TREND MICRO™
Deep Discovery™ Director
(Distributed Mode)
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
Privacy and Personal Data Collection Disclosure

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

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


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

# Table of Contents

## Preface

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

## Chapter 1: Introduction

About Deep Discovery Director (Distributed Mode) ......................................................... 1-2  
Features and Benefits .............................................................................................................. 1-2  

## Chapter 2: System Requirements

## Chapter 3: Installing Deep Discovery Director

## Chapter 4: Configuring Network Addresses on the Preconfiguration Console

## Chapter 5: Logging on to the Management Console

## Chapter 6: Appliances

Directory ................................................................................................................................. 6-2  
   Directory Tasks ......................................................................................................................... 6-2  
   Other Directory Tasks .............................................................................................................. 6-4  
Plans ........................................................................................................................................ 6-7  
   Plan Tasks ................................................................................................................................. 6-9  
   Appliance Statuses ................................................................................................................. 6-10  
   Other Plan Tasks ...................................................................................................................... 6-11
Repository ................................................................................................................. 6-29
  Hotfixes / Critical Patches / Firmware .......................................................... 6-29
  Virtual Analyzer Images ............................................................................... 6-30
  Upload Center .................................................................................................. 6-32
Connection Settings .......................................................................................... 6-34
  Registering to the Deep Discovery Director Management Server 6-34
  Connecting to the Central Repository Server ........................................ 6-35
  Managing Connections to Local Repository Servers ................................ 6-36

Chapter 7: Alerts
  About Alerts ...................................................................................................... 7-2
  Triggered Alerts ............................................................................................... 7-2
  Built-in Rules .................................................................................................. 7-2
    Editing a Built-in Rule ................................................................................. 7-3

Chapter 8: Administration
  Updates ............................................................................................................ 8-2
    Hotfixes / Patches ....................................................................................... 8-2
    Firmware ....................................................................................................... 8-4
  Integrated Products/Services ........................................................................ 8-5
    Microsoft Active Directory ..................................................................... 8-6
  System Settings .............................................................................................. 8-7
    Network ......................................................................................................... 8-8
    Proxy ............................................................................................................. 8-9
    SMTP ............................................................................................................... 8-10
    SNMP ........................................................................................................... 8-11
    Bandwidth ..................................................................................................... 8-16
    Time ................................................................................................................. 8-17
    Certificate ..................................................................................................... 8-18
    Session Timeout ............................................................................................ 8-19
  Account Management ....................................................................................... 8-19
    Accounts ....................................................................................................... 8-20
    Roles .............................................................................................................. 8-24
Chapter 9: Technical Support

Troubleshooting Resources ................................................................. 9-2
  Using the Support Portal ................................................................. 9-2
  Threat Encyclopedia ................................................................. 9-2

Contacting Trend Micro ................................................................. 9-3
  Speeding Up the Support Call .......................................................... 9-4

Sending Suspicious Content to Trend Micro ............................................. 9-4
  Email Reputation Services ................................................................. 9-4
  File Reputation Services ................................................................. 9-5
  Web Reputation Services ................................................................. 9-5

Other Resources ................................................................................. 9-5
  Download Center ........................................................................... 9-5
  Documentation Feedback ................................................................. 9-6
Preface

Welcome to the Trend Micro Deep Discovery Director (Distributed Mode) Administrator's Guide. This guide contains information about product settings.
The documentation set for Deep Discovery Director (Distributed Mode) 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 (Distributed Mode), and explanations on Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) management console. The Online Help contains explanations of Deep Discovery Director (Distributed Mode) components and features, as well as procedures needed to configure Deep Discovery Director (Distributed Mode).</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: http://docs.trendmicro.com/en-us/home.aspx

**Audience**

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

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

**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><img src="image" alt="Note" /></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><img src="image" alt="Tip" /></td>
<td>Recommendations or suggestions</td>
</tr>
</tbody>
</table>
### Convention Description

<table>
<thead>
<tr>
<th><strong>Important</strong></th>
<th>Information regarding required or default configuration settings and product limitations</th>
</tr>
</thead>
<tbody>
<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](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 (Distributed Mode) 5.0 and the features and benefits in this release.
About Deep Discovery Director (Distributed Mode)

Trend Micro Deep Discovery Director (Distributed Mode) 5.0 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.

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

Features and Benefits

Deep Discovery Director (Distributed Mode) includes the following features:

<table>
<thead>
<tr>
<th>Feature/Benefit</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>The <strong>Directory</strong> displays information about Deep Discovery appliances and repository servers that are registered to Deep Discovery Director (Distributed Mode).</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 <strong>Repository</strong> screen displays all update, upgrade, and Virtual Analyzer image files hosted by the server. Upload and delete files from here.</td>
</tr>
<tr>
<td>System Alerts</td>
<td>Administrators can view the details of triggered alerts directly on the management console. Built-in rules can be used to alert users of specific threats.</td>
</tr>
<tr>
<td>Updates</td>
<td>The <strong>Updates</strong> screen enables you to install hotfixes, patches and firmware upgrades to Deep Discovery Director (Distributed Mode). After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.</td>
</tr>
<tr>
<td><strong>Feature/Benefit</strong></td>
<td><strong>Details</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Active Directory Integration</td>
<td>Deep Discovery Director (Distributed Mode) allows Active Directory accounts to access the management console.</td>
</tr>
<tr>
<td>Role-based access control</td>
<td>Built-in roles allow administrators to control which management console screens and features can be accessed.</td>
</tr>
<tr>
<td>System Logs</td>
<td>Deep Discovery Director (Distributed Mode) 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>
# 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></td>
<td>• Network interface card: 1 with E1000 or VMXNET 3 adapter</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Director (Distributed Mode) does not support the VMXNET 2 (Enhanced) adapter type.</td>
</tr>
<tr>
<td></td>
<td>• For port binding, specify the same adapter type to use for all network interface cards.</td>
</tr>
<tr>
<td></td>
<td>• SCSI Controller: LSI Logic Parallel</td>
</tr>
<tr>
<td></td>
<td>• CPU: 1.8GHz (at least 4 cores)</td>
</tr>
<tr>
<td></td>
<td>• Memory: 8GB</td>
</tr>
<tr>
<td></td>
<td>• Hard disk: 120GB (thin provisioned)</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Hypervisor: VMware vSphere ESXi 5.5/6.0/6.5 or Microsoft Hyper-V in Windows Server 2012 R2/2016</td>
</tr>
<tr>
<td></td>
<td>• Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)</td>
</tr>
<tr>
<td><strong>Requirement</strong></td>
<td><strong>Minimum Specifications</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------</td>
</tr>
</tbody>
</table>
| Ports          | • TCP 443 (Deep Discovery Director connection)  
                 • UDP 123 (default NTP server connection) |
| Certificate    | • Self-signed  
                 • PEM format  
                 • Certificate and private key in the same file  
                 • No certificate chain  

