USER} copied content filtering rule {NAME} from {IP}                                     |
| 33413 | Audit log | Policy: {USER} deleted content filtering rule {NAME} from {IP}                                    |
| 33414 | Audit log | Policy: {USER} added antispam rule {NAME} from {IP}   |
| 33415 | Audit log | Policy: {USER} updated antispam rule {NAME} from {IP}   |
| 33416 | Audit log | Policy: {USER} copied antispam rule {NAME} from {IP}  |
| 33417 | Audit log | Policy: {USER} deleted antispam rule {NAME} from {IP}   |
| 33418 | Audit log | Policy: {USER} added advanced threat protection rule {NAME} from {IP}                             |
| 33419 | Audit log | Policy: {USER} updated advanced threat protection rule {NAME} from {IP}                           |
| 33420 | Audit log | Policy: {USER} copied advanced threat protection rule {NAME} from {IP}                            |
| 33421 | Audit log | Policy: {USER} deleted advanced threat protection rule {NAME} from {IP}                           |
| 33422 | Audit log | Policy: {USER} added policy notification {NAME} from {IP}   |
| 33423 | Audit log | Policy: {USER} modified policy notification {NAME} from {IP}                                      |
| 33424 | Audit log | Policy: {USER} deleted some policy notifications from {IP}  |
| 33425 | Audit log | Policy: {USER} copied policy notification {NAME} from {IP}  |
| 33426 | Audit log | Policy: {USER} added archive server {NAME} from {IP}  |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 33427 | Audit log | Policy: {USER} modified archive server {NAME} from {IP}        |
| 33428 | Audit log | Policy: {USER} deleted some archive servers from {IP}          |
| 33429 | Audit log | Policy: {USER} added DLP rule {NAME} from {IP}                 |
| 33430 | Audit log | Policy: {USER} updated DLP rule {NAME} from {IP}               |
| 33431 | Audit log | Policy: {USER} copied DLP rule {NAME} from {IP}                |
| 33432 | Audit log | Policy: {USER} deleted DLP rule {NAME} from {IP}               |
| 33433 | Audit log | Policy Objects: {USER} added expression {NAME} from {IP}       |
| 33434 | Audit log | Policy Objects: {USER} updated expression {NAME} from {IP}     |
| 33435 | Audit log | Policy Objects: {USER} copied expression {NAME} from {IP}      |
| 33436 | Audit log | Policy Objects: {USER} deleted expression {NAME} from {IP}     |
| 33437 | Audit log | Policy Objects: {USER} imported expression file from {IP}      |
| 33438 | Audit log | Policy Objects: {USER} added file attribute {NAME} from {IP}   |
| 33439 | Audit log | Policy Objects: {USER} updated file attribute {NAME} from {IP} |
| 33440 | Audit log | Policy Objects: {USER} copied file attribute {NAME} from {IP}  |
| 33441 | Audit log | Policy Objects: {USER} deleted file attribute {NAME} from {IP} |
| 33442 | Audit log | Policy Objects: {USER} imported file attribute file from {IP}  |
| 33443 | Audit log | Policy Objects: {USER} added keyword list {NAME} from {IP}     |
| 33444 | Audit log | Policy Objects: {USER} updated keyword list {NAME} from {IP}   |
| 33445 | Audit log | Policy Objects: {USER} copied keyword list {NAME} from {IP}    |
| 33446 | Audit log | Policy Objects: {USER} deleted keyword list {NAME} from {IP}   |
| 33447 | Audit log | Policy Objects: {USER} imported keyword list file from {IP}    |
| 33448 | Audit log | Policy Objects: {USER} added template {NAME} from {IP}         |
| 33449 | Audit log | Policy Objects: {USER} updated template {NAME} from {IP}       |

| ID    | LOG TYPE  | MESSAGE   |
|-------|-----------|---|
| 33450 | Audit log | Policy Objects: {USER} copied template {NAME} from {IP}                                 |
| 33451 | Audit log | Policy Objects: {USER} deleted template {NAME} from {IP}                                |
| 33452 | Audit log | Policy Objects: {USER} imported template file from {IP}                                 |
| 33453 | Audit log | Policy Objects: {USER} added policy stamp {NAME} from {IP}                              |
| 33454 | Audit log | Policy Objects: {USER} modified policy stamp {NAME} from {IP}                           |
| 33455 | Audit log | Policy Objects: {USER} deleted some policy stamps from {IP}                             |
| 33456 | Audit log | Policy Objects: {USER} enabled policy stamp {NAME} from {IP}                            |
| 33457 | Audit log | Policy Objects: {USER} disabled policy stamp {NAME} from {IP}                           |
| 33458 | Audit log | Policy Objects: {USER} added address group {NAME} from {IP}                             |
| 33459 | Audit log | Policy Objects: {USER} deleted address group {NAME} from {IP}                           |
| 33460 | Audit log | Policy Objects: {USER} updated address group {NAME} from {IP}                           |
| 33501 | Audit log | Policy: Policy exception settings modified by {USER} from {IP}                          |
| 33502 | Audit log | Policy: Graymail exception settings modified by {USER} from {IP}                        |
| 33601 | Audit log | Alerts: Alert rule settings modified by {USER} from {IP}                                |
| 33701 | Audit log | Report: Report settings changed by {USER} from {IP}                                     |
| 33801 | Audit log | Detected Messages: Message {NAME} downloaded by {USER} from {IP}                        |
| 33802 | Audit log | Detected Messages: Investigation package {NAME} downloaded by {USER} from {IP}          |
| 33803 | Audit log | Detected Messages: Screenshot of message {NAME} viewed by {USER} from {IP}              |
| 33804 | Audit log | Detected Messages: Virtual Analyzer report of message {NAME} viewed by {USER} from {IP} |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 33901 | Audit log | Quarantine: MsgID {ID} released by {USER} from {IP}  |
| 33902 | Audit log | Quarantine: MsgID {ID} deleted by {USER} from {IP}   |
| 33903 | Audit log | Quarantine: Resumed processing message {ID} by {USER} from {IP}  |
| 33904 | Audit log | Quarantine: Message {ID} unlocked and reprocessed by {USER} from {IP}  |
| 34001 | Audit log | Unable to distribute suspicious objects to Check Point OPSEC. Verify that the Check Point OPSEC settings are correct and that no network problem exists.                                     |
| 34002 | Audit log | Unable to distribute suspicious objects to Trend Micro TippingPoint SMS. Verify that the Trend Micro TippingPoint SMS settings are correct and that no network problem exists.               |
| 34003 | Audit log | Unable to distribute suspicious objects to IBM Security Network Protection XGS. Verify that the IBM Security Network Protection XGS settings are correct and that no network problem exists. |
| 34004 | Audit log | Unable to distribute suspicious objects to Palo Alto Panorama or Firewalls. Verify that the Palo Alto Panorama or Firewalls settings are correct and that no network problem exists.         |
| 34005 | Audit log | Unable to generate suspicious objects list. Verify that the Threat Intelligence Sharing settings are correct.  |
| 34101 | Audit log | End-User Quarantine: EUQ settings modified by {USER} from {IP}   |
| 34102 | Audit log | End-User Quarantine: User Quarantine Access settings modified by {USER} from {IP}  |
| 34103 | Audit log | End-User Quarantine: EUQ Digest settings modified by {USER} from {IP}  |
| 34201 | Audit log | Sender Filtering: Approved Senders list modified by {USER} from {IP}   |
| 34202 | Audit log | Sender Filtering: ERS settings modified by {USER} from {IP}  |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 34203 | Audit log | Sender Filtering: DHA protection settings modified by {USER} from {IP}                                 |
| 34204 | Audit log | Sender Filtering: Bounced attack protection settings modified by {USER} from {IP}                      |
| 34205 | Audit log | Sender Filtering: SMTP traffic throttling settings modified by {USER} from {IP}                        |
| 34206 | Audit log | Sender Filtering: Blocked Senders list modified by {USER} from {IP}                                    |
| 34207 | Audit log | Sender Filtering: Some Blocked Senders list entries moved to Approved Senders list by {USER} from {IP} |
| 34208 | Audit log | Sender Filtering: SPF settings modified by {USER} from {IP}  |
| 34209 | Audit log | Sender Filtering: DKIM Authentication settings modified by {USER} from {IP}                            |
| 34210 | Audit log | Sender Filtering: DKIM Signatures settings modified by {USER} from {IP}                                |
| 34211 | Audit log | Sender Filtering: DMARC settings modified by {USER} from {IP}  |
| 35001 | Audit log | Message Queues: Messages deleted by {USER} from {IP}   |
| 35002 | Audit log | Message Queues: Messages delivered by {USER} from {IP}   |
| 35003 | Audit log | Message Queues: All messages delivered by {USER} from {IP}   |
| 35004 | Audit log | Message Tracking: Investigation package {NAME} downloaded by {USER} from {IP}                          |
| 35005 | Audit log | Email Submissions: Message submitted by {USER} from {IP}   |
| 35006 | Audit log | Message Queues: Messages rerouted by to {IP} by {USER} from {IP}                                       |
| 35007 | Audit log | Message Queues: All messages rerouted by to {IP} by {USER} from {IP}                                   |
| 35008 | Audit log | Message Queues: All messages deleted by {USER} from {IP}   |

