1.1 TREND MICRO™
Deep Discovery™ Director
Administrator’s Guide
Breakthrough Protection Against APTs and Targeted Attacks
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

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

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

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
Table of Contents

Preface

Preface ........................................................................................................................................ v
Documentation ....................................................................................................................... vi
Document Conventions ........................................................................................................ vi
About Trend Micro ............................................................................................................... vii

Chapter 1: Introduction

About Deep Discovery Director ............................................................................................. 1-2
What’s New .............................................................................................................................. 1-2
Features and Benefits ........................................................................................................... 1-3

Chapter 2: Deployment and Installation

System Requirements ............................................................................................................. 2-2
Deployment Types ................................................................................................................ 2-3
Installing Deep Discovery Director ...................................................................................... 2-5
Configuring Network Addresses on the Preconfiguration Console ................................... 2-7
Logging on to the Management Console ............................................................................ 2-8

Chapter 3: Directory

Directory Tasks ....................................................................................................................... 3-3
Other Directory Tasks ........................................................................................................... 3-5

Chapter 4: Appliance Updates

Plans ........................................................................................................................................ 4-2
Plan Tasks ............................................................................................................................... 4-3
Appliance Statuses ............................................................................................................... 4-4
Other Plan Tasks .................................................................................................................... 4-5
Chapter 5: Administration

Updates ............................................................................................................. 5-2
  Hotfixes / Patches ................................................................................ 5-2
  Firmware ............................................................................................... 5-4
Alerts ................................................................................................................ 5-5
  Editing Alerts ...................................................................................... 5-6
Microsoft Active Directory Integration ...................................................... 5-7
  Configuring Microsoft Active Directory Integration ....................... 5-8
System Settings ........................................................................................... 5-9
  Network ............................................................................................... 5-9
  Proxy .................................................................................................. 5-12
  SMTP ................................................................................................... 5-13
  Bandwidth ............................................................................................ 5-14
  Time .................................................................................................... 5-15
  Certificate ............................................................................................ 5-16
  Session Timeout .................................................................................. 5-17
Accounts ........................................................................................................ 5-17
  Adding a Local User Account ............................................................ 5-18
  Adding an Active Directory User Account or Group .................... 5-19
  Other Accounts Tasks ......................................................................... 5-20
System Logs ................................................................................................... 5-22
  Querying System Logs ....................................................................... 5-24
System Maintenance ..................................................................................... 5-26
  System Status ...................................................................................... 5-26
  Storage ................................................................................................. 5-27
Table of Contents

Back Up ........................................................................................................ 5-27
Restore ......................................................................................................... 5-30
Power Off / Restart .................................................................................... 5-34
License ............................................................................................................. 5-35

Chapter 6: Technical Support

Troubleshooting Resources ......................................................................... 6-2
Using the Support Portal ............................................................................. 6-2
Threat Encyclopedia .................................................................................... 6-2

Contacting Trend Micro ............................................................................. 6-3
Speeding Up the Support Call ................................................................... 6-4

Sending Suspicious Content to Trend Micro ............................................ 6-4
Email Reputation Services ......................................................................... 6-4
File Reputation Services ............................................................................ 6-5
Web Reputation Services ............................................................................ 6-5

Other Resources .......................................................................................... 6-5
Download Center ........................................................................................ 6-5
Documentation Feedback ........................................................................... 6-6

Index

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

Welcome to the Trend Micro Deep Discovery Director Administrator's Guide. This guide contains information about product settings.
Documentation

The documentation set for Deep Discovery Director includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator's Guide</td>
<td>The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Director, and explanations on Deep Discovery Director concepts and features.</td>
</tr>
<tr>
<td>Readme</td>
<td>The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Web-based documentation that is accessible from the Deep Discovery Director management console. The Online Help contains explanations of Deep Discovery Director components and features, as well as procedures needed to configure Deep Discovery Director.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>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: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

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


Document Conventions

The documentation uses the following conventions:
### TABLE 2. Document Conventions

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

### About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.
As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

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

Introduction

This chapter introduces Trend Micro™ Deep Discovery™ Director 1.1 and the new features in this release.
About Deep Discovery Director

Trend Micro Deep Discovery Director 1.1 is an on-premises management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to Deep Discovery products, as well as configuration replication of Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, and Deep Discovery Inspector.

What's New

<table>
<thead>
<tr>
<th>Feature/Enhancement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Analyzer image Deployment</td>
<td>Deep Discovery Director now enables the centralized deployment of Virtual Analyzer images to Deep Discovery products. To facilitate this, the Directory, Plans, and Repository screens now display additional Virtual Analyzer images related information.</td>
</tr>
<tr>
<td>Configuration replication</td>
<td>Deep Discovery Director now enables the centralized replication of configuration settings of Deep Discovery products. To facilitate this, the Directory, Plans, and Repository screens now display additional configuration replication related information.</td>
</tr>
<tr>
<td>Custom views</td>
<td>The Directory screen now enables creating and saving of custom views. There are three preset custom views specifically tailored to the needs of each plan type, which can be further customized to your liking.</td>
</tr>
<tr>
<td>Bandwidth usage throttling</td>
<td>New bandwidth usage throttling settings help manage the impact downloading and uploading of files may have on your network and internet connection.</td>
</tr>
</tbody>
</table>
### Feature/Enhancement | Details
---|---
Enhanced plan schedule settings | In addition to the server deployment start and appliance execution start times, the plan schedule settings now enable the Appliance Download Period—the time period during which appliances are allowed to download the files required to execute the plan—and the Appliance Execution Start—the date and time when the appliances start executing the plan—to be set independently from each other.

Enhanced file upload options | To facilitate the uploading of large Virtual Analyzer image files, Deep Discovery Director now enables up to three Virtual Analyzer image files to be uploaded via SFTP or network share folder at the same time.

Enhanced system logs | The System Logs screen now enables logs to be directly readable, searchable, and filterable on the management console.

System alerts | Deep Discovery Director monitors a variety of events and can be configured to generate alerts to inform users of those events. Alerts can be configured to be sent through email.

System status | The new System Status screen displays the utilization of key hardware components.

Product activation | As a management solution to other Deep Discovery products, Deep Discovery Director can be activated with the Activation Code of any Deep Discovery product.

Back up and restore | Use the Back Up screen to export a backup file of the Deep Discovery Director configuration settings and database, and the Restore screen to restore or revert configuration settings and database to the point of backup.

Firmware upgrades | In addition to hotfixes and patches, the new Firmware screen now enables Deep Discovery Director to install firmware upgrades.

---

**Features and Benefits**

Deep Discovery Director includes the following features:
<table>
<thead>
<tr>
<th>Feature/Benefit</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>The Directory displays information about Deep Discovery appliances and repository servers that are registered to Deep Discovery Director.</td>
</tr>
<tr>
<td>Plans</td>
<td>Plans define the scope and schedule of deployments to target appliances.</td>
</tr>
<tr>
<td>Repository</td>
<td>The Repository screen displays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here.</td>
</tr>
<tr>
<td>Updates</td>
<td>The Updates screen enables you to install hotfixes, patches and firmware upgrades to Deep Discovery Director. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.</td>
</tr>
<tr>
<td>Microsoft Active Directory Integration</td>
<td>Deep Discovery Director allows Active Directory accounts to access the management console.</td>
</tr>
<tr>
<td>System Logs</td>
<td>Deep Discovery Director maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.</td>
</tr>
</tbody>
</table>
Chapter 2

Deployment and Installation

This chapter contains information about the requirements and procedures for deploying and installing Deep Discovery Director.
# System Requirements

## Table 2-1. System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>• CPU: 1.8GHz (at least 2 cores)</td>
<td></td>
</tr>
<tr>
<td>• Memory:</td>
<td></td>
</tr>
<tr>
<td>• Distributed mode:</td>
<td></td>
</tr>
<tr>
<td>• Management server: 8GB</td>
<td></td>
</tr>
<tr>
<td>• Central Repository server: 8GB</td>
<td></td>
</tr>
<tr>
<td>• Local Repository server: 8GB</td>
<td></td>
</tr>
<tr>
<td>• Consolidated mode: 8GB</td>
<td></td>
</tr>
<tr>
<td>• Network interface card: 1 with E1000 or VMXNET 3 adapter</td>
<td></td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td></td>
</tr>
<tr>
<td>• Deep Discovery Director does not support the VMXNET 2 (Enhanced) adapter type.</td>
<td></td>
</tr>
<tr>
<td>• For port binding, specify the same adapter type to use for all network interface cards.</td>
<td></td>
</tr>
<tr>
<td>• SCSI Controller: LSI Logic Parallel</td>
<td></td>
</tr>
<tr>
<td>• Hard disk:</td>
<td></td>
</tr>
<tr>
<td>• Distributed mode:</td>
<td></td>
</tr>
<tr>
<td>• Management server: 120GB (thin provisioned)</td>
<td></td>
</tr>
<tr>
<td>• Central Repository server: 120GB (thin provisioned)</td>
<td></td>
</tr>
<tr>
<td>• Local Repository server: 120GB (thin provisioned)</td>
<td></td>
</tr>
<tr>
<td>• Consolidated mode: 120GB (thin provisioned)</td>
<td></td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td>• Hypervisor: VMware vSphere ESXi 5.5/6.0/6.5</td>
<td></td>
</tr>
<tr>
<td>• Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>
**Deployment and Installation**

**Requirement**

<table>
<thead>
<tr>
<th>Minimum Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ports</strong></td>
</tr>
<tr>
<td>• TCP 443 (Deep Discovery Director Server connection)</td>
</tr>
<tr>
<td>• UDP 123 (default NTP server connection)</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
</tr>
<tr>
<td>• Self-signed</td>
</tr>
<tr>
<td>• PEM format</td>
</tr>
<tr>
<td>• Certificate and private key in the same file</td>
</tr>
<tr>
<td>• No certificate chain</td>
</tr>
<tr>
<td><strong>Encryption methods:</strong></td>
</tr>
<tr>
<td>• Private key: RSA algorithm only</td>
</tr>
<tr>
<td>• Certificate: Digest size of 256 (SHA-256) or higher</td>
</tr>
</tbody>
</table>

**Generation command example (CentOS):**

```bash
# openssl genpkey -algorithm RSA -out key.pem -pkeyopt rsa_keygen_bits:2048
# openssl req -new -key key.pem -out csr.pem
# openssl req -x509 -sha256 -days 365 -key key.pem -in csr.pem -out certificate.pem
# cat key.pem >> certificate.pem
```

**Deployment Types**

Deep Discovery Director consists of three components that enable centralized deployment of product updates and upgrades: Deep Discovery Director server, Central Repository server, and Local Repository server. You have the option to either install each component on a dedicated server or install all components on a single server depending on the requirements of your network and organization. Regardless of deployment type, Deep Discovery Director provides certificate-based connections to registered Deep Discovery appliances and integration with Microsoft Active Directory server.