Encryption methods:  
• Private key: RSA algorithm only  
• Certificate: Digest size of 256 (SHA-256) or higher

Generation command example (CentOS):

```
# 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
```
Chapter 3

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 4 cores
   • Memory: 8GB
   • Network interface card: 1 with E1000 or VMXNET 3 adapter

   Important
   • Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) ISO image file, and then boot the virtual machine from the CD/DVD drive.

   The Deep Discovery Director (Distributed Mode) Installation screen appears.

4. Select Install software.

   The Deep Discovery Director (Distributed Mode) Components screen appears.

5. Select Install Management Server, Install Central Repository, and Install Central Repository.

   Note
   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 **Disk Space Configuration** screen appears.

9. (Optional) Modify the disk space configuration, and then click **Continue**.

The **Repartition Disks** confirmation message appears.

10. Click **Continue**.

The installation starts.
Chapter 4

Configuring Network Addresses on the Preconfiguration Console

Procedure

1. Open the Deep Discovery Director (Distributed Mode) 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 8-8.

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

The Main Menu screen appears after the settings are successfully saved.
Chapter 5

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 management console appears.
Chapter 6

Appliances

Learn how to manage appliances, perform plan related tasks, maintain the repository, and configure Central Repository and Local Repository settings in the following topics:

• Directory on page 6-2
• Plans on page 6-7
• Repository on page 6-29
• Connection Settings on page 6-34
Directory

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

- 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 (Distributed Mode) 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 object types and the available information for each object.
### TABLE 6-1. Directory Object Types

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
</table>
| Appliances     | • **Plan**: Plans that were or will be deployed to the appliance  
|                | • **Appliance**: 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 |

**Note**

For Deep Discovery Analyzer clusters, Deep Discovery Director (Distributed Mode) also displays the following:

- **Active primary appliance**: Information on the active primary appliance (high availability cluster and load balancing cluster)
- **Passive primary appliance**: Information on the passive primary appliance (high availability cluster)
- **Secondary appliances**: Information on the secondary appliance (load balancing cluster)

- **Updates**: Build number and installation time of all installed updates, and information about where and when the appliance’s configuration settings were replicated from
- **Virtual Analyzer**: Information about the Virtual Analyzer configuration of the appliance, such as type, internal Virtual Analyzer maximum images and instances, and deployed images and instances

**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.
Deep Discovery Director (Distributed Mode) 5.0 Administrator's Guide

### Object Displayed Information

<table>
<thead>
<tr>
<th>OBJECT</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Repository servers</td>
<td>• <strong>Plan</strong>: Plans that were or will be deployed to the server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server</strong>: Identifiers such as IP address, host name and display name, and other information such as the address of the Central Repository server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Updates</strong>: Build number and installation date of all installed updates</td>
</tr>
<tr>
<td></td>
<td>• <strong>Repository</strong>: Files that it hosts and IP address of the Central Repository server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connected Appliances</strong>: Appliances that are configured to download files from it</td>
</tr>
<tr>
<td>Note</td>
<td>You can assign a maximum of three repository servers per appliance.</td>
</tr>
<tr>
<td>Groups</td>
<td>Overview of appliances and plans associated with that group, including statuses and connection information.</td>
</tr>
</tbody>
</table>

### Other Directory Tasks

You can also perform the following actions:

**TABLE 6-2. 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>
</tbody>
</table>
**Action** | **Description**
--- | ---
Edit group or appliance names | To edit a group or appliance name:
1. Click the menu icon beside the group or appliance name and then select **Edit**.
2. In the text box, type a name with a maximum of 256 characters.

Edit appliance repository server assignments | To edit the repository server assignments of an appliance:
1. Click the menu icon beside the appliance name and then select **Edit**.
2. Modify the repository server assignments using the drop-down lists.

Move groups or appliances | To move a group or an appliance to a different group:
1. Click the menu icon beside the group or appliance name and then select **Move**.
2. In the window, select the new folder and then click **Move**.

This function is disabled whenever:
- Deployment of one or more associated plans is pending or in progress.
- The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**.
<table>
<thead>
<tr>
<th><strong>ACTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Delete groups   | 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**.                                                                 |
|                 | **WARNING!**                                                                                                                                                                                                    |
|                 | Deleting a group cancels the plans associated with that group, moves appliances to the **Unmanaged** group, and unregisters repository servers from Deep Discovery Director (Distributed Mode). Only groups without unfinished plans can be deleted. |
|                 | This function is disabled whenever:                                                                                                                                             |
|                 | • Deployment of one or more associated plans is pending or in progress.                                                                               |
|                 | • The appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**.                                                            |
| Delete appliances| To delete an appliance, click the menu icon beside the display name and then select **Delete**.                                                                                                               |
|                 | This function is disabled whenever the appliance tree is filtered by a specific Deep Discovery appliance. To enable the function, change the view to **All**.                                                        |
|                 | **WARNING!**                                                                                                                                                                                                    |
|                 | Deleting an appliance unregisters it from Deep Discovery Director (Distributed Mode), stops all connections, and cancels all associated plans.                                                                     |
| Switch views    | To switch between custom views, click on the name beside **Views** and then select the view to switch to.                                                                                                  |


### 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 plan to be deployed must match the product and language of the target appliances.