| ID    | LOG TYPE  | MESSAGE  |
|-------|-----------|--|
| 35011 | Audit log | Integrated Products/Services: Registered to Email Encryption server by {USER} from {IP}                            |
| 35012 | Audit log | Integrated Products/Services: Domain {DOMAIN} added to Email Encryption server by {USER} from {IP}                 |
| 35013 | Audit log | Integrated Products/Services: Domain {DOMAIN} deleted from Email Encryption server by {USER} from {IP}             |
| 35014 | Audit log | Integrated Products/Services: Key file uploaded to Email Encryption server for domain {DOMAIN} by {USER} from {IP} |
| 35016 | Audit log | Integrated Products/Services: Default sender modified to {SENDER} for Email Encryption by {USER} from {IP}         |
| 35017 | Audit log | Integrated Products/Services: Email address modified to {EMAIL} for Email Encryption by {USER} from {IP}           |
| 35021 | Audit log | Integrated Products/Services: {USER} added identity provider server {NAME} from {IP}                               |
| 35022 | Audit log | Integrated Products/Services: {USER} modified identity provider server {NAME} from {IP}                            |
| 35023 | Audit log | Integrated Products/Services: {USER} deleted identity provider server {NAME} from {IP}                             |
| 35024 | Audit log | Integrated Products/Services: {USER} enabled identity provider server {NAME} from {IP}                             |
| 35025 | Audit log | Integrated Products/Services: {USER} disabled identity provider server {NAME} from {IP}                            |
| 35026 | Audit log | Integrated Products/Services: {USER} updated certificate for management console from {IP}                          |
| 35027 | Audit log | Integrated Products/Services: {USER} updated certificate for EUQ console from {IP}                                 |
| 35028 | Audit log | Logon: {USER} logged on via identity provider server {NAME} as {ROLE} from {IP}                                    |
| 35029 | Audit log | Logon: {USER} logged off via identity provider server {NAME} from {IP}   |

| ID    | LOG TYPE | MESSAGE  |
|-------|----------|--|
| 41001 | EUQ log  | EUQ: {USER} logged on from {IP}                                      |
| 41002 | EUQ log  | EUQ: {USER} logged off from {IP}                                     |
| 41003 | EUQ log  | EUQ: MsgID {ID} released by {USER} from {IP}                         |
| 41004 | EUQ log  | EUQ: MsgID {ID} deleted by {USER} from {IP}                          |
| 41005 | EUQ log  | EUQ: Approved Senders list modified by {USER} from {IP}              |
| 41006 | EUQ log  | EUQ: {USER} logged on via identity provider server {NAME} from {IP}  |
| 41007 | EUQ log  | EUQ: {USER} logged off via identity provider server {NAME} from {IP} |



# Appendix G

## Sender Authentication Error Codes

This appendix includes the error codes for each sender authentication protocols.

### Sender Policy Framework (SPF) Error Codes

**TABLE G-1. SPF Error Code Classification**

| ERROR TYPE         | ERROR CODES |
|--------------------|-------------|
| Invalid SPF record | 3~25, 27~32 |
| No SPF record      | 2           |
| Internal error     | -99, 1, 26  |

**TABLE G-2. SPF Error Codes**

| ERROR CODE | MESSAGE                    |
|------------|----------------------------|
| -99        | Internal error             |
| 1          | Insufficient memory        |
| 2          | No SPF record              |
| 3          | Syntax error               |
| 4          | Modifiers contain prefixes |

| ERROR CODE | MESSAGE                                  |
|------------|--|
| 5          | Invalid characters found                 |
| 6          | Unknown mechanisms found                 |
| 7          | Invalid option found                     |
| 8          | Invalid CIDR length                      |
| 9          | Required option is missing               |
| 10         | Internal error                           |
| 11         | Invalid %-escape character               |
| 12         | Invalid macro variable                   |
| 13         | Subdomain truncation depth too large     |
| 14         | Invalid delimiter character              |
| 15         | Option string too long                   |
| 16         | Excessive mechanisms                     |
| 17         | Excessive modifiers                      |
| 18         | Excessive DNS lookups used in mechanisms |
| 19         | Invalid IPv4 address                     |
| 20         | Invalid IPv6 address                     |
| 21         | Invalid mechanism prefix                 |
| 22         | SPF result is unknown                    |
| 23         | Uninitialized variable                   |
| 24         | Modifier not found                       |
| 25         | Required setting not configured          |
| 26         | DNS lookup unsuccessful                  |
| 27         | Invalid hostname or format               |

| ERROR CODE | MESSAGE  |
|------------|--|
| 28         | Invalid or missing TLD in hostname                                   |
| 29         | Ignore mechanisms after "all:"                                       |
| 30         | SPF result is permerror when an include recursive query returns none |
| 31         | Recursive include  |
| 32         | Multiple SPF or TXT records found                                    |
| 51         | IP address is 0.0.0.0  |
| 52         | from and ehlo parameters are null                                    |
| 53         | none rule matched  |
| 54         | neutral rule matched   |
| 55         | softfail rule matched  |
| 56         | fail rule matched  |
| 57         | temperror rule matched   |
| 58         | permerror rule matched   |