- **Distributed mode:** For large environments, Trend Micro recommends installing the individual components onto dedicated servers for load balancing and scalability. Each server is provided a management console that enables functionalities associated with the installed component.
### Table 2-2. Components

<table>
<thead>
<tr>
<th>Server</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server</td>
<td>• Hosts the main management console that you can use to:</td>
</tr>
<tr>
<td></td>
<td>• Create plans</td>
</tr>
<tr>
<td></td>
<td>• View appliance, plan, and repository information</td>
</tr>
<tr>
<td></td>
<td>• Manage user accounts</td>
</tr>
<tr>
<td></td>
<td>• Configure system and update settings</td>
</tr>
<tr>
<td></td>
<td>• Displays the list of update, upgrade, and Virtual Analyzer image files available on the Central Repository server</td>
</tr>
<tr>
<td></td>
<td>• Receives registration information and status reports from appliances</td>
</tr>
<tr>
<td></td>
<td>• Sends plan information to appliances</td>
</tr>
<tr>
<td>Central Repository</td>
<td>• Enables you to configure system settings through a limited version of the management console</td>
</tr>
<tr>
<td></td>
<td>• Sends a list of available update, upgrade, and Virtual Analyzer image files to the Deep Discovery Director Management Server</td>
</tr>
<tr>
<td></td>
<td>• Sends update, upgrade, and Virtual Analyzer image files to Local Repository servers</td>
</tr>
<tr>
<td>Local Repository</td>
<td>• Enables you to configure system settings through a limited version of the management console</td>
</tr>
<tr>
<td></td>
<td>• Downloads update, upgrade, and Virtual Analyzer image files from the Central Repository server</td>
</tr>
<tr>
<td></td>
<td>• Sends update, upgrade, and Virtual Analyzer image files to appliances</td>
</tr>
</tbody>
</table>

- **Consolidated mode**: For small and medium businesses, Trend Micro recommends installing all three components on a single server for straightforward management and maintenance. You can access all management console functions, including creating plans and uploading files to the repository.
Installing Deep Discovery Director

Procedure

1. Create a custom virtual machine with the following minimum specifications:
   - Virtual machine hardware version: 8
   - Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)
   - CPU: 1 virtual socket with 2 cores
   - Memory: 8GB
   - Network interface card: 1 with E1000 or VMXNET 3 adapter

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

   - SCSI Controller: LSI Logic Parallel
   - Hard disk: 120GB (thin provisioned)
Important

- Setting the hard disk size to 120GB allows three Virtual Analyzer images between 4GB to 10GB to be uploaded to the repository. If you plan on uploading and deploying multiple larger Virtual Analyzer images (10GB to 20GB), set the hard disk size accordingly.

- Trend Micro recommends setting the Local Repository server hard disk size to the same as the Central Repository server hard disk size. Local Repository servers download all update, upgrade, and Virtual Analyzer image files from the Central Repository server. Setting the Local Repository server hard disk size lower than the Central Repository server hard disk size may cause Local Repository servers to be unable to download and send files required to execute plans to managed appliances.

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

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

   The Deep Discovery Director Installation screen appears.

4. Select Install software.

   The Deep Discovery Director Components screen appears.

5. Select one of the following based on your preferred deployment mode:

   - **Consolidated mode**: Install all components
   - **Distributed mode**: Install Management Server, Install Central Repository, and Install Central Repository

   To install all three components, this installation procedure must be completed three times.

   The License Agreement screen appears.

6. Click Accept.

   The Disk Selection screen appears.
7. Click **Continue**.
   The **Hardware Profile** screen appears.

8. Click **Continue**.
   The **Repartition Disks** confirmation message appears.

9. Click **Continue**.
   The installation starts.

---

### Configuring Network Addresses on the Preconfiguration Console

**Procedure**

1. Open the Deep Discovery Director virtual machine console.

2. Log on to the preconfiguration console using the following default credentials:
   - User name: admin
   - Password: admin
   The **Main Menu** screen appears.

3. Select **Configure network settings** and then press **ENTER**.
   The **Configure Network Settings** screen appears.

4. Configure the following required settings:
   - IPv4 address
   - Subnet mask
   - IPv4 gateway
   - DNS server 1
Note

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

For details, see Network on page 5-9.

5. Press TAB to navigate to Save, and then press ENTER.

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

Logging on to the Management Console

Procedure

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

The management console logon screen appears.

2. Type the following default credentials:
   - User name: admin
   - Password: admin

3. Click Log on.

The Directory screen appears.
Chapter 3

Directory

The Directory displays information about Deep Discovery appliances and repository servers that are registered to Deep Discovery Director.

- Left pane: Appliance tree with groups (represented by folders) and appliances (identified by display names, initially identical to their host names)

  Note

  An exclamation mark icon attached to the appliance or repository server icon indicates that the connection with this appliance or repository server has been lost.

- Right pane: Information about plans, appliances, installed or hosted update files, etc.

On fresh installations, the Directory is empty and only displays the following default groups:

- **Managed**: Appliances placed in this group can receive plan information from the Deep Discovery Director server and updates and Virtual Analyzer images from designated repository servers. Appliances can also replicate their configuration to and from other compatible appliances.

- **Unmanaged**: Appliances placed in this group cannot receive plan information, updates, Virtual Analyzer images, or replicate their configuration.
Appliances can register to Deep Discovery Director on their respective management consoles. Newly registered appliances first appear in the Unmanaged group but can be moved to the Managed group at any time.
Directory Tasks

You can use the Directory mainly to view information about groups and appliances, and plans that are associated with these objects. Selecting an object in the left pane displays information in the right pane.

The following table describes the three object types and the available information for each object.
### Table 3-1. Directory Object Types

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances</td>
<td>• <strong>Plan</strong>: Plans that were or will be deployed to the appliance</td>
</tr>
<tr>
<td></td>
<td>• <strong>Appliance</strong>: Identifiers such as IP address, virtual IP address, host name and display name, and other information such as the address of the Local Repository server that it downloads files from</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For Deep Discovery Analyzer clusters, Deep Discovery Director also displays the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active primary appliance</strong>: Information on the active primary appliance (high availability cluster and load balancing cluster)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Passive primary appliance</strong>: Information on the passive primary appliance (high availability cluster)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Secondary appliances</strong>: Information on the secondary appliance (load balancing cluster)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Updates</strong>: Build number and installation date of all installed updates, and information about where and when the appliance’s configuration settings were replicated from</td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Analyzer</strong>: Information about the Virtual Analyzer configuration of the appliance, such as source, internal Virtual Analyzer maximum images and instances, and deployed images and instances</td>
</tr>
</tbody>
</table>

**Note**

For Deep Discovery Analyzer active primary appliances, click on **All Nodes** to display the total number of instances in use for all nodes in the cluster.
### Local Repository servers

- **Plan**: Plans that were or will be deployed to the server
- **Server**: Identifiers such as IP address, host name and display name, and other information such as the address of the Central Repository server
- **Updates**: Build number and installation date of all installed updates
- **Repository**: Files that it hosts and IP address of the Central Repository server
- **Connected Appliances**: Appliances that are configured to download files from it

**Note**
You can assign a maximum of three repository servers per appliance.

### Groups

Overview of appliances and plans associated with that group, including statuses and connection information.