When a plan is deployed, Deep Discovery Director (Distributed Mode) sends instructions to the target appliances on when to download required files from a
designated repository server, and on when to execute the plan. If the plan is not deployed immediately, appliances download files and execute the plan according to a schedule with the following factors:

• Deployment start
• Download period
• Execution start

---

**Important**

All times are based on appliance local time

---

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

**TABLE 6-3. Plans**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specified during plan creation</td>
</tr>
</tbody>
</table>
| Type | Type of plan deployed to targets. Deep Discovery Director (Distributed Mode) currently supports the following plan types:  
  • Hotfix / Critical patch / Firmware  
  • Virtual Analyzer images  
  • Configuration replication |
| Status | 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 (Distributed Mode).  
  • **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. |
Table 6-4. 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>
<tr>
<td>Appliance information</td>
<td>Host name, appliance status, deployment start and completion, and appliance path</td>
</tr>
<tr>
<td></td>
<td>For details, see <em>Appliance Statuses on page 6-10.</em></td>
</tr>
</tbody>
</table>
Appliance Statuses

Deep Discovery Director (Distributed Mode) displays any of the following appliance statuses.

**TABLE 6-5. 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 (Distributed Mode).</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>
<tr>
<td>Unsuccessful</td>
<td>Any of the following situations may apply.</td>
</tr>
<tr>
<td></td>
<td>• The appliance was unable to execute the plan.</td>
</tr>
<tr>
<td></td>
<td>• The appliance is performing tasks that do not match the plan information.</td>
</tr>
<tr>
<td></td>
<td>• The appliance is connected to a Local Repository server that is unavailable or does not exist.</td>
</tr>
</tbody>
</table>
### Status and Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreachable</td>
<td>Any of the following situations may apply.</td>
</tr>
<tr>
<td></td>
<td>• The appliance has unregistered from Deep Discovery Director (Distributed Mode).</td>
</tr>
<tr>
<td></td>
<td>• The appliance has been deleted from Deep Discovery Director (Distributed Mode).</td>
</tr>
<tr>
<td>Cancelled</td>
<td>Any of the following situations may apply:</td>
</tr>
<tr>
<td></td>
<td>• The plan was manually cancelled before the appliance received the plan information from Deep Discovery Director (Distributed Mode).</td>
</tr>
<tr>
<td></td>
<td>• The plan was manually cancelled while the appliance was downloading files or executing the plan.</td>
</tr>
<tr>
<td></td>
<td>• The plan was manually cancelled while the appliance temporarily stopped downloading files.</td>
</tr>
</tbody>
</table>

### Other Plan Tasks

You can also perform the following tasks:
### Table 6-6. 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</td>
</tr>
<tr>
<td></td>
<td>Director (Distributed Mode).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hotfix / Critical Patch / Firmware</strong>: For details, see</td>
</tr>
<tr>
<td></td>
<td>*Adding a Hotfix / Critical Patch / Firmware Deployment</td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Analyzer images</strong>: For details, see *Adding a</td>
</tr>
<tr>
<td></td>
<td><em>Virtual Analyzer Images Deployment Plan on page 6-14.</em></td>
</tr>
<tr>
<td></td>
<td>• <strong>Configuration replication</strong>: For details, see *Adding a</td>
</tr>
<tr>
<td></td>
<td><em>Configuration Replication Plan on page 6-17.</em></td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director (Distributed Mode) does not allow</td>
</tr>
<tr>
<td></td>
<td>the creation of new plans when the license status is <strong>Not</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Activated</strong> or <strong>Expired</strong>. Existing plans will deploy</td>
</tr>
<tr>
<td></td>
<td>and execute as usual.</td>
</tr>
<tr>
<td></td>
<td>To activate Deep Discovery Director (Distributed Mode), see</td>
</tr>
<tr>
<td></td>
<td>License on page 8-38.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click a plan name with the status <strong>Pending</strong> and then click</td>
</tr>
<tr>
<td></td>
<td><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</td>
</tr>
<tr>
<td></td>
<td>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>
</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 Appliances > 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 (Distributed Mode) displays the list of files that are available in the repository. Verify that the file matches the product and language of the target appliances.

6. Select target appliances. Deep Discovery Director (Distributed Mode) only displays compatible appliances.

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

---

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create plan</td>
<td>Click a plan with the status <strong>Unsuccessful</strong> and then click <strong>Create Plan</strong>. Deep Discovery Director (Distributed Mode) will create a new plan based on the settings of the unsuccessfully deployed plan.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select a plan in the list with the status <strong>Pending</strong> and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
7. Specify the schedule.

- **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.
- **Deployment start**: Date at which this plan will be deployed.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plans are always deployed at 12:00 am (00:00) of the selected date.</td>
</tr>
</tbody>
</table>

- **Download period**: Period during which appliances are allowed to download the files required to execute the plan.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.</td>
</tr>
<tr>
<td>Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.</td>
</tr>
</tbody>
</table>

- **Execution start**: Date and time at which this plan will be executed.

<table>
<thead>
<tr>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>By schedule</strong> to prevent the plan from executing at an unexpected time.</td>
</tr>
</tbody>
</table>

- **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 6-7. 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.  
• **Type**: Internal  

| Deep Discovery Director (Distributed Mode) | • Integration with Deep Discovery Director (Distributed Mode) 1.1  
• Must be registered to Deep Discovery Director (Distributed Mode)  
• Must be in a Managed group |

**Procedure**

1. Go to **Appliances > 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 (Distributed Mode) displays the list of Virtual Analyzer images that are available in the repository.

---

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

---

**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.

---

10. (Optional) Modify the instances allocated to any image.

11. Select target appliances. Deep Discovery Director (Distributed Mode) only displays compatible appliances.

---

**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.

---

12. Specify the schedule.

- **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.
- **Deployment start**: Date at which this plan will be deployed.

---

**Note**

Plans are always deployed at 12:00 am (00:00) of the selected date.
• **Download period:** Period during which appliances are allowed to download the files required to execute the plan.

  **Note**
  - If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
  - Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

• **Execution start:** Date and time at which this plan will be executed.

  **Tip**
  Select **By schedule** to prevent the plan from executing at an unexpected time.

• **Immediate:** Starts immediately after the plan is saved.

13. 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 6-19*
• *Deep Discovery Email Inspector Replicated Configuration Settings on page 6-21*
• *Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings on page 6-23*
• *Deep Discovery Inspector 5.0 Replicated Configuration Settings on page 6-26*
Procedure

1. Go to Appliances > 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 (Distributed Mode) only displays compatible appliances.

7. Specify the schedule.
   - **Custom**: Deploys the plan, downloads the files, and executes the plan as specified.
     - **Deployment start**: Date at which this plan will be deployed.