### DomainKeys Identified Mail (DKIM) Error Codes

**TABLE G-3. DKIM Error Code Classification**

| ERROR TYPE              | ERROR CODES   |
|-------------------------|---|
| Invalid DKIM record     | 1, 23~24, 116, 34, 36, 38, 40, 41, 42, 43, 46, 108, 111 |
| No DKIM record          | 22, 103, 104  |
| Invalid DKIM signature  | 2~5, 7~21, 25~27, 31~33, 44~45, 102, 105                |
| DKIM signature mismatch | 28, 37, 101   |
| Internal error          | -1, 6, 39, 107, 112~115 and all others                  |

**TABLE G-4. DKIM Error Codes**

| <b>ERROR CODE</b> | <b>MESSAGE</b>             | <b>RESULT</b> |
|-------------------|----------------------------|---------------|
| -1                | Internal error             | PermError     |
| 0                 | Successful                 | Pass          |
| 1                 | Unsupported version        | Fail          |
| 2                 | Invalid domain (d=/i=)     | PermError     |
| 3                 | Signature expired          | Fail          |
| 4                 | Signature in the future    | Fail          |
| 5                 | x= < t=                    | Fail          |
| 6                 | Obsolete                   | Fail          |
| 7                 | Invalid c= value in header | Neutral       |
| 8                 | Invalid c= value in body   | Neutral       |
| 9                 | Missing a= value           | PermError     |
| 10                | Invalid a= value           | Neutral       |
| 11                | Missing h= value           | PermError     |
| 12                | Invalid l= value           | Neutral       |
| 13                | Invalid q= value           | Neutral       |
| 14                | Invalid q= option          | Neutral       |
| 15                | Missing d=value            | PermError     |
| 16                | d= value is empty          | Neutral       |
| 17                | Missing s= value           | PermError     |
| 18                | s= value is empty          | Neutral       |
| 19                | Missing b= value           | PermError     |
| 20                | b= value is empty          | Neutral       |

| ERROR CODE | MESSAGE                              | RESULT    |
|------------|--------------------------------------|-----------|
| 21         | b= value is corrupt                  | PermError |
| 22         | No key found in DNS                  | None      |
| 23         | Bad DNS reply                        | Neutral   |
| 24         | Unsuccessful DNS reply               | TempError |
| 25         | Missing bh= value                    | PermError |
| 26         | bh= value is empty                   | Neutral   |
| 27         | Bad bh= value                        | PermError |
| 28         | Signature mismatch                   | Fail      |
| 29         | Unauthorized subdomain               | TempError |
| 30         | Multiple records returned            | TempError |
| 31         | h= value is empty                    | Neutral   |
| 32         | Missing required entries in h= value | Neutral   |
| 33         | l= value exceeds body size           | Neutral   |
| 34         | Signing required not met             | Neutral   |
| 35         | Unknown key version                  | Neutral   |
| 36         | Unknown key hash                     | Neutral   |
| 37         | Signature-key hash mismatch          | PermError |
| 38         | Not an email key                     | Neutral   |
| 39         | Obsolete                             | Fail      |
| 40         | Missing key type                     | Neutral   |
| 41         | Unknown key type                     | Neutral   |
| 42         | Key revoked                          | PermError |
| 43         | Undecodable key                      | PermError |

| ERROR CODE | MESSAGE                    | RESULT    |
|------------|----------------------------|-----------|
| 44         | Missing v= tag             | PermError |
| 45         | v= tag is empty            | Fail      |
| 46         | Insufficient key bits      | PermError |
| 101        | Bad signature              | Fail      |
| 102        | No signature available     | Fail      |
| 103        | Public key not found       | None      |
| 104        | No domain key to verify    | None      |
| 105        | Syntax error               | Fail      |
| 106        | Resource unavailable       | Fail      |
| 107        | Internal error             | Fail      |
| 108        | Key revoked                | Fail      |
| 109        | Invalid function parameter | Fail      |
| 110        | Function not implemented   | Fail      |
| 111        | Unable to retrieve key     | Fail      |
| 112        | Callback request rejected  | Fail      |
| 113        | Invalid callback result    | Fail      |
| 114        | Callback timeout           | Fail      |
| 115        | Callback timeout           | Fail      |
| 116        | Multiple DNS replies       | Fail      |

## Domain-based Message Authentication, Reporting & Conformance (DMARC) Error Codes

**TABLE G-5. DMARC Error Code Classification**

| ERROR TYPE                   | ERROR CODES     |
|------------------------------|-----------------|
| Invalid DMARC record         | 2~5, 11         |
| No DMARC record              | 1, 6, 9, 10, 12 |
| Authentication unsuccessful  | 13              |
| Alignment check unsuccessful | 21              |
| Internal error               | 7, 8            |

**TABLE G-6. DMARC Error Codes**

| ERROR CODE | MESSAGE                   |
|------------|---------------------------|
| 0          | Successful                |
| 1          | No data                   |
| 2          | NULL context received     |
| 3          | Invalid v= value          |
| 4          | Invalid p= value          |
| 5          | Missing p= value          |
| 6          | No domain found           |
| 7          | Unable to allocate memory |
| 8          | Not a macro               |
| 9          | No DMARC record           |
| 10         | Domain does not exist     |
| 11         | Recoverable DNS error     |
| 12         | Undefined TLD type        |

| ERROR CODE | MESSAGE  |
|------------|--|
| 13         | From: domain not available                                   |
| 14         | No DMARC record found for custom policy                      |
| 15         | Accept message based on policy settings                      |
| 16         | Reject message based on policy settings                      |
| 17         | Quarantine message based on policy settings                  |
| 18         | Monitor message and generate report based on policy settings |
| 19         | Apply domain policy ('p')                                    |
| 20         | Apply sub-domain policy ('sp')                               |
| 21         | Alignment check unsuccessful                                 |