### Other Directory Tasks

You can also perform the following actions:

**Table 3-2. Other Directory Tasks**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add groups</td>
<td>Add groups to better organize appliances, such as by location or business unit.</td>
</tr>
<tr>
<td></td>
<td>To add a group:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the group name and then select <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the text box, type a name with a maximum of 256 characters.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit group or appliance names</td>
<td>To edit a group or appliance name:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the group or appliance name and then select <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the text box, type a name with a maximum of 256 characters.</td>
</tr>
<tr>
<td>Edit appliance repository server assignments</td>
<td>To edit the repository server assignments of an appliance:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the appliance name and then select <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Modify the repository server assignments using the drop-down lists.</td>
</tr>
<tr>
<td>Move groups or appliances</td>
<td>To move a group or an appliance to a different group:</td>
</tr>
<tr>
<td></td>
<td>1. Click the menu icon beside the group or appliance name and then select <strong>Move</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the window, select the new folder and then click <strong>Move</strong>.</td>
</tr>
<tr>
<td></td>
<td>This function is disabled whenever:</td>
</tr>
<tr>
<td></td>
<td>• Deployment of one or more associated plans is pending or in progress.</td>
</tr>
<tr>
<td></td>
<td>• The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to <strong>All</strong>.</td>
</tr>
</tbody>
</table>
### Directory

<table>
<thead>
<tr>
<th><strong>Action</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete groups</td>
<td>Delete empty or unused groups to simplify the Directory. To delete a group, click the menu icon beside the group name and then select Delete.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong> Deleting a group cancels the plans associated with that group, moves appliances to the <strong>Unmanaged</strong> group, and unregisters repository servers from Deep Discovery Director. Only groups without unfinished plans can be deleted.</td>
</tr>
<tr>
<td></td>
<td>This function is disabled whenever:</td>
</tr>
<tr>
<td></td>
<td>• Deployment of one or more associated plans is pending or in progress.</td>
</tr>
<tr>
<td></td>
<td>• The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to <strong>All</strong>.</td>
</tr>
<tr>
<td>Delete appliances</td>
<td>To delete an appliance, click the menu icon beside the display name and then select Delete.</td>
</tr>
<tr>
<td></td>
<td>This function is disabled whenever the appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to <strong>All</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong> Deleting an appliance unregisters it from Deep Discovery Director, stops all connections, and cancels all associated plans.</td>
</tr>
<tr>
<td>Switch views</td>
<td>To switch between custom views, click on the name beside <strong>Views</strong> and then select the view to switch to.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Customize columns    | Customize columns and save new custom views to better organize all the information.  
To create a custom view:  
1. Click on the name beside **Views** and then select **Customize columns**.  
2. Type a unique custom view name.  
3. Select any combination of columns to include in the custom view.  
4. Click **Save**.  

**Tip**  
The column order can be rearranged using drag-and-drop. |
| Edit custom views    | To edit a custom view:  
1. Click on the name beside **Views** and then select the **pencil** icon beside the view.  
2. (Optional) Edit the custom view name.  
3. Edit the combination of columns.  
4. Click **Save**. |
| Delete custom views  | To delete a custom view, click on the name beside **Views** and then select the **trash can** icon beside the view. |
Chapter 4

Appliance Updates

Learn how to perform plan related tasks, manage the repository, and configure Central Repository and Local Repository related connection settings.
Plans

Plans define the scope and schedule of deployments to target appliances.

Each plan is created for a specific set of target appliances and is deployed only once during a user-defined period. The files to be deployed must match the product and language of the target appliances.

When a plan is deployed, the Deep Discovery Director server sends instructions to the target appliances to download and install the specified files from a designated repository server. If the plan is not deployed immediately, appliances download and install files according to a schedule with the following factors:

- Plan deployment start and expiration (Deep Discovery Director server time)
- Appliance download period (appliance local time)
- Appliance execution start (appliance local time)

**Important**

Plans can expire. If no appliances execute the plan within the specified period, the plan is considered expired.

The Plans screen displays a list of all created plans with the following information:

**TABLE 4-1. Plans**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specified during plan creation</td>
</tr>
<tr>
<td>Type</td>
<td>Type of plan deployed to targets. Deep Discovery Director currently supports the following plan types:</td>
</tr>
<tr>
<td></td>
<td>- Hotfix / Critical patch / Firmware</td>
</tr>
<tr>
<td></td>
<td>- Virtual Analyzer images</td>
</tr>
<tr>
<td></td>
<td>- Configuration replication</td>
</tr>
</tbody>
</table>
A plan can have any of the following statuses.

- **In progress**: Deployment started at the specified time and at least one appliance has executed the plan.
- **Pending**: Deployment has not started or no appliances have received plan information from Deep Discovery Director.
- **Expired**: Deployment did not start at the specified time and no appliances received plan information from Deep Discovery Director.
- **Completed**: Deployment started at the specified time and all appliances successfully executed the plan.
- **Unsuccessful**: Deployment did not start at the specified time or at least one appliance was unable to execute the plan.

### Plan Tasks

Clicking a plan name opens the details screen for that specific plan.

**Table 4-2. Plan Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan information</td>
<td>Plan deployment status and schedule, file details, and other related information</td>
</tr>
</tbody>
</table>
Appliance Information

Appliance information
- Host name, appliance status, deployment start and completion, and appliance path
- For details, see Appliance Statuses on page 4-4.

### Appliance Statuses

Deep Discovery Director displays any of the following appliance statuses.

**Table 4-3. Appliance Statuses**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>The appliance has not received the plan information from Deep Discovery Director.</td>
</tr>
<tr>
<td>In progress</td>
<td>Any of the following situations may apply.</td>
</tr>
<tr>
<td></td>
<td>• The appliance has acknowledged receipt of the plan information and has started downloading files.</td>
</tr>
<tr>
<td></td>
<td>• The appliance has acknowledged receipt of the plan information and has started executing the plan.</td>
</tr>
<tr>
<td></td>
<td>• The appliance is downloading the files required to execute the plan.</td>
</tr>
<tr>
<td></td>
<td>• The appliance has downloaded the files and is executing the plan.</td>
</tr>
<tr>
<td>Suspended</td>
<td>The appliance has temporarily stopped downloading files and will resume on the specified download period.</td>
</tr>
<tr>
<td>Completed</td>
<td>The appliance executed the plan successfully.</td>
</tr>
</tbody>
</table>
### Status Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
</table>
| Unsuccessful | Any of the following situations may apply.  
|            | • The appliance was unable to execute the plan.  
|            | • The appliance is performing tasks that do not match the plan information.  
|            | • The appliance is connected to a Local Repository server that is unavailable or does not exist. |
| Expired    | The appliance did not receive the plan information during the specified execution period. |
| Unreachable | Any of the following situations may apply.  
|            | • The appliance has unregistered from Deep Discovery Director.  
|            | • The appliance has been deleted from Deep Discovery Director. |
| Cancelled  | Any of the following situations may apply:  
|            | • The plan was manually cancelled before the appliance received the plan information from Deep Discovery Director.  
|            | • The plan was manually cancelled while the appliance was downloading files or executing the plan.  
|            | • The plan was manually cancelled while the appliance temporarily stopped downloading files. |

### Other Plan Tasks

You can also perform the following tasks:
## TABLE 4-4. Other Tasks

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add one of the following types of plans to Deep Discovery Director.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hotfix / Critical Patch / Firmware</strong>: For details, see <em>Adding a Hotfix / Critical Patch / Firmware Deployment Plan</em> on page 4-7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Analyzer images</strong>: For details, see <em>Adding a Virtual Analyzer Images Deployment Plan</em> on page 4-8.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration replication</strong>: For details, see <em>Adding a Configuration Replication Plan</em> on page 4-11.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director does not allow the creation of new plans when the license status is <strong>Not Activated</strong> or <strong>Expired</strong>. Existing plans will deploy and execute as usual.</td>
</tr>
<tr>
<td></td>
<td>To activate Deep Discovery Director, see <em>License on page 5-35</em>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click a plan name with the status <strong>Pending</strong> and then click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Only plans that have not been deployed can be edited.</td>
</tr>
<tr>
<td>Cancel plan</td>
<td>Click a plan name with any of the following statuses and then click <strong>Cancel Plan</strong>:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>In progress</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suspended</strong></td>
</tr>
<tr>
<td>Copy</td>
<td>Select a plan in the list and click <strong>Copy</strong>.</td>
</tr>
<tr>
<td>Create plan</td>
<td>Click a plan with the status <strong>Unsuccessful</strong> and then click <strong>Create Plan</strong>.</td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director will create a new plan based on the settings of the unsuccessfully deployed plan.</td>
</tr>
</tbody>
</table>
Adding a Hotfix / Critical Patch / Firmware Deployment Plan

Use this type of plan to deploy product updates and upgrades to compatible appliances.

Procedure

1. Go to **Appliance Updates > Plans** and click on **Add**.
   
   The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select **Hotfix / Critical patch / Firmware** as type.

4. (Optional) Type a description.

5. Select a hotfix, critical patch, or firmware file from the list.

   **Note**
   
   Deep Discovery Director displays the list of files that are available on the repository server. Verify that the file matches the product and language of the target appliances.

6. Select target appliances. Deep Discovery Director only displays compatible appliances.

   **Note**
   
   Installing updates automatically restarts the target appliances.

7. Specify the schedule.

   - **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.

   - **Server deployment start** and **expiration**
• Appliance download period
  • All day
  • From HH:MM to HH:MM

• Appliance execution start
  • Immediately after downloading
  • By schedule
  • **Immediate**: Starts immediately after the plan is saved.

8. Click **Save**.

---

**Adding a Virtual Analyzer Images Deployment Plan**

Use this type of plan to deploy Virtual Analyzer images to compatible appliances.

The following table lists requirements that must be fulfilled by compatible appliances:

**TABLE 4-5. Requirements for Compatible Appliances**

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| License            | • **Status**: Activated  
                     | • **Type**: Full       |
| Virtual Analyzer   | • **Status**: Enabled   |

**Note**

Virtual Analyzer images can be deployed to Deep Discovery Inspector appliances whose Virtual Analyzer status is disabled. Deep Discovery Inspector automatically enables Virtual Analyzer after the images have been deployed.

• **Source**: Internal
<table>
<thead>
<tr>
<th><strong>REQUIREMENT</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Discovery Director</td>
<td>• Integration with Deep Discovery Director 1.1</td>
</tr>
<tr>
<td></td>
<td>• Must be registered to Deep Discovery Director</td>
</tr>
<tr>
<td></td>
<td>• Must in a Managed group</td>
</tr>
</tbody>
</table>

**Procedure**

1. Go to **Appliance Updates > Plans** and click on **Add**. The **Add Plan** screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select **Virtual Analyzer images** as type.