   **Note**
   Plans are always deployed at 12:00 am (00:00) of the selected date.

   - **Download period**: Period during which appliances are allowed to download the files required to execute the plan.
Note

- If the download period is set from 8:00 pm to 4:00 am, appliances will start downloading files around 12:00 am immediately after the plan is deployed, not at 8:00 pm the following day.
- Setting the download period from 8:00 pm to 11:59 pm (or increase the margin) prevents the appliances from downloading files around 12:00 am immediately after the plan is deployed.

- **Execution start**: Date and time at which this plan will be executed.

Tip

Select **By schedule** to prevent the plan from executing at an unexpected time.

- **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 6-8. 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</td>
<td>Submissions</td>
</tr>
<tr>
<td></td>
<td>Filter settings</td>
</tr>
<tr>
<td></td>
<td>Suspicious Objects &gt; User-defined Match List</td>
</tr>
<tr>
<td></td>
<td>User-defined Match List</td>
</tr>
<tr>
<td></td>
<td>Exceptions list</td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Virtual Analyzer &gt; Sandbox Management</strong></td>
<td><strong>Archive Passwords</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Submission Settings</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Smart Feedback</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cloud Sandbox</strong></td>
</tr>
<tr>
<td><strong>Alerts / Reports &gt; Alerts</strong></td>
<td><strong>Rules</strong></td>
</tr>
<tr>
<td><strong>Alerts / Reports &gt; Reports</strong></td>
<td><strong>Schedules</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Customization</strong></td>
</tr>
<tr>
<td><strong>Administration &gt; Updates &gt; Component Update Settings</strong></td>
<td><strong>Component Update</strong></td>
</tr>
<tr>
<td><strong>Administration &gt; Integrated Products/Services</strong></td>
<td><strong>Log Settings</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Smart Protection</strong></td>
</tr>
<tr>
<td><strong>Administration &gt; System Settings</strong></td>
<td><strong>Proxy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SMTP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Time</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SNMP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Password Policy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Session Timeout</strong></td>
</tr>
<tr>
<td><strong>Administration &gt; Accounts / Contacts</strong></td>
<td><strong>Accounts</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Contacts</strong></td>
</tr>
<tr>
<td><strong>Administration &gt; System Maintenance &gt; Back Up</strong></td>
<td><strong>Automatic backup settings</strong></td>
</tr>
</tbody>
</table>
Deep Discovery Email Inspector Replicated Configuration Settings

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

**Table 6-9. 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</td>
<td>Actions settings</td>
</tr>
<tr>
<td></td>
<td>Recipient notification</td>
</tr>
<tr>
<td></td>
<td>subject and message</td>
</tr>
<tr>
<td></td>
<td>Message Tags</td>
</tr>
<tr>
<td></td>
<td>Attachment replacement file</td>
</tr>
<tr>
<td></td>
<td>End Stamp message</td>
</tr>
<tr>
<td>Redirect Pages</td>
<td>Blocking and Warning Pages</td>
</tr>
<tr>
<td></td>
<td>settings</td>
</tr>
<tr>
<td>Policy &gt; Exceptions</td>
<td>Messages</td>
</tr>
<tr>
<td></td>
<td>Specified senders, recipients, and X-headers</td>
</tr>
<tr>
<td></td>
<td>Objects</td>
</tr>
<tr>
<td></td>
<td>Excepted objects list</td>
</tr>
<tr>
<td>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</td>
<td>Schedule setting</td>
</tr>
<tr>
<td></td>
<td>Source</td>
</tr>
<tr>
<td></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</td>
<td>Operation Mode</td>
</tr>
<tr>
<td>Proxy</td>
<td>Proxy settings</td>
</tr>
<tr>
<td>SMTP</td>
<td>SMTP settings</td>
</tr>
<tr>
<td>Time</td>
<td>Time settings</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Administration &gt; Mail Settings</td>
<td>Connections</td>
</tr>
<tr>
<td>Message Delivery</td>
<td>All message delivery profiles</td>
</tr>
<tr>
<td>Limits and Exceptions</td>
<td>Limits and exceptions settings</td>
</tr>
<tr>
<td>SMTP Greeting</td>
<td>SMTP greeting message</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>Log Settings</td>
<td>All syslog server settings</td>
</tr>
<tr>
<td>SFTP</td>
<td>SFTP settings</td>
</tr>
<tr>
<td>Administration &gt; Scanning / Analysis</td>
<td>Settings</td>
</tr>
<tr>
<td>File Passwords</td>
<td>Passwords list</td>
</tr>
<tr>
<td>Smart Protection</td>
<td>Smart Protection settings</td>
</tr>
<tr>
<td>Smart Feedback</td>
<td>Smart Feedback settings</td>
</tr>
<tr>
<td>YARA Rules</td>
<td>All YARA rule files</td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Storage Maintenance</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Accounts / Contacts</td>
<td>Accounts</td>
</tr>
<tr>
<td>Contacts</td>
<td>Contacts list</td>
</tr>
</tbody>
</table>
Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings

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

**TABLE 6-10. Deep Discovery Inspector 3.8 SP5 Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>Affected Hosts</td>
</tr>
<tr>
<td></td>
<td>Only Saved Searches</td>
</tr>
<tr>
<td></td>
<td>Affected Hosts - Host Details</td>
</tr>
<tr>
<td></td>
<td>All Detections</td>
</tr>
<tr>
<td>Reports</td>
<td>Schedules</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Administration &gt; Notifications</td>
<td>Notification Settings &gt; Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Risk Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Suspicious Hosts Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Network Traffic</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Unanalyzed Sample Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Virtual Analyzer Detections</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Deny List</td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Retro Scan Detections</td>
</tr>
<tr>
<td></td>
<td>Delivery Options &gt; Email Settings</td>
</tr>
<tr>
<td></td>
<td>All settings</td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning</td>
<td>Hosts / Ports</td>
</tr>
<tr>
<td></td>
<td>Threat Detections</td>
</tr>
<tr>
<td></td>
<td>Web Reputation</td>
</tr>
<tr>
<td></td>
<td>Application Filters</td>
</tr>
<tr>
<td></td>
<td>Deny List / Allow List</td>
</tr>
<tr>
<td></td>
<td>Detection Rules</td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer</td>
<td>File Submissions</td>
</tr>
<tr>
<td></td>
<td>Internal Virtual Analyzer &gt; Passwords</td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets</td>
<td>Network Groups</td>
</tr>
<tr>
<td></td>
<td>Registered Domains</td>
</tr>
<tr>
<td></td>
<td>Registered Services</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services</td>
<td>Syslog</td>
</tr>
<tr>
<td>Administration &gt; System Settings</td>
<td>Proxy</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>Time</td>
</tr>
<tr>
<td></td>
<td>Session Timeout</td>
</tr>
<tr>
<td>Administration &gt; Accounts</td>
<td>All settings</td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Storage Maintenance</td>
<td>Only File Size Settings</td>
</tr>
</tbody>
</table>
Deep Discovery Inspector 5.0 Replicated Configuration Settings