# Appendix H

## Glossary

| TERM  | DEFINITION   |
|---|--|
| ActiveUpdate Server   | Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.  |
| Advanced Threat Scan Engine<br>Advanced Threat Scan Engine (64-bit) | The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection. |
| Affected Recipient  | A recipient of malicious or suspicious email messages.   |

| TERM                  | DEFINITION  |
|-----------------------|---|
| Alert                 | <p>An occurrence of an event or set of events triggering a predefined condition.</p> <p>Alerts have the following levels of importance:</p> <ul style="list-style-type: none"><li>• Critical Alert<br/>A message about an event that requires immediate attention.</li><li>• Important Alert<br/>A message about an event that does not require immediate attention, but should be observed.</li><li>• Informational Alert<br/>A message about an event that is most likely benign.</li></ul>   |
| Archive               | <p>A file composed of one or more files that have been concatenated, compressed, or encrypted for portability or storage.</p> <p>An “archive” may also be called a “compressed file”.</p>   |
| Archive file password | A password to decrypt an archive.   |
| Attack source         | The first mail server with a public IP address that routes a suspicious message. For example, if a suspicious message routes from IP1 (sender) to IP2 (MTA: 225.237.59.52) to IP3 (company mail gateway) to IP4 (recipient), Deep Discovery Email Inspector identifies 225.237.59.52 (IP2) as the attack source. By studying attack sources, you can identify regional attack patterns or attack patterns that involve the same mail server.  |
| Attacker              | An individual, group, organization, or government that conducts or has the intent to conduct harmful activities.  |
| Authentication        | <p>The verification of the identity of a person or a process. Authentication ensures that the system delivers the digital data transmissions to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).</p> <p>The simplest form of authentication requires a user name and password to gain access to a particular account. Other authentication protocols are secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or public-key systems using digital signatures.</p> |

| TERM                                   | DEFINITION   |
|--|--|
| Bot                                    | A program that infects computers connected to the Internet, allowing them to be remotely controlled by an attacker. Bot-controlled computers become part of a network of compromised machines that are exploited by the attacker for malicious activities.   |
| Botnet                                 | A botnet (short for “bot network”) is a network of hijacked zombie computers controlled remotely by an attacker. The attacker uses the network to send spam and launch Denial of Service attacks, and may rent the network out to other cybercriminals. If one of the computers targeted becomes compromised, the attacker can often take control of that computer and add it to the botnet. |
| BCC mode                               | A Deep Discovery Email Inspector operation mode. Deep Discovery Email Inspector operates as an out-of-band appliance. Deep Discovery Email Inspector silently monitors mirrored email traffic received from an upstream mail server and notifies security administrators about discovered threats.   |
| Callback address                       | <p>An external IP address, host name, or URL that an object requests (“calls back to”) during scanning or analysis. Malware connected to a C&amp;C server often sends requests to it in order to carry out harmful activities.</p> <p>The host name or IP address that an object requests may be called a “callback host”. A URL that an object requests may be called a “callback URL”.</p> |
| Command-and-Control (C&C) server       | The central server (s) for a botnet or entire network of compromised devices used by a malicious bot to propagate malware and infect a host.   |
| Compromised MTA                        | A compromised MTA is usually a third-party open mail relay that attackers can use to send malicious email messages or spam without detection because the mail relay does not check the source or destination for known users.  |
| Certified Safe Software Service (CSSS) | Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources.   |

| TERM                          | DEFINITION  |
|-------------------------------|---|
| Communicator                  | The communications backbone of the Apex Central system. Communicator is part of the Apex Central Management Infrastructure. Commands from the Apex Central server to Deep Discovery Email Inspector, and status reports from Deep Discovery Email Inspector to the Apex Central server all pass through this component. |
| Data port                     | A hardware port that accesses resources available on a network.   |
| Detection                     | A discovered event, file, or network address. Detections include unusual, undesired, suspicious, unknown, and malicious behaviors and connections.  |
| Event                         | An observable, measurable occurrence in a system or network.  |
| False positive                | A detection that is determined to be high risk but is actually benign.  |
| File submission rule          | A set of criteria and conditions used to reduce the number of files in the Virtual Analyzer queue. File submission rules check files based on detection types, detection rules, and file properties.  |
| IntelliTrap                   | A Trend Micro utility that helps reduce the risk of viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics.   |
| IntelliTrap Exception Pattern | The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning.  |
| IntelliTrap Pattern           | The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats.   |
| Log                           | An official record of events occurring in a system or network.  |
| Management console            | A web-based user interface for managing a product.  |
| Management port               | A hardware port that connects to the management network.  |

| TERM                             | DEFINITION   |
|----------------------------------|--|
| Message ID                       | A unique identifier for a digital message, most commonly a globally unique identifier used in email messages. Message IDs must have a specific format (subset of an email address) and be globally unique. A common technique used by many message systems is to use a time and date stamp along with the local host's domain name.                                  |
| Message stamp                    | Text added at the beginning or end of the email message.   |
| Message tag                      | Text added to the subject line of the email message.   |
| MTA mode                         | A Deep Discovery Email Inspector operation mode. Deep Discovery Email Inspector can act as a Mail Transfer Agent (MTA) in the mail traffic flow. As an inline MTA, Deep Discovery Email Inspector directly protects your network from harm by blocking malicious email messages.   |
| Notification                     | A message triggered by an event in an endpoint or network.   |
| Permitted sender                 | An email sender approved by Deep Discovery Email Inspector as being safe.  |
| Permitted sender of relayed mail | An endpoint permitted or denied connection to the appliance based on the IP address of a single endpoint or any endpoint in an IP address range.   |
| Port                             | <p>The following term has multiple definitions depending upon its context:</p> <ul style="list-style-type: none"><li>• Hardware<br/>A socket on an endpoint to connect to a removable device, cable, or other external equipment.</li><li>• TCP/IP Networking<br/>An access channel by which software applications can use hardware resources in parallel.</li></ul> |
| Report                           | A compilation of data generated from selectable criteria, used to provide the user with needed information.  |

| TERM  | DEFINITION   |
|---|--|
| Sample  | <p>A potentially malicious file or URL submitted to Virtual Analyzer. Virtual Analyzer opens the file or accesses the link in the sample to analyze the risk level. If Virtual Analyzer finds any additional links or files while analyzing a sample, Virtual Analyzer also analyzes them.</p> <p>Example: If a user submits an archive that contains multiple files to Virtual Analyzer, Virtual Analyzer will analyze the archive as well as all of the encrypted files.</p> |
| Sandbox image                                     | A template used to deploy sandbox instances in Virtual Analyzer. A sandbox image includes an operating system, installed software, and other settings necessary for that specific computing environment.   |
| Sandbox instance                                  | A single virtual machine based on a sandbox image.   |
| Script Analyzer Engine<br>Script Analyzer Pattern | The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code.  |
| Smart Feedback                                    | Shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains.  |
| Smart Protection Network                          | Rapidly and accurately identifies new threats, delivering global threat intelligence to all Trend Micro products and services. The Smart Protection Network cloud data mining framework advances in the depth and breadth allow Trend Micro to look in more places for threat data, and respond to new threats more effectively, to secure data wherever it resides.   |
| Social engineering                                | A form of attack to psychologically manipulate a person to perform actions or divulge confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.  |
| Source IP address                                 | <p>The IP address of the mail server nearest to the email sender.</p> <p>Examples: gateway mail server, compromised mail server, botnet with mail relay capabilities</p>   |