4. (Optional) Type a description.

5. Select a product from the list.

6. Select a maximum images value from the list.

7. Select a maximum instances value from the list.

8. Click **Images**.

   The **Virtual Analyzer Images** dialog appears.

   **Note**

   Deep Discovery Director displays the list of Virtual Analyzer images that are available on the repository server.

9. Select the final configuration of Virtual Analyzer images to deploy and click **Save**.
10. **Important**

- The selected configuration replaces any configuration currently deployed on target appliances.
- To keep currently deployed images on target appliances, select them as part of the final configuration. The target appliances will automatically determine if the selected images are identical and need to be deployed.

11. **(Optional) Modify the instances allocated to any image.**

12. **Select target appliances.** Deep Discovery Director only displays compatible appliances.

13. **Note**

Deep Discovery Analyzer secondary appliances are not displayed because Virtual Analyzer images and settings are automatically synced from the primary appliance. To deploy Virtual Analyzer images to Deep Discovery Analyzer secondary appliances, select the corresponding primary appliance.

14. **Specify the schedule.**

- **Custom:** Deploys the plan, downloads the files, and executes the plan as specified.
  - **Server deployment start** and **expiration**
  - **Appliance download period**
    - All day
    - From HH:MM to HH:MM
  - **Appliance execution start**
    - Immediately after downloading
    - By schedule
  - **Immediate:** Starts immediately after the plan is saved.

15. **Click Save.**
Adding a Configuration Replication Plan

Use this type of plan to replicate the configuration settings of one appliance to compatible appliances.

Each Deep Discovery product supports the replication of a different combination of configuration settings. For details, see the following:

- Deep Discovery Analyzer Replicated Configuration Settings on page 4-12
- Deep Discovery Email Inspector Replicated Configuration Settings on page 4-14
- Deep Discovery Inspector Replicated Configuration Settings on page 4-16

Procedure

1. Go to Appliance Updates > Plans and click on Add.
   
   The Add Plan screen appears.

2. Type a plan name with a maximum of 256 characters.

3. Select Configuration replication as type.

4. (Optional) Type a description.

5. Select the replication source from the list.

   Tip
   
   Select a product from the View drop-down list to only display the selected product's appliances.

6. Select target appliances. Deep Discovery Director only displays compatible appliances.

7. Specify the schedule.
   
   - Custom: Deploys the plan, downloads the files, and executes the plan as specified.
   
   - Server deployment start and expiration
• Appliance download period
  • All day
  • From HH:MM to HH:MM
• Appliance execution start
  • Immediately after downloading
  • By schedule
    • Immediate: Starts immediately after the plan is saved.

8. Click Save.

---

**Deep Discovery Analyzer Replicated Configuration Settings**

The following table shows the screens and elements with replicated configuration settings.

**TABLE 4-6. Deep Discovery Analyzer Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>All widgets and settings</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Submissions</td>
<td>Filter settings</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Suspicious Objects &gt; User-defined Match List</td>
<td>User-defined Match List</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Exceptions</td>
<td>Exceptions list</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Sandbox Management &gt; Archive Passwords</td>
<td>Passwords list</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Sandbox Management &gt; Submission Settings</td>
<td>File type filter settings</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Sandbox Management &gt; Smart Feedback</td>
<td>Smart Feedback settings</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Virtual Analyzer &gt; Sandbox Management &gt; Cloud Sandbox</td>
<td>Cloud Sandbox setting</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Alerts &gt; Rules</td>
<td>All alert notification rule settings</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports &gt; Schedules</td>
<td>All report schedules</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports &gt; Customization</td>
<td>Report customization settings</td>
</tr>
<tr>
<td>Administration &gt; Updates &gt; Component Update Settings</td>
<td>Component update settings</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/ Services &gt; Log Settings</td>
<td>Log settings</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/ Services &gt; Smart Protection</td>
<td>Smart Protection settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Proxy</td>
<td>Proxy settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; SMTP</td>
<td>SMTP settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Time</td>
<td>Time settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; SNMP</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Password Policy</td>
<td>Password policy setting</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Session Timeout</td>
<td>Session timeout values</td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts &gt; Accounts</td>
<td>All user accounts</td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts &gt; Contacts</td>
<td>All contacts</td>
</tr>
</tbody>
</table>
Deep Discovery Email Inspector Replicated Configuration Settings

The following table shows the screens and elements with replicated configuration settings.

**TABLE 4-7. Deep Discovery Email Inspector Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>All widgets and settings</td>
</tr>
<tr>
<td>Policy &gt; Policy &gt; Actions</td>
<td>Actions settings</td>
</tr>
<tr>
<td>Policy &gt; Policy &gt; Recipient Notification</td>
<td>Recipient notification subject and message</td>
</tr>
<tr>
<td>Policy &gt; Policy &gt; Message Tags</td>
<td>Attachment replacement file, End Stamp message</td>
</tr>
<tr>
<td>Policy &gt; Policy &gt; Redirect Pages</td>
<td>Blocking and Warning Pages settings</td>
</tr>
<tr>
<td>Policy &gt; Exceptions &gt; Messages</td>
<td>Specified senders, recipients, and X-headers</td>
</tr>
<tr>
<td>Policy &gt; Exceptions &gt; Objects</td>
<td>Excepted objects list</td>
</tr>
<tr>
<td>Policy &gt; Exceptions &gt; URL Keywords</td>
<td>Excepted URL keywords list</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Alerts &gt; Rules</td>
<td>All alert notification rule settings</td>
</tr>
<tr>
<td>Alerts / Reports &gt; Reports &gt; Schedules</td>
<td>All report schedules</td>
</tr>
<tr>
<td>Administration &gt; Component Updates &gt; Schedule</td>
<td>Schedule setting</td>
</tr>
<tr>
<td>Administration &gt; Component Updates &gt; Source</td>
<td>Source setting</td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Operation Mode</td>
<td>Operation mode settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Proxy</td>
<td>Proxy settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; SMTP</td>
<td>SMTP settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Time</td>
<td>Time settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; SNMP</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Administration &gt; Mail Settings &gt; Connections</td>
<td>Connections settings</td>
</tr>
<tr>
<td>Administration &gt; Mail Settings &gt; Message Delivery</td>
<td>All message delivery profiles</td>
</tr>
<tr>
<td>Administration &gt; Mail Settings &gt; Limits and Exceptions</td>
<td>Limits and exceptions settings</td>
</tr>
<tr>
<td>Administration &gt; Mail Settings &gt; SMTP Greeting</td>
<td>SMTP greeting message</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services &gt; Microsoft Active Directory</td>
<td>Microsoft Active Directory server settings</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services &gt; Log Settings</td>
<td>All syslog server settings</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services &gt; SFTP</td>
<td>SFTP settings</td>
</tr>
<tr>
<td>Administration &gt; Scanning / Analysis &gt; Settings</td>
<td>Virtual Analyzer settings</td>
</tr>
<tr>
<td>Administration &gt; Scanning / Analysis &gt; File Passwords</td>
<td>Passwords list</td>
</tr>
</tbody>
</table>
The following table shows the screens and elements with replicated configuration settings.

**TABLE 4-8. Deep Discovery Inspector Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections &gt; Affected Hosts</td>
<td>All detections and detailed drill down views</td>
</tr>
<tr>
<td>Detections &gt; All Detections</td>
<td>All detections</td>
</tr>
<tr>
<td>Reports &gt; Schedules</td>
<td>All report schedules</td>
</tr>
<tr>
<td>Reports &gt; Customization</td>
<td>Report customization settings</td>
</tr>
<tr>
<td>Administration &gt; Updates &gt; Component Updates &gt; Scheduled</td>
<td>Schedule setting</td>
</tr>
<tr>
<td>Administration &gt; Updates &gt; Component Updates &gt; Source</td>
<td>Source settings</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Threat Detections</td>
<td>Threat detections notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; High Risk Hosts Detections</td>
<td>High risk hosts detections notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Suspicious Hosts Detections</td>
<td>Suspicious hosts detections notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; High Network Traffic</td>
<td>High network traffic notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Unanalyzed Sample Detections</td>
<td>Unanalyzed sample detections notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Virtual Analyzer Detections</td>
<td>Virtual Analyzer detections notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Deny List</td>
<td>Deny list notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Retro Scan Detections</td>
<td>Retro Scan notification settings</td>
</tr>
<tr>
<td>Administration &gt; Notifications &gt; Email Settings</td>
<td>Notifications email settings</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Hosts / Ports</td>
<td>Hosts / ports setting</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Threat Detections</td>
<td>Threat detections settings</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Web Reputation</td>
<td>Web Reputation settings</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Application Filters</td>
<td>Application filter settings</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Deny List / Allow List</td>
<td>Deny list</td>
</tr>
<tr>
<td></td>
<td>Allow list</td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Detection Rules</td>
<td>Detection rule settings</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning &gt; Exceptions</td>
<td>Exceptions list</td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer &gt; File Submissions</td>
<td>File submission settings</td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer &gt; Internal Virtual Analyzer &gt; Passwords</td>
<td>Passwords list</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets &gt; Network Groups</td>
<td>Monitored networks list</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets &gt; Registered Domains</td>
<td>Registered domains list</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets &gt; Registered Services</td>
<td>Registered services list</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services &gt; Syslog</td>
<td>All syslog server settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Proxy</td>
<td>Proxy settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; SNMP</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; HTTPS Certificate</td>
<td>Certificate</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Time</td>
<td>Time settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Session Timeout</td>
<td>Session timeout value</td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts &gt; Accounts</td>
<td>All user accounts</td>
</tr>
</tbody>
</table>
Repository

The Repository screen displays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here.