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

**TABLE 6-11. Deep Discovery Inspector 5.0 Replicated Configuration Settings**

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>Affected Hosts</td>
<td>Only Saved Searches</td>
</tr>
<tr>
<td></td>
<td>Affected Hosts - Host Details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All Detections</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>Schedules</td>
<td>All settings</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
<td></td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
<td>Settings</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Administration &gt;</td>
<td>Notification Settings &gt; Threat Detections</td>
<td>All settings</td>
</tr>
<tr>
<td>Notifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Risk Hosts Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Suspicious Hosts Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; High Network Traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Unanalyzed Sample Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Virtual Analyzer Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Deny List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notification Settings &gt; Retro Scan Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delivery Options &gt; Email Settings</td>
<td></td>
</tr>
<tr>
<td>Screen</td>
<td>Element</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Monitoring / Scanning</td>
<td>Hosts / Ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Detections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web Reputation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Filters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deny List / Allow List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detection Rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Packet Capture</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Virtual Analyzer</td>
<td>Setup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Submissions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Virtual Analyzer &gt; Passwords</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Network Groups and Assets</td>
<td>Network Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registered Domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registered Services</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/</td>
<td>Threat Intelligence Sharing</td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td>Registered Domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registered Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Active Directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
<tr>
<td>SCREEN</td>
<td>ELEMENT</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; System Settings</td>
<td>Network</td>
<td>Only Secure Protocol setting</td>
</tr>
<tr>
<td>Proxy</td>
<td>All settings</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Accounts</td>
<td>All settings</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; System Maintenance &gt; Storage Maintenance</td>
<td>Only File Size Settings</td>
<td></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 6-30](#)
- [Uploading Virtual Analyzer Images on page 6-31](#)
- [Upload Center on page 6-32](#)

**Hotfixes / Critical Patches / Firmware**

Use the Hotfixes / Critical Patches / Firmware screen, in Appliances > Repository > Hotfixes / Critical Patches / 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 (Distributed Mode) 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 Appliances > Repository > Hotfixes / Critical Patches / 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 Appliances > 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**


---

**Uploading Virtual Analyzer Images**

Deep Discovery Director (Distributed Mode) supports consecutive uploading of up to three Virtual Analyzer image files through SFTP or network folder. Deep Discovery Director (Distributed Mode) 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 **Appliances > 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 (Distributed Mode) 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 on page 6-32**
- **Upload History on page 6-33**

---

**Uploading Files**

Information about files that are being uploaded to Deep Discovery Director (Distributed Mode) 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 6-12. 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>
</tbody>
</table>
2: Uploading to the repository

The file is being uploaded to the repository. All SFTP server and network folder file uploads can be cancelled by any user.

Note

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 6-13. 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>(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 (Distributed Mode) is displayed in this tab.

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

Uploaded files display the following information:
### TABLE 6-14. 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 Management 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** of the Deep Discovery Director Management Server.

3. Under **Connection Settings**, type the **API key** of the Deep Discovery Director Management Server.

### Note

You can find this information on the **Help** screen on the management console of the Deep Discovery Director Management Server.
4. Click **Register**.

**Note**

If the Deep Discovery Director Management Server fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director Management Server 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 Management Server.

---

**Connecting to the Central Repository Server**

**Note**

If proxy settings have been configured, Deep Discovery Director (Distributed Mode) connects to the Central Repository server using the proxy server.

For details, see *Proxy* on page 8-9.

**Procedure**

1. On the management console of the Deep Discovery Director Management Server, go to **Appliances** > **Connection Settings** > **Central Repository**.
2. Type the IPv4 address or FQDN of the Central Repository server.
3. Type the API key of the Central Repository server.

**Note**

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.
4. 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. On the management console of the Deep Discovery Director Management Server, go to **Appliances > Connection Settings > Local Repository**.

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

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

4. 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.

5. Click **Save**.

---
Chapter 7

Alerts

Learn about alert notifications and how to configure them in the following topics:

• About Alerts on page 7-2
• Triggered Alerts on page 7-2
• Built-in Rules on page 7-2
About Alerts

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

Triggered Alerts

The Triggered Alerts screen displays the following information:

**TABLE 7-1. Triggered Alerts Columns**

<table>
<thead>
<tr>
<th>Column</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered</td>
<td>The date and time when the alert was triggered.</td>
</tr>
<tr>
<td>Alert Level</td>
<td>An alert can be classified as any of the following levels.</td>
</tr>
<tr>
<td></td>
<td>• Critical: The event requires immediate attention</td>
</tr>
<tr>
<td></td>
<td>• Important: The event requires observation</td>
</tr>
<tr>
<td></td>
<td>• Informational: The event requires limited observation</td>
</tr>
<tr>
<td>Type</td>
<td>System: A built-in, system related rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggered the alert.</td>
</tr>
<tr>
<td>Criteria</td>
<td>The summarized criteria of the rule.</td>
</tr>
<tr>
<td>Details</td>
<td>Click the icon to view the full alert details, including the list of</td>
</tr>
<tr>
<td></td>
<td>recipients, subject, and message of the alert.</td>
</tr>
</tbody>
</table>

Built-in Rules

The Built-in Rules screen displays the following information:
### TABLE 7-2. Built-in Rules 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>Type</td>
<td><strong>System</strong>: A built-in, system related rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggers the alert.</td>
</tr>
<tr>
<td></td>
<td>To edit a rule, click on any link in the <strong>Rule</strong> column.</td>
</tr>
<tr>
<td>Criteria</td>
<td>The summarized criteria of the rule.</td>
</tr>
<tr>
<td>Alert Frequency</td>
<td>The frequency at which the alert is generated when the rule criteria are</td>
</tr>
<tr>
<td></td>
<td>met or exceeded.</td>
</tr>
<tr>
<td>Last Triggered</td>
<td>The date and time when the alert was last triggered.</td>
</tr>
<tr>
<td>Status</td>
<td>Click the toggle to enable or disable the rule.</td>
</tr>
</tbody>
</table>

### Editing a Built-in Rule

Edit rules to modify the frequency at which alerts are generated, the criteria, and the alert recipients.