| TERM                     | DEFINITION   |
|--------------------------|--|
| SPAN/TAP mode            | A Deep Discovery Email Inspector operation mode. Deep Discovery Email Inspector operates as an out-of-band appliance. Deep Discovery Email Inspector silently monitors mirrored email traffic received from a switch or network tap and notifies security administrators about discovered threats.   |
| Spear phishing           | A type of targeted attack where an attacker sends an email message masquerading as a known or legitimate entity to gain personal information from a targeted person. Spear phishing significantly raises the chances that targets will read a message that will allow to compromise a target network. In many cases, spear-phishing emails use attachments made to appear as legitimate documents because sharing via email is a common practice among large enterprises and government organizations. |
| Spyware Pattern          | The Spyware Pattern identifies spyware and grayware in messages and attachments.   |
| Threat Connect           | Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.  |
| Threat Knowledge Base    | The Threat Knowledge Base provides information for threat correlation.   |
| True file type           | The kind of data stored in a file, regardless of the file extension.<br>Example: A text file may have an extension of HTML, CSV, or TXT, but its true file type remains the same.  |
| Unscannable Archive      | A password-protected archive that cannot be extracted and scanned using a custom-defined password list or heuristically obtained passwords.  |
| Viewer account           | An account that can view detection and system information, but does not have access to most configuration screens on the management console.   |
| Virtual Analyzer         | An isolated virtual environment used to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.  |
| Virtual Analyzer Sensors | The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer.  |

| TERM                    | DEFINITION   |
|-------------------------|--|
| Virus Pattern           | The Trend Micro Virus Scan Engine protects against viruses and malware in files through heuristic, signature-based, and behavior-based detection. Trend Micro updates the virus pattern files as soon as detection routines for new threats are available. |
| Web Reputation Services | Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis.     |
| Widget Framework        | The Widget Framework provides the template for Deep Discovery Email Inspector widgets.   |

# Index

## A

### about

- features, 1-5
- Maintenance Agreement, 8-229
- new threats, 1-10
- product overview, 1-12

### accounts

- administration, 8-209
- managing, 8-210
- role-based access, 8-209
- unlock, 8-214
- using for console access, 8-209

### Active Directory

- group, 8-212
- user account, 8-212
- User Principle Name (UPN), 8-212

### Active Directory Federation Services (AD FS), 8-173

### add local user account, 8-212

### address groups, 5-81

- add, 5-82
- edit, 5-82

### address modification, 8-109

- address rewriting, 8-109
- domain rewriting, 8-111

### address rewriting, 8-109

### AD FS, 8-173

### admin

- default account, 8-210

### admin accounts, 8-211, 8-213

### administration, 8-1, 8-2, 8-4-8-12, 8-14, 8-16, 8-17, 8-20, 8-21, 8-28, 8-34, 8-35, 8-94, 8-95, 8-97, 8-98, 8-100, 8-101, 8-105, 8-178, 8-181, 8-187, 8-190, 8-193, 8-194, 8-197, 8-211-8-214, 8-217-8-219, 8-223, 8-224, 8-226-8-228

### account roles, 8-211

### accounts, managing accounts, 8-210

### accounts / contacts, overview, 8-209

### Active Directory group, 8-212

### Active Directory user account, 8-212

### admin account, 8-213, 8-214

### archive file passwords, 8-34, 8-35

### backup recommendations, 8-219

### back up settings, 8-217-8-219, 8-223

### components, 8-2, 8-4-8-6

### contacts, 8-217

### email scanning, 8-10

### export debug file, 8-226

### file passwords, 8-34

### license, 8-228

### local user account, 8-212

### log level, 8-227

### log settings, 8-178

### mail settings, 8-94

### message delivery, 8-94

### network settings, 8-187

### operation mode, 8-190

### product upgrades, 8-6-8-8

### proxy settings, 8-193

### restore settings, 8-217-8-219, 8-223

### scanning / analysis, 8-9

### SFTP upload, 8-181

### SMTP, 8-101

### SMTP connections, 8-95

### SMTP greeting, 8-105

### SMTP routing, 8-98, 8-100

### SMTP server, 8-194

- storage management, 8-224
- system and accounts, 8-197
- system maintenance, 8-217
- system settings, 8-187
- TLS, 8-97
- unable to restore settings, 8-219, 8-223
- Virtual Analyzer, 8-11, 8-12, 8-14, 8-16, 8-17, 8-20, 8-21, 8-28
- administrator accounts
  - role, 8-210
- advanced detection, 1-5
- Advanced Threat Scan Engine, 1-13, 8-10, H-1
  - about, 1-13
- affected recipients, 4-15
- alerts, 6-1–6-3, 6-5–6-7, 6-10, 6-24
  - contacts for receiving, 8-209
  - critical alerts, 6-2
  - delete, 6-6
  - export, 6-6
  - important alerts, 6-3
  - informational alerts, 6-5
  - manage, 6-6
  - notification parameters, 6-7, 6-10, 6-24
  - required settings, 6-5
    - alerts, 6-5
  - triggered alerts, 6-6
  - view, 6-6
- analysis, 8-9, 8-10
- Analysis reports, 8-124
- Antispam Engine, 8-2
- Antispam Pattern, 8-2
- antispam protection, 1-7
- antispam rule, 5-45, 5-46

- Apex Central
  - about, 8-127
  - unregister, 8-132
- approved senders, 8-57, 8-59, 8-61
- Business Email Compromise (BEC), 8-50
- End-User Quarantine, 8-92
- Approved Senders list, 8-52, 8-57
  - add, 8-59
  - Business Email Compromise (BEC), 8-50
  - delete, 8-57
  - End-User Quarantine, 8-92
  - import, 8-61
- atse, 8-10
- ATSE, 1-13, H-1
  - about, 1-13
- attacker, 1-11
- attack sources, 4-16
- audit logs, F-1
- average Virtual Analyzer queue time alert, 6-3