- **Uploading a Hotfix / Critical Patch / Firmware File** on page 4-19
- **Uploading Virtual Analyzer Images** on page 4-20
- **Upload Center** on page 4-21

**Hotfix / Critical Patch / Firmware**

Use the Hotfix / Critical Patch / Firmware screen, in Appliance Updates > Repository > Hotfix / Critical Patch / Firmware, to view already uploaded update files, delete unused update files, and upload new update files for deployment.

Use filters to search by update or upgrade type, product, language, and file name or version.

To delete a file, select the file from the list and then click **Delete**.

**Uploading a Hotfix / Critical Patch / Firmware File**

Deep Discovery Director supports simultaneous uploading of up to five files through single-file upload sessions.

---

**Important**

Closing the browser or tab that contains the management console cancels all uploads in progress.
Procedure

1. Go to Appliance Updates > Repository > Hotfix / Critical Patch / Firmware.
2. Click Upload.
3. Click Select and then select a valid TAR file.
4. (Optional) Type or paste the 64-character SHA-256 hash value of the selected file for verification.
5. (Optional) Type a description.
6. Click Upload.

Virtual Analyzer Images

Use the Virtual Analyzer Images screen, in Appliance Updates > Repository > Virtual Analyzer Images, to view already uploaded image files, delete unused image files, and upload new image files for deployment.

To delete a file, select the file from the list and then click Delete.

Important

Only Virtual Analyzer images compressed in TAR format by the Virtual Analyzer Image Preparation Tool can be uploaded to and deployed from Deep Discovery Director. For details, see http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Uploading Virtual Analyzer Images

Deep Discovery Director supports consecutive uploading of up to three Virtual Analyzer image files through SFTP or network folder. Deep Discovery Director opens a connection to the SFTP or network server in the background for the upload session, allowing you to navigate away from the screen and perform other tasks while waiting for the upload to complete.
Procedure

1. Go to Appliance Updates > Repository > Virtual Analyzer Images.

2. Click Upload.

3. Select a source from the list.
   - SFTP
   - Network Folder

4. Type the server details.
   - SFTP: Type the IP address or FQDN of the server, the port number, the user name, and the password.
   - Network Folder: Type the user name and password.

   **Note**
   Deep Discovery Director saves the server information and logon credentials automatically.

5. Type the details of at least one Virtual Analyzer image file.
   a. Type file paths.
   b. Type unique image names.
   c. (Optional) Type descriptions.

6. Click Upload.

Upload Center

Information about files that are uploading and that have been uploaded can be displayed using the Upload Center panel. Toggle the panel by clicking on the up-arrow-drawer icon in the top right corner of the screen. The panel is divided into the following two tabs:
Uploading Files

Information about files that are being uploaded to Deep Discovery Director is displayed in this tab.

To cancel a file upload, click on the x beside the upload.

File uploads are done in the following stages:

**TABLE 4-9. File Upload Stages**

<table>
<thead>
<tr>
<th>STAGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Calculating</td>
<td>The first parts of the file upload are being verified to ensure that the file upload is valid.</td>
</tr>
<tr>
<td>2: Uploading to the repository</td>
<td>The file is being uploaded to the repository. All SFTP server and network folder file uploads can be cancelled by any user.</td>
</tr>
</tbody>
</table>

**Note**

In **Distributed mode**, files are temporarily uploaded to the Management Server first before being uploaded to the Central Repository server. Browser uploads that are in the stage of being uploaded to the Management Server can only be cancelled by the uploader. Afterward the browser upload can be cancelled by any user.

| 3: Processing               | The file upload to the repository has completed and integrity is being verified. File uploads cannot be cancelled in this stage. |

File uploads display the following information:

**TABLE 4-10. Information about File Uploads**

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>The file name.</td>
</tr>
<tr>
<td>INFORMATION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(X KB / MB / GB)</td>
<td>The file size in KB / MB / GB.</td>
</tr>
<tr>
<td>Time left</td>
<td>The estimated time until the file upload is complete based on the file size and upload speed.</td>
</tr>
<tr>
<td>(X KB/s / MB/s / GB/s)</td>
<td>The upload speed in KB/s / MB/s / GB/s.</td>
</tr>
</tbody>
</table>

### Upload History

Information about files that have been uploaded to Deep Discovery Director is displayed in this tab.

To clear the upload history, click **Clear All**.

Uploaded files display the following information:

**TABLE 4-11. Information about Uploaded Files**

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>One of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Successful</strong>: The file upload was successful.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unsuccessful</strong>: The file upload was unsuccessful.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cancelled</strong>: The file upload was cancelled.</td>
</tr>
<tr>
<td>File name</td>
<td>The file name.</td>
</tr>
</tbody>
</table>

### Connection Settings

In **Distributed mode**, this screen enables you to configure Central Repository connection settings, and Local Repository connection, off-hour, and appliance assignment settings.
Registering to the Deep Discovery Director Server

Procedure

1. On the management console of a Local Repository server, go to Administration > Connect to Deep Discover Director.

2. Under Connection Settings, type the Server address for Deep Discovery Director.

3. Under Connection Settings, type the API key for Deep Discovery Director.

   Note
   You can find this information on the Help screen on the management console of Deep Discovery Director.

4. Click Register.

   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.

Connecting to the Central Repository Server

Note
If proxy settings have been configured, Deep Discovery Director connects to the Central Repository server using the proxy server.

For details, see Proxy on page 5-12.
Procedure

1. Type the following:
   - IPv4 address or FQDN of the Central Repository server
   - API key of the Central Repository server

   You can find this information on the Help screen on the management console of the Central Repository server.

   **Important**
   If you want to modify the server address and API key values, click Disconnect first.

2. Click Connect.

   The public key fingerprint (SHA-256) of the Central Repository server appears on the screen.

Managing Connections to Local Repository Servers

Procedure

1. (Optional) Select or disable the usage of host names instead of IP addresses as the identities of all Local Repository servers.

2. (Optional) Specify the preferred period for downloading update, upgrade, and Virtual Analyzer image files.

3. Assign at least one repository server to each appliance.

   **Note**
   You can assign up to two secondary repository servers only after selecting the primary repository server.

4. Click Save.
Chapter 5

Administration

Learn how to administer Deep Discovery Director in the following sections:

- Updates on page 5-2
- Alerts on page 5-5
- Microsoft Active Directory Integration on page 5-7
- System Settings on page 5-9
- Accounts on page 5-17
- System Logs on page 5-22
- System Maintenance on page 5-26
- License on page 5-35
Updates

Use the Updates screen, in Administration > Updates, to install hotfixes, patches, and firmware upgrades to Deep Discovery Director.

Hotfixes / Patches

Use the Hotfixes / Patches screen, in Administration > Updates > Hotfixes / Patches, to install Deep Discovery Director hotfixes and patches. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

<table>
<thead>
<tr>
<th>TABLE 5-1. Hotfixes / Patches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM UPDATE</strong></td>
</tr>
<tr>
<td>Hotfix</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Patch</td>
</tr>
</tbody>
</table>

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

http://downloadcenter.trendmicro.com/
Installing a Hotfix / Patch

Procedure

1. Obtain the product update file from Trend Micro.
   • If the file is an official patch, download it from the download center.
     http://downloadcenter.trendmicro.com/
   • If the file is a hotfix, send a request to Trend Micro support.

2. Go to Administration > Updates > Hotfixes / Patches.
   The Hotfixes / Patches screen appears.

3. Click Select and select the product update file.

4. Click Upload.

5. Click Install.

   ![Important]
   • Some updates cannot be rolled back once installed.
   • Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.

Deep Discovery Director installs the update and will automatically restart if it is required to complete the update.

6. Log on to the management console.

7. Go back to the Administration > Updates screen.

8. Verify that the hotfix / patch displays in the History section as the latest update.
Rolling Back a Hotfix / Patch

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

---

**Note**

Rolling back a hotfix or patch will automatically restart Deep Discovery Director if it is required to complete the rollback. Verify that all tasks on the management console have been completed before rollback.

---

**Procedure**

1. Go to **Administration > Updates > Hotfixes / Patches**.

2. In the **History** section, click **Roll Back**.

   Deep Discovery Director will automatically restart if it is required to complete the rollback.

3. Log on to the management console.

4. Go back to the **Administration > Updates > Hotfixes / Patches** screen.

5. Verify that the hotfix or patch rollback is displayed as the most recent entry in the **History** section.

---

**Firmware**

Use the **Firmware** screen, in **Administration > Updates > Firmware**, to install a Deep Discovery Director upgrade. Trend Micro prepares a readme file for each upgrade. Read the accompanying readme file before installing an upgrade for feature information and for special installation instructions.
Installing a Firmware Upgrade

Procedure

1. Go to Administration > Updates > Firmware.

   The Firmware screen appears.

2. Click Select and select the firmware upgrade file.

3. Click Upload.

4. Click Install.

---

**Important**

- Firmware upgrades cannot be rolled back once installed.
- Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the server until upgrading is complete.

---

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

5. Log on to the management console.

6. Go back to the Administration > Updates > Firmware screen.

7. Verify that the firmware version is correct.

---

**Alerts**

Deep Discovery Director monitors a variety of events and can be configured to generate alerts to inform users of those events.