#### Note
- By default, built-in rules are enabled and configured to send alerts to all contacts with valid email addresses.

#### Procedure

1. Go to Alerts > Built-in Rules.

   The **Built-in Rules** screen appears.
2. Click the name of the rule you want to edit in the Rule column.

   The Edit Rule screen appears.

3. Toggle the status of this rule.

4. Configure how often alerts are generated:

   • **Check frequency**: Select the frequency at which the rule criteria are checked

   • **Alert frequency**: Select the frequency at which the alert is generated when the rule criteria are met or exceeded

   **Note**

   - Shorter frequencies mean that the alert will be generated more often. Select longer frequencies to reduce the noise the alert generates.

   - System rules are configured to continuously check the rule criteria. Only the Alert frequency can be modified.

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

   **Note**

   This setting can be used in combination with the additional recipients field.

6. (Optional) Select a contact, type to search, or type an email address and press ENTER.

   The contact or account is added to the recipients.

7. (Optional) Modify the subject line. Compatible tokens are displayed on the right side and can be inserted at the text cursor's position by clicking the token.

8. Click **Save**.

   **Tip**

   Click **Restore Defaults** to restore this rule to its default values.
Administration

Learn how to administer Deep Discovery Director (Distributed Mode) in the following sections:

• Updates on page 8-2
• Integrated Products/Services on page 8-5
• System Settings on page 8-7
• Account Management on page 8-19
• System Logs on page 8-26
• System Maintenance on page 8-30
• License on page 8-38
Updates

Use the **Updates** screen, in **Administration > Updates**, to update components and install hotfixes, patches, and firmware upgrades to Deep Discovery Director (Distributed Mode).

Hotfixes / Patches

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

**TABLE 8-1. Hotfixes / Patches**

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

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 (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode) 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.

---

Integrated Products/Services

Deep Discovery Director (Distributed Mode) integrates with Microsoft Active Directory:

- Microsoft Active Directory on page 8-6
Microsoft Active Directory

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

Configuring Microsoft Active Directory Settings

Procedure

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

2. Go to Administration > Integrated Products/Services > Microsoft Active Directory.

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 8-8
- Proxy on page 8-9
- SMTP on page 8-10
- SNMP on page 8-11
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 (Distributed Mode) 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 4-1*.

---

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

**Configuring Port Binding**

Deep Discovery Director (Distributed Mode) supports the binding of services to a second network port.

When this feature is selected, Deep Discovery Director (Distributed Mode) directs all connections to the Central Repository server and the license update server through eth1.

---

**Note**

- This feature cannot be configured from the preconfiguration console.
- 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

The **Management Server** and **Local Repository** servers support 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

Deep Discovery Director (Distributed Mode) can be configured to use a proxy server to connect to the Central Repository and license update 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. Select Use a proxy server to connect to the Internet.
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. Select the security protocol to use for connections to the SMTP server.

5. (Optional) Modify the port number.

6. Type a sender email address.

7. (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 (Distributed Mode).

---

8. (Optional) Verify that Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) 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.

---

**SNMP**

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

Use the Administration > System Settings > SNMP screen to perform the following tasks:

• Configure Deep Discovery Director (Distributed Mode) to send trap messages.
  For details, see Configuring Trap Messages on page 8-12.

• Configure Deep Discovery Director (Distributed Mode) to listen for manager requests.
  For details, see Configuring Manager Requests on page 8-14.

Configuring Trap Messages

A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.

Procedure

1. Go to Administration > System Settings > SNMP.
2. Under Trap Messages, select Send SNMP trap messages.
3. Specify the trap message settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager server address</td>
<td>Specify the manager server address.</td>
</tr>
<tr>
<td><strong>OPTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| SNMP version | Select the SNMP version:  
  - SNMPv1/SNMPv2c  
  - SNMPv3  
  If you use SNMPv3, configure the SNMP server as follows:  
    - Context Name: "" (default context)  
    - Context Engine ID: <Auto>  
    - (Optional) Authentication protocol: HMAC-SHA  
    - (Optional) Privacy protocol: CBC-AES-128 |
| Community name | Specify a community name. |
| Security model | **Note**  
  This field is only available for SNMPv3.  
  Select the security model:  
  - No authentication or privacy  
  - Authenticated  
  - Authenticated with privacy |
| User name | **Note**  
  This field is only available for SNMPv3.  
  Specify the user name. |
| Password | **Note**  
  This field is only available for SNMPv3.  
  Specify the password. |
4. Click Save.

5. (Optional) Click Download MIB to download the Management Information Database (MIB) files.

Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

## Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request Deep Discovery Director (Distributed Mode) system information.

### Procedure

1. Go to Administration > System Settings > SNMP.

2. Under Manager Requests, select Listen for requests from SNMP managers.

3. Specify the manager request settings.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device location</td>
<td>Specify the location of this appliance.</td>
</tr>
<tr>
<td>Administrator contact</td>
<td>Specify the administrator contact of this appliance.</td>
</tr>
<tr>
<td><strong>OPTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Select the SNMP version:</td>
</tr>
<tr>
<td></td>
<td>• SNMPv1/SNMPv2c</td>
</tr>
<tr>
<td></td>
<td>• SNMPv3</td>
</tr>
<tr>
<td></td>
<td>If you use SNMPv3, configure the SNMP server as follows:</td>
</tr>
<tr>
<td></td>
<td>• Context Name: &quot;&quot; (default context)</td>
</tr>
<tr>
<td></td>
<td>• Context Engine ID: &lt;Auto&gt;</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Authentication protocol: <a href="https://www.snmp.org/standard/rfc1213">https://www.snmp.org/standard/rfc1213</a></td>
</tr>
<tr>
<td></td>
<td>• (Optional) Privacy protocol: <a href="https://www.snmp.org/standard/rfc1323">https://www.snmp.org/standard/rfc1323</a></td>
</tr>
<tr>
<td>Allowed community names</td>
<td>Specify a maximum of 5 community names.</td>
</tr>
<tr>
<td>Security model</td>
<td>Select the security model:</td>
</tr>
<tr>
<td></td>
<td>• No authentication or privacy</td>
</tr>
<tr>
<td></td>
<td>• Authenticated</td>
</tr>
<tr>
<td></td>
<td>• Authenticated with privacy</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password.</td>
</tr>
</tbody>
</table>

**Note**
This field is only available for SNMPv3.
### Privacy passphrase

**Note**

This field is only available for SNMPv3.