**B**

- backup, 8-217–8-219, 8-223
- backup recommendations, 8-219
- benefits, 1-5
- blocked senders, 8-61, 8-64, 8-65
- Blocked Senders list, 8-52, 8-61, 8-64, 8-65
- blocking page, 5-59
- Bounce attack protection, 8-53
- built-in redirect pages, 5-59
- Business Email Compromise (BEC), 8-48–8-50
  - approved senders, 8-50
  - high-profile users, 8-48

internal domains, 8-49

## C

C&C, 1-11

callback, 1-11

certificate authority (CA), 8-207

Certificate Authority (CA), 8-202

certificate management, 1-2, 8-203

certificates, 8-202

assign to services, 8-207

Certificate Authority (CA), 8-202

export, 8-207

HTTPS, 8-203

import, 8-206, 8-208

obtain, 8-113

SMTP, 8-203

tasks, 8-203, 8-208

trusted CA, 8-207

Certified Safe Software Service, 8-20

change password, 8-215

CLI, A-1

command-and-control, 1-11

command line interface

entering the shell environment,

A-3

Command Line Interface, A-1

accessing, A-2

using, A-2

components, 8-2

rollback, 8-5

update components, 8-5

updates, 8-6

update source, 8-4

component updates, 8-1

condition statements, 5-77

configuration, 2-1, 8-1

local user account, 8-212

management console, 2-5, 2-7

overview, 2-2

policy, 5-59

configure

import SMTP settings, 8-100

Messaged Delivery settings, 8-99,  
8-100

message delivery settings, 8-97,  
8-98, 8-101, 8-105

SMTP connections, 8-95

configure system time, 8-197

connection security, 8-209

console access

using accounts for, 8-209

contacts

administration, 8-209

for receiving alerts and reports,  
8-209

content filtering, 5-37, 5-38, 5-41

scanning conditions, 5-41

attachments, 5-41

content filtering rule, 5-38, 5-42

cousin domains, 8-50, 8-51

exceptions, 8-51

settings, 8-51

thresholds, 8-51

CPU usage alert, 6-3

criteria

customized expressions, 5-65, 5-66

keyword list, 5-73, 5-74

critical alerts, 6-2, 6-5, 6-7

CSSS, 8-20

customized DLP templates

exporting, 5-80

customized expressions, 5-64-5-66

- criteria, 5-65, 5-66
- customized keyword list
  - criteria, 5-73, 5-74
- customized keyword lists
  - importing, 5-75
- customized keywords, 5-72
- customized templates, 5-77
  - importing, 5-80

## **D**

- dashboard, 3-1, 3-2, 3-4–3-6, 3-8–3-17
  - dashboard
    - tabs, 3-2
  - overview, 3-2, 3-6
  - tabs, 3-2
  - widgets, 3-2, 3-4–3-17
- data identifiers, 5-62
  - expressions, 5-62
  - file attributes, 5-62
  - keywords, 5-62
- Data Loss Prevention, 5-62
  - data identifiers, 5-62
  - expressions, 5-63–5-66
  - file attributes, 5-68–5-71
  - keyword lists, 5-72–5-75
  - keywords, 5-72
  - templates, 5-77, 5-78, 5-80
- Data Loss Prevention (DLP), 5-43
  - rule, 5-43
  - templates, 5-76
- daylight savings time, 7-2
- Deep Discovery Analyzer integration, 8-28
- Deep Discovery Malware Pattern, 8-3
- default account
  - admin, 8-210

- delete admin accounts, 8-214
- delete alerts, 6-6
- delete image, 8-17
- deleting, editing, adding
  - accounts, 8-210
- deployment, 1-5
- deploy TLS, 8-112
- detected message alert, 6-3
- detected risk, 4-2
- detections, 4-1
  - detected risk, 4-2
  - email message risk levels, 4-2
  - sender filtering/authentication, 4-34
  - suspicious message, 4-7
  - suspicious messages, 4-6, 4-7, 4-9, 4-13, 4-15, 4-16, 4-18, 4-19, 4-21–4-24, 4-26, 4-28, 4-31, 4-33
  - threat types, 4-5
  - Virtual Analyzer risk levels, 4-4
- detection surge alert, 6-5
- DHA protection, 8-53
- directory harvest attack (DHA), 8-66
- disk space alert, 6-3
- DKIM, 8-74
  - add signature, 8-77
  - authentication settings, 8-74
  - edit signature, 8-77
  - error code classification, G-3
  - error codes, G-3
  - import signature list, 8-79
  - signatures, 8-76
  - signing, 8-76
- DKIM signatures, 8-76
  - add, 8-77
  - edit, 8-77

- import list, 8-79
- DLP rule, 5-44
- DLP templates, 5-80
  - customized, 5-80
- DMARC, 8-79
  - error code classification, G-7
  - error codes, G-7
  - settings, 8-80
- documentation feedback, 9-5
- Domain-based Message Authentication, Reporting & Conformance (DMARC), 8-79
  - settings, 8-80
- DomainKeys Identified Mail (DKIM), 8-74
  - add signature, 8-77
  - authentication settings, 8-74
  - edit signature, 8-77
  - import signature list, 8-79
  - signatures, 8-76
  - signing, 8-76
- domain rewriting, 8-111
- Download Center, 8-7, 8-8
- downloader, 1-11
- DST, 7-2
- E**
- edge MTA relay server, 8-105
- edge MTA relay servers
  - configure, 8-106
- edit admin account, 8-213, 8-214
- Email Encryption, 1-7
  - about, 8-182
  - configuration overview, 8-182
  - default email identity, 8-186
  - default sender address, 8-186
  - delete domains, 8-184
  - domain key files, 8-184
  - domain ownership verification, 8-184
  - import domains, 8-184
  - registering domains, 8-184
- email message tracking, 7-1, 7-2
  - query, 7-2
- Email reputation, 8-52
- Email Reputation Services (ERS), 8-56
- email scanning, 8-10
  - archive file passwords, 8-34, 8-35
  - file passwords, 8-34
- email subjects, 4-19
- email submission
  - log query, 7-14
- email submission logs, 7-14
- email submissions, 8-29
  - important notes, 8-29
  - message details, 8-30
  - message format, 8-29
  - submit samples, 8-30
- end-user quarantine, 8-1
- End-User Quarantine
  - Accessing EUQ console, 8-89
  - approved senders, 8-92
  - EUQ digest, 8-86
  - inline actions, 8-86
  - notifications, 8-86
- End-User Quarantine (EUQ), 1-10, 8-82, 8-224
- enter CLI, A-1
- EUQ, 1-10, 8-82
- EUQ console, 8-88
  - AD group quarantined messages, 8-92

- quarantine messages, 8-90
- EUQ digest, 8-86
- exceptions
  - graymail, 5-89
- exfiltrate, 1-11
- export alerts, 6-6
- export debug file, 8-226
- export debugging files, 8-217
- exporting detections, 4-6
- export settings, 8-217–8-219
- expressions, 5-62, 5-63
  - customized, 5-64
    - criteria, 5-65, 5-66
  - export, 5-68
  - importing, 5-67
  - predefined, 5-63
- external integration, 8-28
- external redirect pages, 5-59

## **F**

- features, 1-5
- file attributes, 5-62, 5-68, 5-70, 5-71
  - configure, 5-69
  - creating, 5-70
  - export, 5-71
  - importing, 5-71
  - predefined, 5-69
  - wildcards, 5-70
- file passwords, 8-34
- firmware update, 8-8