The Alerts screen displays a list of all rules that are used to configure alerts with the following information:
Table 5-2. Alerts Columns

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Level</td>
<td>An alert can be classified as any of the following levels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>: The event requires immediate attention</td>
</tr>
<tr>
<td></td>
<td>• <strong>Important</strong>: The event requires observation</td>
</tr>
<tr>
<td></td>
<td>• <strong>Informational</strong>: The event requires limited observation</td>
</tr>
<tr>
<td>Rule</td>
<td>Rule that triggered the alert.</td>
</tr>
<tr>
<td></td>
<td>To edit an alert, click on any link in the Rule column.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Description of the rule.</td>
</tr>
<tr>
<td>Alert Frequency</td>
<td>Frequency at which the alert is generated when the rule criteria are met or exceeded.</td>
</tr>
<tr>
<td>Status</td>
<td>Click the toggle to enable or disable the alert.</td>
</tr>
</tbody>
</table>

Editing Alerts

Edit alerts to modify the frequency at which they are generated, and to modify alert recipients. The rule criteria are displayed at the beginning of the screen.

**Note**

By default, alerts are enabled and configured to be sent to all contacts with valid email addresses.

**Procedure**

1. Go to **Administration > Alerts**.

   The **Edit Alerts** screen appears.
2. Toggle the status of this alert.

3. Select the frequency at which the alert is generated when the rule criteria are met or exceeded:
   - Immediate
   - Once every 5 minutes
   - Once every 30 minutes
   - Once every 1 hour
   - Once a day

   **Note**
   - A shorter alert frequency means that the alert will be generated more often. Select a longer alert frequency to reduce the noise the alert generates.
   - This setting cannot be configured for all alerts.

4. (Optional) Select or disable **Send to all accounts**.

   **Note**
   This setting can be used in combination with the recipients list.

5. (Optional) Select a contact, type to search, or type an email address and press ENTER.
   The contact or account is added to the recipients list.

6. Click **Save**.

---

**Microsoft Active Directory Integration**

Use the **Microsoft Active Directory Integration** screen to integrate a Microsoft Active Directory server with Deep Discovery Director. Deep Discovery Director can then add...
Active Directory accounts to the list of accounts that can access the management console.

**Configuring Microsoft Active Directory Integration**

**Procedure**

1. Obtain the information required to configure Microsoft Active Directory integration from the server administrator.

2. Go to **Administration > Microsoft Active Directory Integration**.

3. Select the server type that is integrating:
   - **Microsoft Active Directory**
   - **Microsoft AD Global Catalog**

4. Type the server address.

5. Select the encryption method:
   - **SSL**
   - **STARTTLS**

6. Type the port number.

**Note**

Trend Micro recommends using the following default ports:

- For **Microsoft Active Directory**:
  - **SSL**: 636
  - **STARTTLS**: 389

- For **Microsoft AD Global Catalog**:
  - **SSL**: 3269
  - **StartTLS**: 3268
7. Type the base distinguished name.

8. Type the user name.

9. Type the password.

10. (Optional) Click Test Connection to verify that a connection to the Microsoft Active Directory server can be established using the specified information.

11. (Optional) If your organization uses a CA certificate, select Use CA certificate and click Select to locate the CA certificate file.

12. Click Save.

---

**System Settings**

The System Settings screen, in Administration > System Settings, includes the following:

- Network on page 5-9
- Proxy on page 5-12
- SMTP on page 5-13
- Bandwidth on page 5-14
- Time on page 5-15
- Certificate on page 5-16
- Session Timeout on page 5-17

**Network**

Use this screen to configure the host name or fully qualified domain name, IP address, and other network settings of the Deep Discovery Director appliance.

Modify the IP address immediately after completing all deployment tasks.
Note
You can also use the Preconfiguration Console to modify the network settings.
For details, see Configuring Network Addresses on the Preconfiguration Console on page 2-7.

Deep Discovery Director uses the specified IP address to connect to the Internet. The IP address also determines the URL used to access the management console.

Using Host Name as the Identity

In Consolidated mode, Deep Discovery Director supports using the host name instead of the IP address as the identity of the server.

When this feature is selected, appliances connect to Deep Discovery Director using the host name to download files required to execute plans.

Note
The host name must be resolvable within your network.

Procedure
1. Select Use host name instead of IP address as the identity of this server.
2. Configure the IP address and other network settings.
3. Click Save.

Configuring Port Binding

Deep Discovery Director supports the binding of services to a second network port.

When this feature is selected, Deep Discovery Director directs all connections to the license update server through eth1.
Note

- This feature cannot be configured from the Preconfiguration Console.
- In Distributed mode:
  - All connections to the Central Repository server and the license update server are directed through eth1.
  - This feature can only be configured on the management console of the Management Server and the Local Repository.

Procedure

1. Select eth0 (management) and eth1 to bind your services to.

Important

This feature requires at least two network interface cards to be installed and configured. The feature will be hidden from the Network screen otherwise.

A new eth1 section to configure network settings for the second network port displays under the existing eth0 (management) section.

2. Configure the IP address and other network settings of the second network port.

3. Click Save.

Using IPv4 and IPv6 Dual Stack

Deep Discovery Director supports IPv4 and IPv6 dual-stack configuration to function in network environments that communicate using the IPv6 protocol.

Procedure

1. Select IPv4 and IPv6 (dual stack) as Type.

A new section to configure IPv6 settings displays between the existing IPv4 and DNS settings.
2. Configure the IPv6 settings.

3. Click Save.

Proxy

**Distributed mode**: Specify proxy settings if Deep Discovery Director connects to the Central Repository and license update server through a proxy server.

**Consolidated mode**: Specify proxy settings if Deep Discovery Director connects to the license update server through a proxy server.

**Note**
When port binding is configured, only eth1 will use the proxy settings.

**Procedure**

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

   The **Proxy** screen appears.

2. Enable proxy settings.

   • **Distributed mode**: Select **Connect to the Central Repository using a proxy server**.
   
   • **Consolidated mode**: Select **Connect to the license update server using a proxy server**.

3. Select the protocol to use for proxying.

   • HTTP
   
   • SOCKS4
   
   • SOCKS5

4. Type the IPv4 address or FQDN of the proxy server.
5. Type the port number. The default port number is 80.

6. (Optional) If you selected HTTP or SOCKS5 as protocol, and your proxy server requires authentication, select Specify authentication credentials, and then type the user name and password used for authentication.

7. (Optional) Click Test Connection to verify the connection to the proxy server.

8. Click Save.

SMTP

Use the SMTP screen, in Administration > System Settings > SMTP, to enable using a SMTP server to send alert notifications through email.

Procedure

1. Go to Administration > System Settings > SMTP.

   The SMTP screen appears.

2. Select Use a SMTP server.

3. Type the IPv4 address or FQDN of the SMTP server.

4. Type the port number. The default port number is 25.

5. Type a sender email address

6. (Optional) If the SMTP server requires authentication, select SMTP server requires authentication, and then type the user name and password used for authentication.

   **WARNING!**

   Verify that the user name and password are valid. Connections made using an incorrect user name and password may cause some SMTP servers to reject all network request originating from Deep Discovery Director.

7. (Optional) Verify that Deep Discovery Director can communicate with the specified SMTP server and send emails.
a. Click **Send Test Message**.
   The **Send Test Message** dialog appears.

b. Type at least one valid email address, and then click **Send**.
   If Deep Discovery Director can communicate with the specified SMTP server, an email with the predefined subject and message will be sent to the specified email addresses.

c. Check your email account for receipt of the email.

---

### Bandwidth

Use the **Bandwidth** screen, in **Administration > System Settings > Bandwidth**, to enable bandwidth usage throttling settings. Bandwidth usage throttling helps manage the impact downloading and uploading of files may have on your network and internet connection.

For details, see *Configuring Bandwidth Usage Throttling on page 5-14.*

### Configuring Bandwidth Usage Throttling

**Procedure**

1. Go to **Administration > System Settings > Bandwidth**.
   The **Bandwidth** screen appears.

2. Select **Enable bandwidth usage throttling**.

3. Under **Upload**, type a speed limit value to limit the speed for uploading files from the Management Server to the Central Repository server.

   **Note**

   This setting is only available when Deep Discovery Director is deployed in **Distributed mode**.
4. Under **Download**, type a speed limit value to:
   - **Distributed mode**: Limit the speed per connection for downloading files from the Central Repository server to the Local Repository server. Each Local Repository server establishes one connection.
   - **Consolidated mode**: Limit the speed per connection for downloading files from the Deep Discovery Director server to the appliance. Each appliance establishes one connection.

5. Under **Download**, type a maximum value to limit the number of connections to.

6. Click **Save**.

---

**Time**

Configure date and time settings immediately after installation.

---

**Procedure**

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

   The **Time** screen appears.

2. Select one of the following methods and configure the applicable settings.
   - Select **Connect to an NTP server** and type the FQDN or IP address of the NTP server.
   - Select **Set manually** and configure the time.

3. Select the applicable time zone.

   **Note**
   
   Daylight Saving Time (DST) is used when applicable.

4. Select the preferred date and time format.
5. Click Save.

Certificate

Digital certificates are electronic documents that are used to create secure connections between clients and servers or websites. A valid and trusted certificate ensures clients that they are connecting to a trusted server or website, and helps protect against man-in-the-middle attacks.

Certificates become trusted by going through a validation process of a Certificate Authority (CA). Certificate Authorities themselves are usually third-party companies that are trusted by both the client and server or website.

On first installation, Deep Discovery Director creates a self-signed SSL certificate that will be used to securely communicate with other Deep Discovery appliances and Local Repository. In doing so, Deep Discovery Director also acts as its own CA.

Users who wish to adopt their own organizations' CA can import a certificate signed by that CA to Deep Discovery Director.

---

**Important**

Accessing the management console of a Deep Discovery Director server with an untrusted or expired certificate displays a security warning in the web browser.

An untrusted or expired certificate does not affect the communication between Deep Discovery Director servers and Deep Discovery appliances. Deep Discovery Director servers with untrusted or expired certificates can still deploy plans to Deep Discovery appliances, and appliances can still download the files required to execute the plans from those servers.