Specify the privacy passphrase.

**Trusted manager server addresses**

Specify a maximum of 32 trusted manager server addresses.

---

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

---

### 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 8-16*.

### 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.

4. Under **Download**, type a speed limit value to 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.

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 (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode).

---

**Important**

Accessing the management console of a Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) servers and Deep Discovery appliances. Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) uses a certificate to create secure connections to clients. Import a new certificate to change the fingerprint, or to adopt another Certificate Authority.
WARNING!

• Verify that your web browser accepts the new certificate before importing it. Importing a certificate that is not accepted by your web browser will leave you unable to access the management console.

• 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.

Account Management

Deep Discovery Director (Distributed Mode) uses role-based administration to grant and control access to the management console. Use this feature to assign specific management console privileges to the accounts and present them with only the tools and permissions necessary to perform specific tasks.

Each account is assigned a specific role. A role defines the level of access to the management console.
Accounts

Use the Accounts screen, in Administration > Account Management > 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 (Distributed Mode) supports the creation of user accounts by using the following methods:

- Adding a Local User Account on page 8-20
- Adding an Active Directory User Account or Group on page 8-21

**Note**

This method is only available if Microsoft Active Directory settings have been configured.

For details, see Microsoft Active Directory on page 8-6.

Adding a Local User Account

**Procedure**

1. Go to Administration > Account Management > 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
Click the **Show password** icon to unmask the password and skip this step.

7. (Optional) Type a valid email address that can be used to receive alerts sent by Deep Discovery Director (Distributed Mode).

8. Select a **Role** for this account. The role determines the level of access this account has.
   
   For details, see *Roles on page 8-24*.

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 (Distributed Mode).

---

*Note*

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

  For details, see *Microsoft Active Directory on page 8-6*.

- Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) 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 (Distributed Mode) is determined by the highest level of access granted to the user's Deep Discovery Director (Distributed Mode) account or any group the user is a member of.
Procedure

1. Go to **Administration > Account Management > 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.

   ![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

5. Select the Active Directory user account or group to add.

   ![Note]

   The Active Directory email address of the user account or group will be used on Deep Discovery Director (Distributed Mode).

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

   For details, see [Roles on page 8-24](#).

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

8. Click **Save**.
Other Accounts Tasks

You can also perform the following tasks:

### TABLE 8-2. Other Tasks

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Edit account | Click on a user name to open the **Edit Account** screen and do the following:  
• Toggle the account status  
• Change the password  
• Change the email address  
• Change the role  
• Modify the description |

**Note**  
- The passwords and email addresses of Microsoft Active Directory accounts cannot be changed from the management console.  
- 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.

| Delete account | Select one or more user accounts to delete and then click **Delete**.  
|----------------|-------------------------------------------------------------|

**Note**  
- There must be at least one local user account using the built-in administrator role.  
- You cannot delete the logged-on account.  
- Users who are currently logged on to the management console will be logged off automatically.
Deep Discovery Director (Distributed Mode) 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.

**Note**
Microsoft Active Directory accounts are never locked.

**Toggle account status**
Click on the toggle in the **Status** column to enable or disable the user account.

**Note**
- At least one local user account using the built-in administrator role must be enabled.
- Users who are currently logged on to the management console and whose accounts are disabled will be logged off automatically.

### Roles

Use the **Roles** screen, in **Administration > Account Management > Roles**, to create and manage user roles. Assign each user a role that will restrict their activities to all but those necessary for the completion of their duties.

Deep Discovery Director (Distributed Mode) comes with a set of built-in user roles that you cannot delete:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Built-in Administrator role with full access to all management console features</td>
</tr>
<tr>
<td>Operator</td>
<td>Built-in Operator role with read-only access to all management console features</td>
</tr>
</tbody>
</table>
Deep Discovery Director (Distributed Mode) also supports custom user roles. Create new roles to limit access to the management console, and to restrict users from seeing and managing specific appliances.

**Adding a Role**

**Procedure**

1. Go to Administration > Account Management > Roles, and then click Add.
   
   The Add Role screen appears.

2. Type a role name.

3. Select a Permission for this role.

4. Select the appliances this role can see and manage.

5. Select an account, or type to search and press ENTER, and then click Add to add the selected account to this rule.

   **Note**
   
   Added accounts will be removed from all other roles.

6. (Optional) Type a description for this role.

7. Click Save.

**Other Roles Tasks**

You can also perform the following tasks:
TABLE 8-3. Other Tasks

<table>
<thead>
<tr>
<th>TASK</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Edit role     | Click on a role name to open the **Edit Role** screen and do the following:  
|               | • Modify the role name  
|               | • Change the permission  
|               | • Modify the appliances this role can see and manage  
|               | • Add accounts to this role  
|               | • Modify the description  
|               |  
| **Note**      | You cannot modify the role name, permission, appliance access rights, and description of built-in roles.  
|               | • Users who are currently logged on to the management console and whose appliance access rights are modified 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.  
| Delete role    | Select one or more user roles to delete and then click **Delete**.  
|               |  
| **Note**      | You cannot delete built-in roles.  
|               | You cannot delete roles that are in use by at least one account.  

System Logs

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

Deep Discovery Director (Distributed Mode) 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 8-28.

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

**Table 8-4. System Log Information**

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged</td>
<td>Event date and time</td>
</tr>
</tbody>
</table>
| Event ID   | Event identifier  
Each specific action has its own event ID. Examples:  
• 20001  
  **Description:** User logged on  
• 20002  
  **Description:** User logged off |
| Type       | One of the following types displays:  
• Account Logon/Logoff  
• System  
• Update |
| Level      | One of the following levels displays:  
• Informational  
• Warning  
• Error |
### 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 8-30*
- *Storage on page 8-31*
- *Back Up on page 8-31*
- *Restore on page 8-34*
- *Power Off / Restart on page 8-38*

---

**System Status**

The **System Status** screen displays the utilization of key hardware components:

- 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 (Distributed Mode) saves database entries and system logs.