## **G**

- getting started, 2-1
  - management console, 2-7
  - management console access, 2-5
  - summary, 2-2

- graymail, 1-8
  - exceptions, 5-89
- graymail scanning, 1-8

## **H**

- high-profile users, 8-48

## **I**

- identity provider, 8-170
  - configure, 8-170
  - federation metadata file, 8-170
- images, 8-12, 8-14, 8-16, 8-17
- important alerts, 6-2, 6-3, 6-5, 6-10
- import settings, 8-217, 8-218, 8-223
- informational alerts, 6-2, 6-24
- instances, 8-12
- IntelliTrap Exception Pattern, 8-3, H-4
- IntelliTrap Pattern, 8-3, H-4
- internal domains, 8-49
  - import, 8-108
- internal postfix, 8-194
- IPv6 support, E-1

## **K**

- keyword list
  - customized, 5-73, 5-74
- keyword lists, 5-72
  - customized, 5-75
  - export, 5-75
- keywords, 5-62, 5-72, 5-75
  - customized, 5-72
  - predefined, 5-72

## **L**

- LDAP, 8-165
  - configure, 8-166

- license expiration alert, 6-2
- local user accounts, 8-212
- logical operators, 5-77
- log level, 8-227
- logs, 7-1, 7-2, 7-7-7-9, 7-14, 7-15
  - audit, F-1
  - email message tracking, 7-2
  - email submission, 7-14
  - email submissions, 7-14
  - filters, 7-2
  - message queues, 7-10
  - MTA events, 7-7
  - system, 7-8
  - system events, 7-9, F-1
  - Time-of-Click protection, 7-15
    - log query, 7-15
- log settings, 8-178
  - syslog server, 8-179
- look-alike domains, 8-50
- Lotus Domino, 8-165

## M

- mail settings, 8-94
- maintenance agreement, 8-228
- Maintenance Agreement
  - about, 8-229
  - expiration, 8-229
  - renewal, 8-229
- malicious URLs, 4-5
- malware, 4-5
- management console, 2-5, 2-7
  - navigation, 2-9
  - session timeout, 8-202
- management network, 8-20
- management port, 8-187
- managing

- accounts, 8-210
- message delivery, 8-94, 8-99, 8-100
- message delivery alert, 6-3
- message delivery domains, 8-94
- message delivery settings, 8-98, 8-100
- Message Delivery settings
  - configure, 8-99, 8-100
- message details, 4-33
- message queue logs, 7-10
  - query, 7-11
- message queues
  - delete messages, 7-11
  - deliver messages, 7-11
  - reroute messages, 7-11, 7-13
- message scanning order, 5-5
- message stamps, 5-56
- message tokens, 6-2
- Microsoft Active Directory, 8-165, 8-212.  
*See also* Active Directory
- Microsoft AD Global Catalog, 8-165
- modify image, 8-17
- MTA events, 7-1, 7-7
- MTA server, 8-105
- MTA servers, 8-106

## N

- Network Content Correlation Pattern, 8-3
- Network Content Inspection Pattern, 8-3
- network interface status, 8-189
- network settings, 8-1, 8-187
- NIC teaming, 8-189
- notification parameters, 6-7
- notifications, 5-54
  - End-User Quarantine, 8-86

notification SMTP server, 8-187

## O

OAuth 2.0, 8-170

Okta, 8-170

on-demand reports, 6-27, 6-29

OpenLDAP, 8-165

operation mode

- BCC mode, 8-190

- MTA mode, 8-190

- SPAN/TAP mode, 8-190

operator accounts

- role, 8-210

## P

password, 8-215

password derivation, 1-5

patches, 8-7

PCRE, 5-64

Perle Compatible Regular

Expressions, 5-64

permitted recipient domains, 8-102

- export, 8-102

- import, 8-102

permitted senders, 8-103

phishing, 1-11

polices

- copy, 5-30

- delete, 5-30

- export, 5-30

- import, 5-30

- policy rules, 5-36

policies, 1-6, 5-2, 5-30

- add, 5-30, 5-31

- edit, 5-31

- management guidelines, 5-6

- policy objects, 5-53

policy, 1-5, 5-1, 5-55, 5-56, 5-59

- actions, 5-55–5-57, 5-59

- configuration, 5-59

- exceptions, 5-4, 5-83–5-85, 5-87, 5-88

  - import, 5-88

- graymail exceptions, 5-90

  - import, 5-90

policy actions, 5-55–5-57, 5-59

policy list, 5-30

- add, 5-30

- copy, 5-30

- delete, 5-30

- export, 5-30

- import, 5-30

- search filters, 5-30

policy management, 1-6

policy matching, 5-25

policy object

- notifications, 5-54

policy objects, 5-53

- expressions, 5-67, 5-68

- file attributes, 5-71

- keyword lists, 5-75

policy rule

- antispam rule, 5-45, 5-46

- DLP rule, 5-44

- threat protection rule, 5-50

policy rules, 5-36

policy splintering, 5-28

ports, C-4

predefined expressions, 5-63

- viewing, 5-63

predefined templates, 5-77

processing surge alert, 6-5

product components, 8-228

Product Connector, 8-124  
 product license, 8-1, 8-228  
     Advanced Threat Protection, 8-228  
     components, 8-228  
     Gateway Module, 8-228  
     view, 8-231  
 product updates, 8-1  
 product upgrade, 8-6–8-8  
 proxy settings, 8-187, 8-193

## Q

quarantine, 4-26  
     investigate, 4-31  
     message details, 4-33  
     search filters, 4-28  
     view, 4-26  
 query logs, 7-2, 7-9, 7-14, 7-15

## R

RAT, 1-11  
 recipient notifications, 5-54  
 redirect pages, 5-59  
 reject messages, 8-101  
 relay control, 8-101  
 replacement file, 5-55, 5-56  
 report formats, 6-27  
 reports, 6-1, 6-27–6-29  
     contacts for receiving, 8-209  
     on demand, 6-29  
     scheduled, 6-28  
 restore, 8-217–8-219, 8-223  
 risk level, 4-2  
 risk levels, 4-2, 4-4  
 rollback, 8-5

## S

safe domains, 5-85, 5-87, 5-88

safe files, 5-85, 5-87, 5-88  
 safe IP addresses, 5-85, 5-87, 5-88  
 safe recipients, 5-4, 5-83, 5-84  
 safe senders, 5-4, 5-83, 5-84  
 safe URLs, 5-85, 5-87, 5-88  
 SAML authentication, 8-168  
     Configuration overview, 8-168  
     Supported identity providers, 8-168  
 SAML integration  
     configuring identify provider settings, 8-170  
 sandbox error alert, 6-2  
 sandbox images, 8-12  
 sandbox queue alert, 6-3  
 scanning, 8-9  
 scanning and analysis, 8-1  
 scheduled reports, 6-28  
 schedule reports, 6-27  
 schedule updates, 8-6  
 Script Analyzer Pattern, 8-3, H-6  
 search, 7-2  
 search filters, 4-28  
 Security Assertion Markup Language (SAML), 8-168  
 sender authentication, 8-52  
     detections, 4-34  
     error codes, G-1  
 sender filtering, 8-1, 8-52, 8-56  
     detections, 4-34  
 Sender Policy Framework (SPF), 8-71  
     enable, 8-72  
     settings, 8-72  
 Service Gateway, 8-124  
 service provider, 8-169  
     certificate, 8-169