---

Importing a Certificate

Deep Discovery Director uses a certificate to create secure connections to clients. Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.
Important

Importing the certificate will restart the service. Existing connections to repositories and Deep Discovery appliances will be interrupted, and clients will have to trust the new fingerprint to restore the connection.

Procedure

1. Go to Administration > System Settings > Certificate.

   The Certificate screen appears.

2. Click Import, select the certificate, and then click Open.

   The certificate will be imported immediately.

Session Timeout

Select the time period after which users are logged out due to inactivity. The default value is 15 minutes.

Accounts

Use the Accounts screen, in Administration > Accounts, to create and manage user accounts. Users can use these accounts, instead of the default administrator account, to access the management console.

Deep Discovery Director supports the creation of user accounts by using the following methods:

- *Adding a Local User Account on page 5-18*
- *Adding an Active Directory User Account or Group on page 5-19*
Note

This method is only available if Microsoft Active Directory Integration has been configured.

For details, see Microsoft Active Directory Integration on page 5-7.

Adding a Local User Account

Procedure

1. Go to Administration > Accounts, and then click Add.

The Add Account screen appears.

2. Toggle the Status of this account.

3. Select Local user as the Type of this account.

4. Type a valid user name.

5. Type a valid password.

6. Type the password again to confirm it.

   Tip

   Select Show as plain text to unmask the password and skip this step.

7. (Optional) Type a valid email address.

8. Select a Role for this account. The role determines the level of access this account has.

   • Administrator: Users with this role have full access to all management console features.

   • Operator: Users with this role have read-only access to all management console features.

9. (Optional) Type a description for this account.
10. Click **Save**.

---

**Adding an Active Directory User Account or Group**

If your company uses Microsoft Active Directory to manage user accounts and groups, you can enable those user accounts and groups access to Deep Discovery Director.

---

**Note**

- Microsoft Active Directory Integration has to be configured before an Active Directory user account or group can be added.

  For details, see *Microsoft Active Directory Integration on page 5-7*.

- Deep Discovery Director syncs Microsoft Active Directory user accounts and groups every 24 hours. User accounts or groups that are removed from the Active Directory server will be removed from Deep Discovery Director after syncing with the Active Directory server.

- If a Microsoft Active Directory user is a member of one or more groups, the user's level of access in Deep Discovery Director is determined by the highest level of access granted to the user's Deep Discovery Director account or any group the user is a member of.

---

**Procedure**

1. Go to **Administration > Accounts**, and then click **Add**.

   The **Add Account** screen appears.

2. Toggle the **Status** of this account.

3. Select **Active Directory user or group** as the **Type** of this account.

4. Type a user or group name and click **Search** to search the Active Directory for matching user accounts or groups.

   Matching user accounts and groups are displayed in the results table.
5. Select the Active Directory user account or group to add.

Note
User accounts are not displayed in the results table if:

- The user account's User Principle Name (UPN) is not specified on the Active Directory server
- The user account is disabled on the Active Directory server

6. Select a **Role** for this account. The role determines the level of access this account has.

   - **Administrator**: Users with this role have full access to all management console features.
   - **Operator**: Users with this role have read-only access to all management console features.

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

8. Click **Save**.

**Other Accounts Tasks**

You can also perform the following tasks:
### TABLE 5-3. Other Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit account</td>
<td>Click on a user name to open the <strong>Edit Account</strong> screen and do the following:</td>
</tr>
<tr>
<td></td>
<td>• Toggle the account status</td>
</tr>
<tr>
<td></td>
<td>• Change the password</td>
</tr>
<tr>
<td></td>
<td>• Change the email address</td>
</tr>
<tr>
<td></td>
<td>• Change the role</td>
</tr>
<tr>
<td></td>
<td>• Modify the description</td>
</tr>
</tbody>
</table>

**Note**

- The passwords of Microsoft Active Directory accounts cannot be changed from the management console.
- Clicking on the user name of the logged-on local account only allows you to modify the password, email address, and description.
- Clicking on the user name of the logged-on Microsoft Active Directory account only allows you to modify the description.
- Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.
- Users who are currently logged on to the management console and whose roles are changed will be logged off automatically.
<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete account</td>
<td>Select one or more user accounts to delete and then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• There must be at least one local administrator account.</td>
</tr>
<tr>
<td></td>
<td>• You cannot delete the logged-on account.</td>
</tr>
<tr>
<td></td>
<td>• Users who are currently logged on to the management console will be logged off automatically.</td>
</tr>
<tr>
<td>View account lock</td>
<td>Deep Discovery Director includes a security feature that locks an account in case the user typed an incorrect password three times in a row. This feature cannot be disabled. Accounts locked this way, even administrator accounts, unlock automatically after ten minutes.</td>
</tr>
<tr>
<td>status</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Microsoft Active Directory accounts are never locked.</td>
</tr>
<tr>
<td>Toggle account status</td>
<td>Click on the toggle in the <strong>Status</strong> column to enable or disable the user account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• There must be at least one active local administrator account.</td>
</tr>
<tr>
<td></td>
<td>• Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.</td>
</tr>
</tbody>
</table>

**System Logs**

Use the **System Logs** screen, under **Administration > System Logs**, to view, query and export system logs.
Deep Discovery Director maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.

Deep Discovery Director stores system logs in the appliance hard drive.

Query system logs to gather information from the database. The queried system logs can be exported in CSV format for offline viewing.

For details, see *Querying System Logs on page 5-24*.

The following table lists all system-log-related information:

**TABLE 5-4. System Log Information**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged</td>
<td>Event date and time</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event identifier&lt;br&gt;Each specific action has its own event ID. Examples:&lt;br&gt;</td>
</tr>
<tr>
<td></td>
<td>• 20001&lt;br&gt;<strong>Description:</strong> User logged on&lt;br&gt;• 20002&lt;br&gt;<strong>Description:</strong> User logged off</td>
</tr>
<tr>
<td>Type</td>
<td>One of the following types displays:&lt;br&gt;• Account Logon/Logoff&lt;br&gt;• System&lt;br&gt;• Update</td>
</tr>
<tr>
<td>Level</td>
<td>One of the following levels displays:&lt;br&gt;• Informational&lt;br&gt;• Warning&lt;br&gt;• Error</td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Result     | One of the following results displays:  
  • Successful  
  • Unsuccessful |
| Source     | Activity by source  
Information about the following sources may display:  
  • user name  
    Example: johnadmin  
  • system  
    Example: SYSTEM |
| IP Address | Event IP address |
| Description| Event details |

**Querying System Logs**

The task of finding a specific system log entry can be difficult when there may be hundreds or thousands to go through. Use the filters and search box to lower the number of entries shown.

**Procedure**

1. Go to **Administration > System Logs**.  
   The **System Logs** screen appears.

2. Click the **Filters** button.  
   Filter drop-down lists and a search box appear.

3. Select a log type.  
   • All types
• Account Logon/Logoff
• System
• Update

The screen is updated immediately.

4. Select a log level.
   • All levels
   • Error
   • Warning
   • Informational

The screen is updated immediately.

5. Select a log result.
   • All results
   • Successful
   • Unsuccessful

The screen is updated immediately.

6. Select a period or specify a custom period using the calendar and clock.

The screen is updated immediately.

7. Type a event ID, source, or description keyword in the search box and press ENTER to only display system logs whose event ID, source, or description contain the keyword.

8. Click Export to export the currently filtered system logs.

The Export dialog displays.

9. Confirm the system log filters and select a delimiter to use.
   • Comma
10. Click OK to export and download the currently filtered system logs to a CSV file with the chosen delimiter.

![Note]

The exported system logs are ordered by Log ID, a consecutive number that coincides with the Logged date and time.

System Maintenance

The System Maintenance screen, in Administration > System Maintenance, includes the following tabs:

- System Status on page 5-26
- Storage on page 5-27
- Back Up on page 5-27
- Restore on page 5-30
- Power Off / Restart on page 5-34

System Status

The System Status screen displays the utilization of key hardware components.

When Deep Discovery Director is deployed in Distributed mode:

- The Management Server displays the utilization of both itself and the Central Repository server
- The Central Repository server only displays the utilization of itself
The Local Repository server only displays the utilization of itself.

## Storage

Use the Storage screen, in Administration > System Maintenance > Storage, to configure how long Deep Discovery Director saves database entries and system logs.

- **Delete database entries older than X days**: Type the number of days to save database entries. Entries older than the specified value are automatically deleted.

  **Tip**

  A database entry in this context refers to a Deep Discovery Director plan.

- **Delete system logs older than X days**: Type the number of days to save system logs. Logs older than the specified value are automatically deleted.

  **Note**

  In addition to the settings above, Deep Discovery Director automatically purges system logs until there is 200 MB free database disk space. This threshold cannot be modified.

## Back Up

Use the Back Up screen, in Administration > System Maintenance > Back Up, to export a backup file of most of the configuration settings and the database, and to configure automatic backups of those.