Under Database Storage, configure the following:

- **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 (Distributed Mode) 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 (Distributed Mode) 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 8-33*

- *Configuring Automatic Backups on page 8-33*

The following table shows the screens and elements with backed up configuration settings.
# Table 8-5. Backed Up Configuration Settings

<table>
<thead>
<tr>
<th>Screen</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances &gt; Directory</td>
<td>Appliance tree with group structure</td>
</tr>
<tr>
<td></td>
<td>Registered appliances and appliance details</td>
</tr>
<tr>
<td>Appliances &gt; Plans</td>
<td>All plans</td>
</tr>
<tr>
<td>Appliances &gt; Connection Settings</td>
<td>Central Repository settings</td>
</tr>
<tr>
<td></td>
<td>Local Repository off-hour settings</td>
</tr>
<tr>
<td></td>
<td>Local Repository server assignments</td>
</tr>
<tr>
<td>Alerts</td>
<td>All triggered alert records</td>
</tr>
<tr>
<td></td>
<td>All rule settings</td>
</tr>
<tr>
<td>Administration &gt; Integrated Products/Services</td>
<td>Microsoft Active Directory server settings</td>
</tr>
<tr>
<td>Administration &gt; System Settings</td>
<td>Proxy settings</td>
</tr>
<tr>
<td></td>
<td>Bandwidth usage throttling settings</td>
</tr>
<tr>
<td></td>
<td>Time settings</td>
</tr>
<tr>
<td></td>
<td>Certificate</td>
</tr>
<tr>
<td></td>
<td>Session timeout value</td>
</tr>
<tr>
<td>Administration &gt; Account Management</td>
<td>All user accounts</td>
</tr>
<tr>
<td></td>
<td>All roles</td>
</tr>
<tr>
<td>Administration &gt; System Logs</td>
<td>All system logs</td>
</tr>
</tbody>
</table>
Exporting a Configuration Settings and Database Backup

Deep Discovery Director (Distributed Mode) can export a backup file of most configuration settings and the database. Use the backup file to restore Deep Discovery Director (Distributed Mode) 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 8-31.

3. Download and save the backup file.

Configuring Automatic Backups

Deep Discovery Director (Distributed Mode) 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 (Distributed Mode) creates up to five backup files, after which the oldest one is deleted in order to keep the number of backup files at five.

<table>
<thead>
<tr>
<th>SCREEN</th>
<th>ELEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; System Maintenance</td>
<td>Storage</td>
</tr>
<tr>
<td></td>
<td>Storage values</td>
</tr>
<tr>
<td></td>
<td>Back Up</td>
</tr>
<tr>
<td></td>
<td>Automatic backup settings</td>
</tr>
<tr>
<td>Help</td>
<td>API key</td>
</tr>
</tbody>
</table>
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 (Distributed Mode) 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 8-35
- Replacing the Active Server with Another Server on page 8-36

---

Note

For more information on exporting a configuration settings and database backup, see Exporting a Configuration Settings and Database Backup on page 8-33.
Restoring a Configuration Settings and Database Backup

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

If the active Deep Discovery Director (Distributed Mode) 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 8-36.

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 (Distributed Mode) displays information about the backup file.

4. Click Restore.

   Deep Discovery Director (Distributed Mode) displays a confirmation message.

5. Click OK.

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

6. (Optional) Verify that the repository is functional. 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 8-8.

8. (Optional) Activate Deep Discovery Director (Distributed Mode). For details, see License on page 8-38.
The server is now ready to resume operation.

Replacing the Active Server with Another Server

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

Host machine hardware, host machine software, and Deep Discovery Director (Distributed Mode) version and build of the replacement server must be the same as the active server.

For details, see System Requirements on page 2-1.

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 8-31.
   c. Download and save the backup file.

2. Install Deep Discovery Director (Distributed Mode) on the replacement server.
   For details, see Installing Deep Discovery Director on page 3-1.

3. Configure temporary network addresses for the replacement server.
   For details, see Configuring Network Addresses on the Preconfiguration Console on page 4-1.

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 (Distributed Mode) displays information about the backup file.
   d. Click **Restore**.
      
      Deep Discovery Director (Distributed Mode) displays a confirmation message.
   e. Click **OK**.
      
      Deep Discovery Director (Distributed Mode) restores configuration settings and database from the backup file, and then restarts the server.

6. Verify that the repository is functional. 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 8-8.

9. Activate Deep Discovery Director (Distributed Mode). For details, see License on page 8-38.

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 > System Maintenance > 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 (Distributed Mode) license.

The License screen includes the following information and options.
### Table 8-6. License Details

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays either <strong>Activated</strong>, <strong>Not Activated</strong>, or <strong>Expired</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Director (Distributed Mode) 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>Click <strong>View details</strong> to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated in the screen, click <strong>Refresh</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If proxy settings are enabled, Deep Discovery Director (Distributed Mode) connects to the license update server using the proxy server.</td>
</tr>
<tr>
<td>Type</td>
<td>• <strong>Full</strong>: Provides access to all product features</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trial</strong>: 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 it expires. Click <strong>View renewal instructions</strong> to view instructions from the Trend Micro website.</td>
</tr>
</tbody>
</table>
### Field Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>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 <strong>New Activation Code</strong>, and type the new Activation Code. The <strong>License</strong> screen reappears displaying the number of days left before the product expires.</td>
</tr>
</tbody>
</table>

**Tip**

Deep Discovery Director (Distributed Mode) can be activated with the Activation Code of any Deep Discovery product.
Chapter 9

Technical Support

Learn about the following topics:

• Troubleshooting Resources on page 9-2
• Contacting Trend Micro on page 9-3
• Sending Suspicious Content to Trend Micro on page 9-4
• Other Resources on page 9-5
Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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:

| Address | Trend Micro, Incorporated  
|---------|---------------------------|
|         | 225 E. John Carpenter Freeway, Suite 1500  
|         | Irving, Texas 75062 U.S.A.  
| Phone   | Phone: +1 (817) 569-8900  
|         | Toll-free: (888) 762-8736  
| Website | [http://www.trendmicro.com](http://www.trendmicro.com)  
| Email address | support@trendmicro.com  

- 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