- metadata file, 8-169
  - service stopped alert, 6-2
  - session timeout, 8-202
  - SFTP upload, 8-181
  - shell environment, A-3
  - smart protection, 1-14
    - Web Reputation Services, 1-14
  - SMTP connections, 8-95
  - SMTP error codes, 8-56
  - SMTP greeting, 8-101, 8-105
  - SMTP routing, 8-94, 8-98, 8-100
  - SMTP server, 8-194
  - SMTP traffic throttling, 8-53
  - spam scanning, 1-7
  - spear-phishing, 1-11
  - SPF, 8-71
    - error code classification, G-1
    - error codes, G-1
  - Spyware/Grayware Pattern, 8-3
  - Spyware Pattern, H-7
  - SSL, 8-209
  - stamps, 5-57
  - storage management, 8-224
  - support
    - resolve issues faster, 9-3
  - supported archive file types, 8-21
  - supported file types, 8-21
  - suspicious files, 4-5, 4-23
  - suspicious hosts, 4-21
  - suspicious messages, 4-7
    - affected recipients, 4-15
    - attack sources, 4-16
    - email subjects, 4-19
    - exporting detections, 4-6
    - message details, 4-13
    - quarantine, 4-26, 4-28, 4-31, 4-33
    - search filters, 4-9
    - suspicious objects, 4-21–4-23
    - suspicious senders, 4-18
    - synchronized suspicious objects, 4-24
    - viewing, 4-7
  - suspicious objects, 4-21
    - files, 4-23
    - hosts, 4-21
    - synchronized suspicious objects, 4-24
    - URLs, 4-22
  - suspicious senders, 4-18
  - suspicious URLs, 4-5, 4-22
  - synchronized suspicious objects, 4-24
  - syslog, 8-178
  - syslog server, 8-179
  - system and accounts, 8-1
  - system event logs, F-1
  - system events, 7-1, 7-8
    - query, 7-9
  - system maintenance
    - power off, 8-226
    - restart, 8-226
  - system updates, 8-6
- ## T
- tabs, 3-2
    - overview, 3-2
    - system status, 3-2
    - threat monitoring, 3-2
    - top trends, 3-2
    - Virtual Analyzer, 3-2
  - targeted malware, 1-11, 4-5
  - templates, 5-76–5-78, 5-80
    - condition statements, 5-77

- customized, 5-77, 5-78, 5-80
  - logical operators, 5-77
  - predefined, 5-77
- Threat Knowledge Base, H-7
- threat protection rule, 5-50
- threat types, 4-5
- time-based filters, 7-1, 7-2, 8-1
- Time-of-Click protection, 7-15, 8-46
  - configuration, 8-46
  - log query, 7-15
  - redirect pages, 8-46
- TLS, 8-97, 8-209
  - about, 8-112
  - cipher grades, 8-116, 8-122
  - configuration, 8-113
  - deploy, 8-112
  - incoming messages, 8-114
  - outgoing messages, 8-116
  - prerequisites, 8-113
  - security levels, 8-115, 8-121
- TMASE, 8-2
- transport layer, 8-97
- transport layer security, 8-97
- Transport Layer Security (TLS), 8-209
- Trend Micro TippingPoint Security Management System (SMS)
  - about, 8-139
  - tag categories, 8-141
- Trend Vision One, 1-15
  - integration, 8-125
  - Product Connector, 8-124
  - Service Gateway, 8-124
  - unregister, 8-127
- triggered alerts, 6-2, 6-6

## U

- unreachable relay MTA alert, 6-2

- update completed surge, 6-5
- update failed alert, 6-3
- updates, 8-5
  - components, 8-2
  - source, 8-4
- update source, 8-4
- URL scanning, 8-31
  - disable, 8-32
- User Principle Name (UPN), 8-212
- using CLI, A-1

## V

- viewer accounts, 8-211
- Virtual Analyzer, 8-9, 8-10, 8-34, 8-35
  - archive file passwords, 8-34, 8-35
  - archive file types, 8-21
  - exceptions, 8-17
  - external integration, 8-28
  - file submission filtering, 8-17
  - file types, 8-17, 8-20, 8-21
  - images, 8-12, 8-14, 8-16, 8-17
  - instances, 8-12
  - network settings, 8-17
  - network types, 8-20
  - overall status, 8-12
  - overview screen, 8-11
  - risk levels, 4-4
  - statuses, 8-12
  - URL submission filtering, 8-17
- Virtual Analyzer Configuration Pattern, 8-4
- Virtual Analyzer Sensors, 8-3, H-7
- VSAPI, 8-3

## W

- warning page, 5-59

- watchlist alert, 6-3
  - web reputation, 1-14
  - Web Reputation Services, 8-10
  - Widget Framework, H-8
  - widgets, 3-4-3-17
    - add, 3-4
    - analysis
      - top attachment names, 3-12
      - top attachment types, 3-12
      - top callback hosts from Virtual Analyzer, 3-14
      - top callback URLs from Virtual Analyzer, 3-14
      - top email subjects, 3-15
    - detection summary, 3-7
    - overview
      - detection summary, 3-7
      - message queue, 3-8
      - processed messages, 3-8
      - quarantined messages, 3-8
      - top policy violations, 3-8
    - quarantined messages, 3-8
    - sandbox performance, 3-16
      - average sandbox processing time, 3-17
      - messages submitted to Virtual Analyzer, 3-16
      - suspicious objects from sandbox, 3-17
    - Sender filtering/authentication, 3-7
    - system performance
      - hardware status, 3-16
      - processing volume, 3-15
    - system status, 3-15
    - tasks, 3-5, 3-6
    - threat monitoring, 3-9
      - advanced threat indicators, 3-11
      - attack sources, 3-9
      - detected messages, 3-10
      - high-risk messages, 3-10
      - top affected recipients, 3-12
      - top attack sources, 3-13
    - Time-of-Click protection, 3-11
    - top trends, 3-12
  - wildcards, 5-70
    - file attributes, 5-70
  - wrs, 8-10
- X**
- X-header, 5-4, 5-83, 5-84
- Y**
- YARA rule file
    - add, 8-44
    - create, 8-42
    - delete, 8-45
    - edit, 8-45
    - export, 8-46
    - requirements, 8-43
  - YARA rules, 8-42



**TREND MICRO INCORPORATED**

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

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: APEM59194/210115