- **Exporting a Configuration Settings and Database Backup on page 5-29**

- **Configuring Automatic Backups on page 5-29**

The following table shows the screens and elements with backed up configuration settings.
### Table 5-5. Backed Up Configuration Settings

<table>
<thead>
<tr>
<th>Screen</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Appliance tree with group structure</td>
</tr>
<tr>
<td></td>
<td>Registered appliances and appliance details</td>
</tr>
<tr>
<td>Appliance Updates &gt; Plans</td>
<td>All plans</td>
</tr>
<tr>
<td>Appliance Updates &gt; Connection Settings &gt; Central Repository</td>
<td>Central Repository settings</td>
</tr>
<tr>
<td>Appliance Updates &gt; Connection Settings &gt; Local Repository</td>
<td>Local Repository off-hour settings</td>
</tr>
<tr>
<td></td>
<td>Local Repository server assignments</td>
</tr>
<tr>
<td>Administration &gt; Alerts</td>
<td>All alert settings</td>
</tr>
<tr>
<td>Administration &gt; Microsoft Active Directory Integration</td>
<td>Microsoft Active Directory server settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Proxy</td>
<td>Proxy settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Bandwidth</td>
<td>Bandwidth usage throttling settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Time</td>
<td>Time settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Certificate</td>
<td>Certificate</td>
</tr>
<tr>
<td>Administration &gt; System Settings &gt; Session Timeout</td>
<td>Session timeout value</td>
</tr>
<tr>
<td>Administration &gt; Accounts</td>
<td>All user accounts</td>
</tr>
<tr>
<td>Administration &gt; System Logs</td>
<td>All system logs</td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Storage</td>
<td>Storage values</td>
</tr>
</tbody>
</table>
Exporting a Configuration Settings and Database Backup

Deep Discovery Director can export a backup file of most configuration settings and the database. Use the backup file to restore Deep Discovery Director to a previous point in time. Use the backup file on another server, when the active server is unresponsive and cannot be restored, to restore operation and minimize downtime.

Procedure

1. Go to Administration > System Maintenance > Back Up.  
   The Back Up screen appears.
2. Under Configuration Settings and Database Backup, click Export.  
   The active server exports a backup file with the configuration settings and database. For details, see Back Up on page 5-27.
3. Download and save the backup file.

Configuring Automatic Backups

Deep Discovery Director can be configured to create and upload automatic backups of its configuration settings and database to a SFTP server of your choice. Deep Discovery Director creates up to five backup files, after which the oldest one is deleted in order to keep the number of backup files at five.

Procedure

1. Go to Administration > System Maintenance > Back Up.  
   The Back Up screen appears.
2. Under **Automatic Backups**, select **Automatically back up to SFTP server**.

3. Type the IP address or FQDN of the SFTP server.

4. Type the port number. The default port number is 22.

5. Type the folder path to use on the SFTP server.

6. Type the user name and password used to log on to the SFTP server.

7. Specify a backup frequency using the drop-down lists and the clock tool.

8. Click **Save**.

---

**Restore**

Use the **Restore** screen, in **Administration > System Maintenance > Restore**, to restore configuration settings and database from a backup file. If the active Deep Discovery Director server is unresponsive or cannot be restored, a configuration settings and database backup can also be used on another server to restore operation and minimize downtime.

- **Restoring a Configuration Settings and Database Backup on page 5-30**
- **Replacing the Active Server with Another Server on page 5-32**

---

**Note**

For information on exporting a configuration settings and database backup, see **Exporting a Configuration Settings and Database Backup on page 5-29**.

---

**Restoring a Configuration Settings and Database Backup**

A configuration settings and database backup can be used to restore Deep Discovery Director to a previous point in time.

If the active Deep Discovery Director is unresponsive or cannot be restored, a configuration settings and database backup can also be used on another server to restore operation and minimize downtime.
For details, see Replacing the Active Server with Another Server on page 5-32.

### Procedure

1. Go to Administration > System Maintenance > Restore.

   The Restore screen appears.

2. Click Select File... and select the backup file.

3. Click Upload.

   The backup file is uploaded, and Deep Discovery Director displays information about the backup file.

4. Click Restore.

   Deep Discovery Director displays a confirmation message.

5. Click OK.

   Deep Discovery Director restores configuration settings and database from the backup file, and then restarts the server.

6. (Optional) Restore the repository.
   - **Consolidated mode**: Re-upload all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

   **Important**

   Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.

   - **Distributed mode**: The Management Server automatically receives the list of available update, upgrade, and Virtual Analyzer image files from the Central Repository server.

7. (Optional) Configure the network addresses. For details, see Network on page 5-9.

8. (Optional) Activate Deep Discovery Director. For details, see License on page 5-35.
The server is now ready to resume operation.

Replacing the Active Server with Another Server

If the Deep Discovery Director server is unresponsive or cannot be restored, it can be replaced by another server.

The following table lists requirements that need to be fulfilled by the replacement server. For details, see System Requirements on page 2-2.

**TABLE 5-6. Replacement Server Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host machine hardware</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>Host machine software</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>Deep Discovery Director deployment type</td>
<td>Must be the same as active server</td>
</tr>
<tr>
<td>Deep Discovery Director version and build</td>
<td>Must be the same as active server</td>
</tr>
</tbody>
</table>

**Procedure**

1. Back up the configuration settings and database of the active server.
   a. On the management console of the active server, go to Administration > System Maintenance > Back Up.
   b. Under Configuration Settings and Database Backup, click Export.
      The active server exports a backup file with the configuration settings and database. For details, see Back Up on page 5-27.
   c. Download and save the backup file.

2. Install Deep Discovery Director on the replacement server.
   For details, see Installing Deep Discovery Director on page 2-5.

3. Configure temporary network addresses for the replacement server.
For details, see Configuring Network Addresses on the Preconfiguration Console on page 2-7.

**Important**
Verify that the temporary network addresses are different from the network addresses of the active server to avoid IP addressing conflicts.

4. Log on to the management console of the replacement server.

5. Restore the configuration settings and database on the replacement server.
   a. On the management console of the replacement server, go to Administration > System Maintenance > Restore.
   b. Click Select File... and select the backup file.
   c. Click Upload.
      The backup file is uploaded, and Deep Discovery Director displays information about the backup file.
   d. Click Restore.
      Deep Discovery Director displays a confirmation message.
   e. Click OK.
      Deep Discovery Director restores configuration settings and database from the backup file, and then restarts the server.

6. Restore the repository.
   - **Consolidated mode:** Re-upload all previously uploaded update, upgrade, and Virtual Analyzer image files to the repository.

**Important**
Update, upgrade, and Virtual Analyzer image files are not included in the backup file and are not restored automatically. Appliances cannot download and execute plans if the files are not re-uploaded to the repository.
• Distributed mode: The Management Server automatically receives the list of available update, upgrade, and Virtual Analyzer image files from the Central Repository server.

7. Power off the active server.
   a. On the management console of the active server, go to Administration > System Maintenance > Power Off / Restart.
   b. Click Power Off.

   The active server stops all services and gracefully shuts down.

   WARNING!

   The replacement server will be configured to use the network addresses of the active server. Leaving the active server powered on will cause IP addressing conflicts.

8. Configure the replacement server to use the network addresses of the active server. For details, see Network on page 5-9.

9. Activate Deep Discovery Director. For details, see License on page 5-35.

   The replacement server is now ready to resume operation as the new active server.

Power Off / Restart

Use the Power Off / Restart screen, in Administration > Power Off / Restart, to power off or restart the server.

• Power Off: All active tasks are stopped, and then the server gracefully shuts down.

• Restart: All active tasks are stopped, and then the server is restarted.

Integrated products may queue data while the server is unavailable.
License

Use the License screen, in Administration > License, to view, activate, and renew the Deep Discovery Director license.

The License screen includes the following information and options.

**TABLE 5-7. License Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays either Activated, Not Activated, or Expired.</td>
</tr>
<tr>
<td>![Important]</td>
<td>Deep Discovery Director does not allow the creation of new plans when</td>
</tr>
<tr>
<td></td>
<td>the license status is Not Activated or Expired. Existing plans will</td>
</tr>
<tr>
<td></td>
<td>deploy and execute as usual.</td>
</tr>
<tr>
<td></td>
<td>Click View details to view detailed license information from the Trend</td>
</tr>
<tr>
<td></td>
<td>Micro website. If the status changes (for example, after you renewed</td>
</tr>
<tr>
<td></td>
<td>the license) but the correct status is not indicated in the screen,</td>
</tr>
<tr>
<td></td>
<td>click Refresh.</td>
</tr>
<tr>
<td>![Note]</td>
<td>If proxy settings are enabled, Deep Discovery Director connects to the</td>
</tr>
<tr>
<td></td>
<td>license update server using the proxy server.</td>
</tr>
<tr>
<td>Type</td>
<td>• Full: Provides access to all product features</td>
</tr>
<tr>
<td></td>
<td>• Trial: Provides access to all product features</td>
</tr>
<tr>
<td>Expiration date</td>
<td>View the expiration date of the license. Renew the license before</td>
</tr>
<tr>
<td></td>
<td>it expires. Click View renewal instructions to view instructions from</td>
</tr>
<tr>
<td></td>
<td>the Trend Micro website.</td>
</tr>
</tbody>
</table>
View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code.

The **License** screen reappears displaying the number of days left before the product expires.

---

**Tip**

Deep Discovery Director can be activated with the Activation Code of any Deep Discovery product.
Chapter 6

Technical Support

Learn about the following topics:

- Troubleshooting Resources on page 6-2
- Contacting Trend Micro on page 6-3
- Sending Suspicious Content to Trend Micro on page 6-4
- Other Resources on page 6-5
Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

2. Select from the available products or click the appropriate button to search for solutions.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Contact Support and select the type of support needed.

Tip

To submit a support case online, visit the following URL:


A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia
provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to [http://about-threats.trendmicro.com/us/threatencyclopedia#malware](http://about-threats.trendmicro.com/us/threatencyclopedia#malware) to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

### Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone: +1 (817) 569-8900</td>
</tr>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:
  

- Trend Micro product documentation:
  
  [http://docs.trendmicro.com](http://docs.trendmicro.com)
Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:


Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.
Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

D
documentation feedback, 6-6

S
support
  resolve issues faster, 6-4